THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

REVISITED 2015: 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 national and 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. In 2008, the author recommended two critical amendments to the Economic Espionage Act that have been vetted and have been the subject of legislative proposals for the past 7 years. The author now revisits developments since 2008 and underscores the urgency and the compelling national and economic interests in amending the Economic Espionage Act of 1996 in the 114th Congress.

Cite as R. Mark Halligan , *Revisited 2015: Protection of* U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996, 14 J. MARSHALL REV. INTELL. PROP. L. 476 (2015).

REVISITED 2015: PROTECTION OF U.S. TRADE SECRET ASSETS: CRITICAL AMENDMENTS TO THE ECONOMIC ESPIONAGE ACT OF 1996

R. MARK HALLIGAN

REVISITED 2015: PROTECTION OF U.S. TRADE SECRET ASSETS: CRITICAL AMENDMENTS TO THE ECONOMIC ESPIONAGE ACT OF 1996

R. MARK HALLIGAN *

I. 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] In 2008, this author recommended two critical amendments to the Economic Espionage Act of 1996: (1) the addition of a private civil cause of action; (2) the addition of a civil ex parte seizure provision.[3] Alarm bells were ringing loud and clear in 2008: trade secret theft had become rampant, United States' industry had 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] Consequently, legislation was introduced in the 112th and 113th Congress to add a private civil cause of action to the Economic Espionage Act and to add ex parte provisions to the EEA.[5] In

---

 Mr. Halligan is an accomplished trial lawyer who focuses his practice on intellectual property litigation and complex commercial litigation, including antitrust and licensing issues.Mr. Halligan has successfully represented both individuals and corporations as plaintiffs and defendants in federal and state courts throughout the United States and Mr. Halligan is recognized as a one of the leading lawyers in trade secrets litigation in the United States by Legal 500 and he is recognized by Chambers USA: America's Leading Lawyers for Business for his exceptional standing in intellectual property law. In recent years, Mr. Halligan has been at the forefront of international developments in intellectual property law and he is a recognized thought leader in the ever-growing area of trade secrets law having spoken worldwide to numerous organizations and corporations on the topic.

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

[2] *Id.* at sec. 101, 110 Stat. 3489 (codified at 18 U.S.C. § 1832(a) (2006)).

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

[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); *see also* NAT'L INTELLECTUAL. PROP. LAW. ENFORCEMENT COORDINATION COUNCIL, REPORT TO THE PRESIDENT AND CONGRESS ON COORDINATION OF INTELLECTUAL PROPERTY ENFORCEMENT AND PROTECTION at 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.*

[5] *See* 142 CONG. REC. S12,207 (statement of Sen. Specter):

> 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 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

the 113th Congress, Senators Chris Coons (D-DE) and Orrin Hatch (R-UT) introduced The Defend Trade Secrets Act of 2014, S.2267, the first major bipartisan effort in this regard. Subsequently, Representatives George Holding (R-NC) and Jerrold Nadler (D-NY), along with over 20 bipartisan cosponsors, introduced a modified version of the Coons-Hatch bill as The Trade Secret Protection Act of 2014, H.R. 5233. In September 2014, the House Judiciary Committee favorably reported H.R. 5233 by voice vote. No further action occurred on the bill in the 113th Congress.[6] In the 114th Congress, on July 30, 2015, the legislation was reintroduced in both chambers in identical and concerted fashion. That legislation, named The Defend Trade Secrets Act of 2015 (S. 1890 and H.R. 3326) was introduced in the Senate by Senators Hatch, Coons, Jeff Flake (R-AZ), Dick Durbin (D-IL), Thom Tillis (R-NC) and Tammy Baldwin (D-WI), and in the House by Representatives Doug Collins (R-GA), Nadler, Holding, John Conyers (D-MI), Steve Chabot (R-OH) and Hakeem Jeffries (D-NY). Committee action is expected on the legislation in both chambers later this Congress.[7]

II. 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.[8] Congress recognized that protecting U.S. trade secrets was necessary to "maintain our industrial and economic edge and thus safeguard our national security."[9] According to Senator Herbert H. Kohl, a company's proprietary information is incredibly important:

> [B]usinesses spend huge amounts of money, time, and though developing proprietary economic information -- their customer lists, pricing schedules, business agreements, manufacturing processes. This information is literally

---

minds of Americans, both native born and immigrants who find the freedom here to try new ideas and add to our economic strength."

Id.; see also 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").

[6] Trade Secret Protection Act of 2014 [hereinafter TSPA], H.R. 5233, 113th Cong. (2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/5233/cosponsors (last visited May 25, 2015).

[7] *See* CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/house-bill/5233 (last visited May 28, 2015)(showing that the Trade Secret Protection Act, H.R. 5233, has been introduced, but not passed during the 113th Congress).

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

[9] 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.").

> 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.[10]

These observations by Senator Kohl almost 20 years ago are manifested every day in 2015. U.S. corporations are immersed in intense global competition and American industry is being challenged both at home and abroad.[11] Today, it is estimated that 80% of the assets of new economy companies are intangible assets and the vast bulk of intangible assets are trade secret assets.[12] 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.[13] These structural changes have been accompanied by a computer revolution and transition to the Information Age.[14] The power of computer technology has increased exponentially, resulting in more powerful means for the theft and transfer of proprietary information.[15] The rapid growth of the Internet is a reflection of this boom.[16] In fact, the corollary is also true: the Internet is now a tool for the destruction of trade secret assets.[17]

---

[10] 142 CONG. REC. S740 (daily ed. Feb. 1, 1996) (statement of Sen. Kohl).

[11] *See generally* 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").

[12] *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 . . . ."); Mary Juetten, *Pay Attention to Innovation and Intangibles – They're More than 80% of your Business' Value*, FORBES.COM, http://www.forbes.com/sites/maryjuetten/2014/10/02/pay-attention-to-innovation-and-intangibles-more-than-80-of-your-business-value/ (Oct. 2, 2014)(noting that innovation and intellectual property assets comprise 80% or more of a business's assets).

[13] *See* NIPLECC Report, *supra* note 4, at 45 ("Protecting IP . . . is crucial to increasing trade and competing in the global economy.").

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

[15] *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.").

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

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

Computers facilitate the instant copying and transfer of proprietary information surreptitiously.[18] 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.[19] The receiving party can do the same thing -- and the cycle can be repeated -- over and over again.[20] Within days or even hours, a U.S. company can lose complete control over its trade secret assets forever.[21]

Before the EEA, federal prosecutors relied primarily upon the National Stolen Property Act[22] and the wire and mail fraud statutes to commence criminal prosecutions for trade secret theft. Both statutes were ineffective.[23] On the day the EEA was enacted, President Clinton issued the following statement:[24]

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

---

[18] *Id.*

[19] *See* World Intellectual Property Organization, *Intellectual Property on the Internet, A Survey of Issues*, https://web.archive.org/web/20030604133814/http://ecommerce.wipo.int/survey/html/index.html#_ftnref68 [hereinafter "WIPO Report"] (December 2002)(noting that users can make unlimited copies, virtually instantaneously).

[20] *Id.* (calling the internet the "world's biggest copy machine.").

[21] 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):

> 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 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 assets.

Id. at 225 (footnote omitted); *See also* 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):

> 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.

Id. at 1154; 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).

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

[23] *See* Rustad, *supra* note 4, at 465-66.

[24] 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.

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, damage, or steal from computer networks. I am pleased to sign it into law.[25] The EEA is a watershed statute, recognizing U.S. national and economic interests in protecting the trade secret assets of U.S. companies.[26] However, the EEA is ineffective as just a criminal statute. This was true in 2008 and remains critically so today in 2015.

III. PROPRIETARY INFORMATION LOSSES

At the time of the original article in 2008, ASIS International (ASIS) is the largest organization for security professionals with approximately 38,000 members worldwide.[27] ASIS has conducted seven Trends in Proprietary Information Loss Surveys over the past 17 years.[28] "The resulting reports have been used by U.S. government agencies and private entities."[29] The ASIS survey was considered the most authoritative resource on proprietary information losses by U.S. companies and the survey findings are relied upon by and cited in the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.[30]

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.[31] The results confirm that proprietary information losses are continuing and

---

[25] *Id.*

[26] 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.").

[27] ASIS International, About ASIS, https://www.asisonline.org/About-ASIS/Pages/default.aspx (last visited May 23, 2015).

[28] ASIS INTERNATIONAL, TRENDS IN PROPRIETARY INFORMATION LOSS at 4 (2007), *available at* https://web.archive.org/web/20071030203849/https://www.asisonline.org/newsroom/surveys/spi2.pdf.

[29] *Id.*

[30] *Id.* at 1 (noting that the survey "has come to be recognized as the premier study of its kind"); *Id.* at 4 (noting that the survey "findings have been cited in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*").

[31] *Id.* at 1.

increasing both in the United States and abroad.[32] 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.[33] 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.[34] The top three foreign countries identified were China, Russia and India.[35] 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 data mining software all contributed to proprietary information losses.[36] These losses ranged from less than $ 10,000 to more than $ 5.5 million.[37]

The FBI was also sounding a five-alarm fire. Former FBI Director Robert Mueller testified that the ASIS estimate was grossly understated and estimated that as much as $ 200 billion was lost by U.S. companies to economic espionage in 2002 alone.[38] Other credible sources estimated loss as high as $ 400 billion annually.[39]

Now fast forward to 2015. Study after study, report after report, virtually every agency and department of the government reports that trade secret theft is accelerating.[40] There is a confluence of factors at work emanating from the digital environment in which we now live and work.[41] Advancements in technology, increased

---

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

[33] *Id.*

[34] *Id.*

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

[36] *Id.* at 3.

[37] *Id*

[38] 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.").

[39] 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."); *but see* OFFICE OF THE PRESIDENT OF THE UNITED STATES, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter Executive Office Trade Secret Summary](Feb. 2013)(noting that "estimates from academic literature on the losses of economic espionage range so widely as to be meaningless – from $2 billion to $400 billion annually – reflecting the scarcity of data and variety of methods used to calculate losses.").

[40] Executive Office Trade Secret Summary, *supra* note 39 at 1; *see also* OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, *Foreign Spies Stealing US Economic Secrets In Cyberspace* (November 2011) *available at*
http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[41] Jonathan L. Sulds, *Trade Secret Protection*, ASIS ONLINE, https://sm.asisonline.org/Pages/Trade-Secret-Protection.aspx (Nov. 1. 2011).

mobility, globalization and sophisticated cyber-tools and devices all contribute as catalysts for trade secret theft.[42]

The statistics are staggering. Last year, for example, the FBI sponsored a campaign in nine U.S. cities with billboards stating: "$13 Billion Lost—Protect America's Trade Secrets."[43] National Security Agency Director General Keith Alexander calls cyber-espionage "the greatest transfer of wealth in history."[44] Symantec places the cost of intellectual property theft for the U.S. economy at $250 billion a year.[45] McAfee estimates global remediation costs at $1 trillion per year.[46] Not a day goes by without another report of foreign economic espionage, computer attacks, and trade secret theft.

The U.S. Chamber of Commerce has estimated that publically traded U.S. companies own an estimated $5 trillion worth of trade secret assets.[47] Another recent study by PricewaterhouseCooper (PwC) and the Center for Responsible Enterprise and Trade (CREATe.org) estimates that the economic loss attributable to trade secret theft is between 1% and 3% of the U.S. Gross Domestic Product.[48]

IV. FEDERAL PROTECTION OF INTELLECTUAL PROPERTY ASSETS

U.S. law protects patents, copyrights, trademarks and trade secrets.[49] There is a civil cause of action under federal law for patent infringement.[50] There is a civil cause of action under federal law for copyright infringement.[51] There is a civil cause of action under federal law for trademark infringement.[52] There is not, however, a civil cause of action under federal law for trade secret misappropriation.[53]

---

[42] Executive Office Trade Secret Summary, *supra* note 39 at 20.

[43] FEDERAL BUREAU OF INVESTIGATIONS, *Economic Espionage. How to Spot A Possible Threat*, http://www.fbi.gov/news/stories/2012/may/insider_051112/insider_051112 (May 11, 2012)

[44] Keith Alexander, *An Introduction by General Alexander*, THE NEXT WAVE, Vol. 19, No. 4, https://www.nsa.gov/research/tnw/tnw194/article2.shtml (last visited May 24, 2015).

[45] Rich Dandliker, *Putting a face on Intellectual Property Theft*, SYMANTEC, https://www.nsa.gov/research/tnw/tnw194/article2.shtml (Jul. 11, 2012)

[46] The Economic Impact of Cybercrime and Cyber Espionage, Center for Strategic and International Studies, MCAFEE (July 2013) http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

[47] UNITED STATES CHAMBER OF COMMERCE, *The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement*, https://www.uschamber.com/sites/default/files/legacy/international/files/Final%20TPP%20Trade%20Secrets%208_0.pdf (last visited May 24, 2015).

[48] PRICEWATERHOUSECOOPER, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats* [hereinafter "PwC Report"] (February 2014), https://www.uschamber.com/sites/default/files/legacy/international/files/Final%20TPP%20Trade%20Secrets%208_0.pdf

[49] 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).

[50] *See* 35 U.S.C. §§ 271-73.

[51] *See* 17 U.S.C. §§ 501-05.

[52] *See* 15 U.S.C. §§ 1114-17.

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

The reasons for the step-child treatment of trade secrets are historical.[54] Patents and trademarks are the by-products of the Industrial Revolution.[55] Copyrights date back to the invention of the printing press, if not earlier.[56] 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.[57]

Even though the protection of confidential information dates back to Roman law,[58] and even though the birth of every patent starts out as a trade secret,[59] 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. in 1974.[60] Shortly thereafter, the Uniform Trade Secrets Act (UTSA) was promulgated by the National Conference of Commissioners on Uniform State Laws in 1979.[61] The stage was now set. In 1984,

---

[54] *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)(describing trade secrets protection evolving from a property right into the prevention of unfair competition).

[55] *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 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, *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).

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

[57] 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, 42 Wake Forest L. Rev. 1, 9 (2007):

> 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.

Id. at P18 (footnotes omitted); Simpson, *supra* note 54, at 1142 (discussing trade secret law's evolution into something similar to contract law).

[58] 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).

[59] 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).

[60] 416 U.S. 470 (1974).

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

the United States Supreme Court in Ruckelshaus v. Monsanto held that a trade secret asset was a property right protected by the United States Constitution.[62]

Of course, it has been decades since the computer revolution began and we now live in a completely different world where the protection of trade secret assets is of paramount importance.[63] Whatever advantages the United States has achieved in the development of the law of trade secrets will be lost if we do not deploy effective means to protect trade secret assets. U.S. companies are victims of international trade secret theft, and U.S. companies need access to the federal courts to protect trade secret assets.

There is no justification or policy interest today for depriving U.S. companies of access to the federal courts to protect U.S. trade secret assets.

V. PRIVATE ENFORCEMENT

U.S. businesses are the creators and owners of trade secret assets.[64] U.S. businesses are the victims of trade secret theft and foreign economic espionage.[65] U.S. businesses have the fiduciary and statutory obligation to protect trade secret assets;[66] finally, U.S. corporations have the financial means and financial incentive to protect trade secret assets.[67] The legislative history of the EEA recognizes that the protection

---

[62] 467 U.S. 986, 1002 (1984) (stating that a government taking of a trade secrets is governed by the Fifth Amendment).

[63] 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 (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."); 142 CONG. REC. S377 (1996) (statement of Sen. Cohen):

> 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.

[64] Scott Stewart, *At Work, Can You Keep What You A Trade Secret?,* ST. LOUIS POST-DISPATCH, Apr. 20, 2008, at E7 (articulating that businesses put significant efforts into creating intellectual property but fail to put the same effort into protecting that intellectual property).

[65] 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).

[66] 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).

[67] Czapracka, *supra* note 54, 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 21, 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.

of trade secret assets is in the national interest of the United States.[68] 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.[69]

Trade secret assets are the backbone of an information-based economy.[70] Trade secrets no longer comprise some paper files locked in a file cabinet in technology department. Today, trade secret assets and other intangible assets comprise over 80% of new economy companies and reside in computers and networks all over the world.[71]

Trade secret assets are critical to the competitiveness of companies creating jobs in the United States and abroad.[72] The creation of trade secrets means the creation of jobs; conversely, the loss of trade secret assets means the loss of jobs.[73] Focusing on the types of offenders does not change this fundamental equation. Whether the offender is an insider, a foreign intelligence service, a corporate competitor, or a transnational criminal organization, the effects of trade secret misappropriation are the same.[74]

Looking back another 25 years from now, it will undoubtedly be a historical footnote that the United States compromised and lost billions of dollars of wealth in trade secret assets because there was no federal cause of action to protect against the actual or threatened misappropriation of trade secrets and no statutory provisions for civil ex parte seizure orders to preserve evidence and to prevent the transfer of U.S. trade secret assets outside the United States.

Not surprisingly, there is now strong bipartisan support and strong corporate support for the two proposed amendments to the Economic Espionage Act of 1996.[75] Various proposals have been proposed and vetted by the American Bar Association (ABA), the American Intellectual Property Law Association (AIPLA), the Intellectual Property Owners Association (IPO) and there have been daily blogs recognizing that

---

[68] 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.").

[69] *See* Kevin Kelly, *New Rules for the New Economy*, WIRED.COM http://archive.wired.com/wired/archive/5.09/newrules_pr.html (last visited May 28, 2015)(noting that the term "new economy" was first mentioned in 1969, marking the beginning of "knowledge workers," and is often referred to as the "Information Economy").

[70] *"Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" Hearing Before the Subcomm. On Crime and Terrorism of the Judiciary Committee,* 114th Cong. (May 13, 2014)(Statement of Douglas K. Norman).

[71] Executive Office Trade Secret Summary, *supra* note 39 at 20, Juetten, *supra* note 12.

[72] *See* Michael B.G. Froman, *2015 Special 301 Report*, UNITED STATES TRADE REPRESENTATIVE https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf (April 2015)

[73] *Id.* (noting that an estimated 40 million U.S. jobs directly or indirectly rely on intellectual property intensive industries).

[74] *See generally* PwC, *supra* note 48 (discussing the undifferentiated effects of trade secret theft).

[75] *See* Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014) [hereinafter DTSA], *available at* https://www.congress.gov/bill/113th-congress/senate-bill/2267/text (last visited May 25, 2014); Trade Secret Protection Act of 2014, H.R. 5233, 113th Cong. (2014) [hereinafter TSPA], *available at* https://www.congress.gov/bill/113th-congress/house-bill/5233/text (last visited May 25, 2015).

these two critical amendments must be enacted to protect U.S. companies and U.S. economic interests.[76]

Recently, a law review article was published entitled "Here Come the Trade Secret Trolls" by David S. Levine and Sharon K. Sandeen raising for the first time the possibility that a new type of entity—which the authors call a "trade secret troll"—could emerge if the Congress amends the EEA to provide a private cause of action for trade secret misappropriation and statutory procedures for ex parte seizure orders.[77]

The academic exercise of attempting to conflate a "patent troll" with a non-existent possibility of the emergence of a "trade secret troll" is nonsense and ignores the historical development of trade secrets law in the United States over 200 years and almost 40 years of development of statutory case law under the Uniform Trade Secrets Act. Where are the trade secret trolls now or in the past?

So-called patent trolls (or non-practicing entities), some argue, purchase issued patents to file frivolous patent infringement lawsuits hoping to secure a quick-payday settlement because defendants want to avoid an expensive patent infringement lawsuit. There is no evidence of this alleged frivolous misconduct in trade secrets law. A trade secret is a fragile asset that exists as a trade secret because reasonable measures are being actively taken to protect the secrecy of the information and the owner of the trade secret is deriving economic value from the secrecy of the trade secret.

There is no registration system in trade secrets law; trade secrets cannot be bundled like a portfolio of patents. Establishing a prima facie case for trade secret misappropriation is not as simple as attached a publically issued patent as an exhibit to a federal complaint for patent infringement. Proving up a cause of action for trade secret misappropriation is a complex legal task; an identification of the alleged trade secret with particularity is required; a six-factor examination of the alleged trade secret is required; the reasonable measures taken to protect the alleged trade secret must be disclosed and proven up for that trade secret; then moving to the misappropriation analysis, the plaintiff must prove that the defendant breached a confidential relationship or used other improper means to acquire the trade secret, and then, made an unauthorized disclosure or use of the trade secret resulting in damages. Any trial lawyer (including this author) who has tried both patent and trade secrets cases will tell you without hesitation that trade secret cases are more difficult cases than patent infringement cases.

One of the key provisions of the Uniform Trade Secrets Act is Section 4—"Attorney's Fees."[78] This section provides that if a claim of misappropriation is made in bad faith, the court may award reasonable attorney's fees.[79] The courts have

---

[76] *See* Wayne P. Sobon, *AIPLA Support for H.R. 5233, the Trade Secrets Protection Act of 2014* (September 9, 2014), http://www.aipla.org/advocacy/congress/Documents/AIPLA%20Letter%20Supporting%20HR5233%20Trade%20Secret%209-9-2014.pdf; Lisa A. Dunner, *Letter to Representative Kevin McCarthy* (October 16, 2014), http://www.americanbar.org/content/dam/aba/administrative/intellectual_property_law/advocacy/advocacy-20141016-comments-hr5233.authcheckdam.pdf

[77] David S. Levine and Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH & LEE L. REV. ONLINE 230 (2015), http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss4/3

[78] *Id.* § 4.

[79] *Id.*

construed this provision to award attorney's fees if a complaint for trade secret misappropriation is filed in bad faith or if, after discovery, the Plaintiff continues to maintain and prosecute the specious trade secret misappropriation claim in bad faith.[80] The "bad faith" provision has deterred abuses for over 40 years and enacting a federal civil cause of action under the EEA will not change that because the recovery of attorney's fees for bad faith prosecution of a trade secret misappropriation claim will be incorporated in the EEA amendments.[81]

VI. 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).[82] This article proposes amendments to the EEA that will create a private cause of action under Section 1832; however there will be no amendments to the EEA relating to Section 1831 violations.

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;"[83]
>
> . "[W]ithout authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;"[84]
>
> . "[R]eceives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization."[85]

The EEA does not prohibit legitimate means of obtaining information, such as reverse engineering or independent development.[86] Moreover, the EEA was not

---

[80] Degussa Admixtures, Inc. v. Burnett, 277 Fed.Appx. 530, 533 (6th Cir. 2008)(awarding attorneys fees under Michigan trade secrets statute); FLIR Systems, Inc. v. Parrish, 174 Cal.App.4th 1270, 1276 (2009)(noting that an award of attorneys' fees is proper under California statute is the claim is groundless or if the claim is pursued "beyond a point where the plaintiff no longer believes the case has merit.").

[81] *See* TSPA, *supra* note 75.

[82] 18 U.S.C. § 1831 (2006) (entitled "Economic Espionage"); *id.* § 1832 (entitled "Theft of Trade Secrets").

[83] 18 U.S.C. § 1832(a)(1).

[84] 18 U.S.C. § 1832(a)(2).

[85] 18 U.S.C. § 1832(a)(3).

[86] *See* 142 CONG. REC. S12,213 (1996) (Manager's Statement for H.R. 3723, The Economic Espionage Act) ("If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent or [the EEA], then that form of 'reverse engineering' should be fine.").

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.[87]

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.[88]

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.[89]

Conspiracies and attempted thefts are also proscribed by the EEA.[90] The same types of penalties apply with increased penalties imposed if the trade secret misappropriation benefits a foreign government, foreign instrumentality or foreign agent.[91]

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

---

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 variety 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. *Id.,* 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).

[87] *See* 142 CONG. REC. S12,213 (1996) (Manager's Statement for H.R. 3723, The Economic Espionage Act) ("[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 86, at 1143.

[88] 18 U.S.C. § 1831(a)(3); *id.* § 1832(a)(3).

[89] 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).

[90] 18 U.S.C. § 1831(a)(5); *id.* § 1832(a)(3).

[91] 18 U.S.C. § 1831(a). *Compare id.* § 1832(a)(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).

any property used or intended to be used, in any manner or part, to commit or facilitate a violation of the act.[92]

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.[93] These are the same investigative tools available in other federal criminal prosecutions.[94]

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.[95] 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.[96] 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.[97]

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.[98]

---

[92] 18 U.S.C. § 1834(a).

[93] *Id.* § 2516(1)(a).

[94] *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).

[95] 18 U.S.C. § 1837.

[96] *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.

[97] *Id.* § 1836.

[98] *Id.* § 1838.

VII. PROSECUTION UNDER THE EEA

At the time of the original law review article in 2008, there had been less than sixty prosecutions, mainly Section 1832 prosecutions.[99] Most of these prosecutions were filed in the Northern District of California.[100] In fact, Justice Department statistics confirm that approximately 80% of the eighty six federal judicial districts nationwide have had no EEA prosecutions.[101]

Recently, Peter Toren went back and collected updated statistics for the 16-year period from 1996 to 2012.[102] During this period, the total number of EEA indictments comes to only 124—less than 8 indictments a year on average.[103] The statistics reveal that the number of indictments has remained relatively flat with no dramatic increases since the enactment of the EEA.[104]

It is instructive that the United States recognized—at the birth of the Internet revolution—that the protection of trade secrets was in the economic and national security interest of the United States.[105] But Congress failed to include a private civil cause of action in the original Act based on the same "fears" now being posited by academics today that somehow providing the victims of trade secret theft with access to the federal courts will somehow tip the scales against employee mobility and create a chilling effect on businesses competing in the marketplace.[106] In fact, just the opposite has occurred. Trade secret theft and economic espionage are crippling the U.S. economy and causing the loss of jobs, inhibiting employee mobility, and unfair competition in the marketplace.[107]

The reality is that the EEA as solely a criminal statute has not deterred theft and foreign economic espionage.[108] The Computer Crime and Intellectual Property Section

---

[99] 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).

[100] *See* Computer Crime & Intellectual Property Section, U.S. Dep't of Justice, Trade Secret/Economic Espionage Cases, https://web.archive.org/web/20110228154211/http://www.justice.gov/criminal/cybercrime/ipcases.html#operations (last visited May 24, 2015)(showing that many of the recent U.S. Department of Justice Economic Espionage Act prosecutions are in the Northern District of California).

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

[102] Peter Toren, *A Look At 16 Years of EEA Prosecutions*, LAW 360, http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions (September 19, 2012, 12:18 PM).

[103] *Id.*

[104] *Id.*

[105] 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.").

[106] *See* Levine, *supra* note 77; *see also* Dave Levine, *The Dangers of the New Trade Secret Act*, FREEDOM TO TINKER, https://freedom-to-tinker.com/blog/davelevine/the-dangers-of-the-new-trade-secrets-acts/ (Aug. 27, 2014).

[107] *See generally*, PwC Report, *supra* note 48.

[108] *Trade Secrets: Promoting and Protecting American Innovation, Competitiveness, and Market Access in Foreign Markets, Hearing before the Subcomm. On Courts, Intell. Prop. And the Internet of*

of the United States Department of Justice has done an excellent job, but the burden on the government is too great. Without a federal civil cause of action, U.S. companies simply cannot adequately protect U.S. trade secret assets in a worldwide economy that now crosses international boundaries.

VIII. NO PREEMPTION

The amendments to the EEA proposed in this article should not preempt either the UTSA or the common law. The law of trade secrets has developed over many centuries and should not be displaced.[109] Once again, academics and others have confused this critical jurisdictional issue.[110] The law of trade secrets can be traced back to Roman times.[111] For almost 200 years the law of trade secrets has grown under the common law and in the past 40 years the common law has been captured and refined in UTSA decisions culminating in the Restatement Third of Unfair Competition in 1995 recognizing that the modern-day definition of a trade secret protects any information that can be used in the operation of a business or other enterprise that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.[112]

The uniformity/no-uniformity argument of academics and law professors is a red herring. The modern day cause of action for trade secret misappropriation and the remedies available for trade secret misappropriation are well-defined.[113] The EEA was built upon the UTSA and any suggestion that adding a private civil cause of action to the EEA will undermine or seriously disrupt trade secrets law is simply wrong.

Take for example the decision by the Federal Circuit in Tianrui Group Co. v. ITC.[114] The case involved the misappropriation of Amsted's trade secrets used to manufacture cast steel railway wheels.[115] After a 10-day evidentiary hearing, the ITC found that TianRui, a Chinese company, had hired employees from Amsted's Chinese foundries and misappropriated 128 Amsted trade secrets.[116] The ITC issued a Section 337 limited exclusion order and the Federal Circuit affirmed the ITC.[117]

---

the Judiciary Comm., 113th Cong. at 9 (Jun. 24, 2014)("Since enactment of the Economic Espionage Act, the problem with trade secret theft has grown dramatically.").

[109] 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).

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

[111] *See* Jager, *supra* note 109; *see also* Alan Watson, *Trade Secrets and Roman Law: The Myth Exploded*, 11 TUL. EUR. & CIV. L.F. 19, 20 (1996), *available at* http://digitalcommons.law.uga.edu/fac_artchop/476 (discussing the cause of action for misappropriation of trade secrets in Roman law).

[112] *See generally* Miguel Deutch, *The Property Concept of Trade Secrets In Anglo-American Law: An Ongoing Debate*, 31 U. RICH. L. REV. 313 (1997)(providing historical development of trade secret law up to adoption of the Restatement (Third) of Unfair Competition).

[113] Savor, Inc. v. FMR Corp., 812 A.2d 894, 897 (Del. 2002).

[114] 661 F.3d 1322, 1337 (Fed. Cir. 2011).

[115] *Id.* at 1324.

[116] *Id.* at 1325.

[117] *Id.* at 1326.

During the ITC proceedings, the ITC relied on the Illinois Uniform Trade Secrets Act for the adjudication of the "trade secret" and "misappropriation" claims.[118] On appeal, TianRui argued that state trade secret law should not apply to an ITC section 337 proceeding.[119] In a case of first impression, the Federal Circuit agreed that a single federal standard, rather than the law of a particular state, should determine what constitutes misappropriation of a trade secret sufficient to establish an "unfair method of competition" under section 337. Citing the Restatement Third of Unfair Competition, the Uniform Trade Secrets Act, and the Economic Espionage Act of 1996, the Court readily identified a consonance in the general principles of trade secret law. There was no dispute about the substantive law of trade secrets. The Federal Circuit therefore affirmed the decision by the FTC under the generally recognized law of trade secrets.[120] Once again, the law of trade secrets in the United States is well defined and access to our federal courts will ensure that the modern law of trade secrets grows and thrives in the digital age.[121] The suggestion by some academics that a federal civil cause of action will weaken or destroy U.S. trade secrets law is fallacious.

The UTSA will often be the cause of action of choice where federal jurisdiction is not absolutely necessary.[122] Original jurisdiction is not unusual and original jurisdiction will preserve and build upon the historical and modern developments in U.S. trade secret law. The Lanham Act and the Computer Fraud and Abuse Act are two other federal statutes built upon original not exclusive jurisdiction.[123]

IX. NATIONAL SERVICE OF PROCESS

The federal courts provide for national service of process.[124] 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.[125]

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 with

---

[118] *Id.* at 1328.

[119] *Id.* at 1326-27.

[120] *Tianrui Group Co.*, 661 F.3d at 1327.

[121] *Trade Secrets: Promoting and Protecting American Innovation, Competitiveness, and Market Access in Foreign Markets, Hearing before the Subcomm. On Courts, Intell. Prop. And the Internet of the Judiciary Comm. 113th Cong. at 9* (Jun. 24, 2014) National Association of Manufacturers' Senior Director, Chris Moore, testified that the lack of a civil cause of action for trade secret theft leaves small businesses "without an essential means to deter theft and recover losses," and that "it makes it harder for the United States to lead internationally to improve trade secret protection." *Id.* at 44.

[122] *See* Paul Hanna and Matthew Leal, *The Computer Fraud and Abuse Act: An Attractive but Risky Alternative to Texas Trade Secret Law*, 45 ST. MARY'S L.J. 491, 492-493 (2014)(noting that in 2013, when Texas adopted the UTSA, it joined the 46 other states that had already done so); *see generally*, Sarah Boyer, *Current Issues in Public Policy: Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y. 661 (2009).

[123] 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); 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.").

[124] 28 U.S.C. § 1391 (2006) (providing for national service of process in all civil actions).

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

discovery anywhere in the country.[126] 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.[127] This explains why trade secret litigators are now filing federal Computer Fraud and Abuse Act ("CFAA") claims which establish original subject matter jurisdiction over the CFAA claim and supplemental or pendent jurisdiction of the related state law (UTSA) claims.[128]

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.[129] 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.[130] The whole process can take months with briefings both in the Illinois courts and the California courts.[131]

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.[132] Trade secret cases are time sensitive -- "[a] trade secret once lost is, of course, lost forever."[133] This procedural advantage alone, without more, merits amendments to the EEA.

X. *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.[134] Once

---

[126] *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).

[127] *Id.* at 159-60.

[128] 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).

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

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

[131] 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).

[132] 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).

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

[134] *See* Mark L. Krotoski, *The Time is Ripe for New Federal Civil Trade Secret Law*, BLOOMBERG BUREAU OF NATIONAL AFFAIRS (December 3, 2014), http://www.bna.com/time-ripe-new-

again, in today's environment, trade secrets can be transferred to foreign countries and other parts of the world in seconds.[135] 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.[136] 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.

However, there must be safeguards to protect against any abuse of the statutory provision authorizing ex parte seizure orders. For example, the final House version (H.R. 5233) set forth 7 requirements that must be met for the issuance of an ex parte seizure order as well as the Court issue a written order with required findings of fact, conclusions of law, and a hearing set not later than 7 days after the issuance of the order.[137] The party seeking the order must also post a bond and there are separate provisions for the recovery of damages for excessive or wrongful seizure.[138]

XI. 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.[139] 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[140] 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[141] and (2) wrongful conduct if any acts in furtherance of the offense occurred in the United States.[142]

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.

---

n17179917951/ (noting that both the DTSA and TSPA contain civil ex parte seizure provisions, to eliminate the current "catch me if you can" environment of economic espionage).

[135] *See* WIPO Report, *supra* note 19.

[136] *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).

[137] *See* TSPA, *supra* note 75.

[138] *Id.*

[139] *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).

[140] *Id.* at 761-62.

[141] 18 U.S.C. § 1837(1) (2006); Ballon, *supra* note 139, at 761-62.

[142] 18 U.S.C. § 1837(2); Ballon, *supra* note 139, at 761-62.

XII. UNIFORMITY

There has been much discussion regarding the lack of uniformity in state trade secret laws.[143] 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;[144] what constitutes "misappropriation" is now defined by statute;[145] there is a uniform statute of limitations;[146] statutory standards for injunctive relief;[147] 109 statutory provisions for compensatory damages[148] 110 and so on.[149]

However, there are still some glaring holes and discrepancies.[150] New York, for example, has never enacted the UTSA. Massachusetts has not enacted the UTSA either.[151] There are other state variances requiring U.S. courts to address choice of law questions in most national trade secret cases.[152] 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.[153]

---

[143] *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).

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

[145] *Id.* § 1(2).

[146] *Id.* § 6.

[147] *Id.* § 2.

[148] *Id.* § 3.

[149] *See id.* §§ 1-12.

[150] *See* Pace, *supra* note143, 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).

[151] 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 143, at 443 (noting that New York continues to prefer the Restatement approach to trade secret misappropriation).

[152] *See* Hutter, *supra* note 151, at 6-8; Pace, *supra* note 143, at 443; 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).

[153] 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):

> 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

XIII. 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.[154]

The two most significant examples of this trend are the North American Free Trade Agreement ("NAFTA")[155] 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").[156]

Both NAFTA and the TRIPS Agreement require national standards for trade secret protection.[157] 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.[158] 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? 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 to the EEA. The United States leads the world in research and development. Historically, this has been due to a strong patent system.[159] However, in the Information Age, we also need a strong regime for the protection of trade secret assets. These critical amendments to the EEA will show the world that we are the leader in the protection of these critical intellectual property assets and it will jump-start the rest of the world in moving in the same direction to harmonize the modern law of trade secrets.

> 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 (1996); *see generally* MELVIN F. JAGER, TRADE SECRETS THROUGHOUT THE WORLD (Thomson/West 2007) (detailing the various trade secret rules and laws in effect internationally).

[154] *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 143, 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).

[155] North American Free Trade Agreement, U.S.-Can.-Mex., Dec. 17, 1992, 32 I.L.M. 289 (1993) [hereinafter NAFTA]; Pace, *supra* note 143143, at 450.

[156] 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 143, at 450.

[157] TRIPs, *supra* note 156; NAFTA, *supra* note 155; *see* Pace, *supra* note 143, at 450.

[158] *See* McKenzie, *supra* note 152, at 314; Pace, *supra* note 143, at 443, 451-52.

[159] *See* Chris J. Katopis, *Patients v. Patents?: Policy Implications of Recent Patent Legislation*, 71 ST. JOHN'S L. REV. 329, 329-335 (1997)(discussing the historical policy goals of patent protection and analyzing in light of current health care legislation, stating that the current patent system "encourages innovation and new consumer goods and trade benefits.").

Other countries are also coming to the realization that trade secret assets may, in many instances, be the intellectual property asset of choice in the New Economy.[160] The European Union has studied trade secrets extensively and the studies and surveys show that 75% of respondents in a business survey ranked trade secrets as strategically important to their company's growth, competitiveness and innovative performance.[161]

On November 28 2013, the European Commission (the "Commission") announced a proposal for a Directive on Trade Secrets and Confidential Information which is now making its way through the European Parliament.[162]

Trade secrets and economic espionage are also intertwined in the TPP and TTIP negotiations.[163] The Trans-Pacific Partnership (TPP) is a proposed regional regulatory and investment treaty.[164] As of 2014, twelve countries throughout the Asia-Pacific region have participated in negotiations on the TPP: Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United States and Vietnam.[165] In turn, the Trans-Atlantic Trade and Investment Partnership (TTIP) involves EU-US negotiations.[166] In both negotiations, there have been discussions about protecting trade secrets in computer systems.[167]

These developments demand that the United States step forward and show strong leadership regarding trade secret asset management in the 21st Century. Adopting the proposed EEA amendments will accomplish this role for the United States in these worldwide negotiations immediately.

---

[160] *See Trade Secrets,* EUROPEAN COMMISSION, http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets/index_en.htm (Updated May 22, 2015)(noting that in an economy where information, knowledge, and inventiveness are the raw materials, trade secret protection is beneficial for large companies able to develop large IP portfolios, as well as small companies unable to protect their IP through formal channels).

[161] *Study on Trade Secrets and Confidential Business Information in the Internal Market*, EUROPEAN COMMISSION (April 2013), *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.

[162] *See* Theresa Papademetriou, *European Union: Draft Directive on the Protection of Trade Secrets*, LIBRARY OF CONGRESS (Jun. 12, 2014) http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404026_text.

[163] *See* OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/tpp/outlines-of-TPP [hereinafter TPP Outlines](last visited May 25, 2015); EUROPEAN COMMISSION [hereinafter TTIP Factsheet], http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/contents/ (last visited May 27, 2015).

[164] *See* TPP Outlines, *supra* note 163.

[165] *Id.*

[166] *See* TTIP Factsheet, *supra* note 163.

[167] *Id.*; TPP Outlines, *supra* note 163.

XIV. MORE EFFECTIVE PROTECTION OF TRADE SECRET ASSETS

There were many fears when the EEA was enacted.[168] A major concern was that aggressive business competition would be exposed to EEA criminal indictment.[169] This has not happened.[170] 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.[171] EEA prosecutions have been targeted only to egregious and "open-and-shut" cases.[172] Most indictments involve "offers to sell" or "offers to buy" purloined trade secrets.[173]

---

[168] 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.

[169] 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).

[170] *See* Brenner & Crescenzi, *supra* note 99, at 433 n.184 (noting the number of prosecutions under the EEA is small compared to other intellectual property violations).

[171] 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.

[172] Van Arnam, *supra* note 168, 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).

[173] *See generally* Hosteny, *supra* note 172, 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,

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.[174] Trade secrets thefts are no longer a high priority.[175] The perception exists that these are business crimes that U.S. companies can litigate in the civil courts.[176] 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.[177]

For years, multi-national U.S. corporations have been faced with the dilemma that major trade secret theft cases are within the "prosecutorial discretion" of the Justice Department under the EEA[178] or limited to the vagaries and procedural disadvantages of state court litigation.[179] Neither option is satisfactory.

The two proposed critical amendments to the EEA will change the entire landscape immediately upon passage and President Obama's signature into law. Our foreign adversaries and competitors will no longer be able to raid the cookie jar. The United States will be better able to maintain its competitive and innovation advantages in the worldwide marketplace. U.S. companies will invest in necessary measures to protect trade secret assets because they will now have an effective enforcement and protection in the U.S. courts. Extraterritorial jurisdiction will be exercised to the full extent of the U.S. Constitution. The competitive innovation advantages that the United States enjoys will be better protected by these two EEA amendments. Misappropriators will be caught before further damage can be done. The amendments to the EEA are critical to provide U.S. corporations with the full benefits of the EEA and balance the playing field in multi-national competition.

XV. COMPARISONS TO THE COMPUTER FRAUD AND ABUSE ACT

In 2008, it appeared that the CFAA might become the savior for bringing UTSA trade secret misappropriation actions in state court when there was no diversity of citizenship.[180] Like the EEA, the CFAA is a criminal statute.181 The difference: the

---

supra note 58, at 1-5 (discussing an example of employees misappropriating trade secrets and attempting to sell them on the Internet).

[174] *Hearing before the Subcomm. on Commercial and Admin. Law, Comm. on House Judiciary, 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).

[175] Rustad, *supra* note 4, at 479 n.119. *See* Hosteny, *supra* note 172172, 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.*

[176] Hosteny, *supra* note 172, at 8.

[177] 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).

[178] Hosteny, *supra* note 172, at 10.

[179] McKenzie, *supra* note 152, at 314-15 (noting that state trade secrets laws do not fill the gap that federal laws leave open).

[180] *See* 18 U.S.C. § 1030 (2006).

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

CFAA provides a civil cause of action: "Any person who suffers damage or loss may maintain a civil action against the violator...."[182]

Since most trade secrets now reside in an electronic environment, it was not surprising that there was an upsurge in CFAA actions:[183] Today, "employers...are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."[184]

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."[185] 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.[186]

The seminal decisions in Shurgard Storage Centers, Inc. v. Safeguard Self-Storage, Inc.[187] and International Airport Centers, L.L.C. v. Citrin[188] illustrate the attempt to use of the CFAA to combat trade secret misappropriation and to provide access to the U.S. federal courts.[189]

In Shurgard, employees accessed plaintiff's computer to transmit trade secrets to the new employer.[190] The district court rejected the argument that these employees had authorized access to Shurgard's computer system because they were still employed at Shurgard.[191] 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.[192]

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.[193] Once again, the facts involved a disloyal employee who decided to quit and start up his own competing business.[194] Before he quit, however, Citrin deleted all the

---

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

[183] 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).

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

[185] *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).

[186] 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).

[187] 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[188] 440 F.3d 418 (7th Cir. 2006).

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

[190] *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.*

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

[192] *Id.*

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

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

data that he had collected on potential acquisition targets for the benefit of IAC.[195] The issue was whether such pre-termination activities violated the CFAA because Citrin was authorized to use the laptop computer.[196] 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.[197]

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 misuse.[198] 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.[199]

In addition, there are now splits in the appellate courts regarding the necessary elements to prove up a CFAA violation together and the $5000 jurisdictional requirement.[200] The CFAA is a patchwork of amendments dating back to 1984 and reflect the attempts by the Congress to prohibit Internet computer crimes.[201] In recent years, the CFAA has been under attack for overzealous prosecutions of alleged CFAA violations.[202]

Those who suggest that the CFAA can fill the gap in existing federal law for a federal trade secret cause of action are out of step with judicial decisions and attacks on the CFAA in recent years. 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.

XVI. 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.

---

[195] *Id.*

[196] *Id.* at 420.

[197] *Id.* at 421.

[198] 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).

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

[200] *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I)(2011)(requiring a showing of "a loss to one or more persons during any one-year period aggregating at least $5,000…."); *see also* Jennifer M. Gozdecki, *The Patchwork Application of the Computer Fraud and Abuse Act - CFAA*, NATIONAL LAW REVIEW, http://www.natlawreview.com/article/patchwork-application-computer-fraud-and-abuse-act-cfaa (Aug. 22, 2012)(noting the circuit split in application and construction of provisions in the CFAA).

[201] *See* Gozdecki, *supra* note 200200; *see generally* Ed Hagen, *Prosecuting Computer Crimes,* OFFICE OF LEGAL EDUCATION EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (discussing the implications of Congressional amendments to the CFAA on prosecutors).

[202] *See* Boyer, *supra* note 122.

The primary obstacle is the high burden of proof to obtain a criminal conviction requiring proof beyond a reasonable doubt.[203] 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.[204]

Invocation of the Fifth Amendment privilege against self-incrimination also hampers EEA prosecutions.[205] 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.[206]

Finally, adding a civil cause of action to the EEA will lower the burden of proof standard to the "preponderance of the evidence".[207] 159 This is the same burden of proof standard for UTSA actions in state court.[208] 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.

XVII. CONCLUSION

Preventing cybercrime and protection from would-be trade secret thieves is in the national and economic interest of the United States. This was true in 2008 and it is even more so today. Economic espionage and trade secret thefts compromise American companies and entrepreneurs, result in the loss of jobs and the loss of intellectual property investments, and weaken the American economy both at home and abroad. Two critical EEA amendments are necessary and compelling: (1) a civil cause of action providing federal subject matter jurisdiction for the theft of trade secrets; (2) a civil seizure provision, with appropriate protections and judicial oversight, to prevent the destruction of evidence and the unlawful transfer and loss of trade secrets to other countries outside the United States. After 7 years of vetting these two critical amendments, the time has come for the bicameral introduction and swift passage of the Defend Trade Secrets Act of 2015.

---

[203] 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.

[204] Hosteny, *supra* note 172, 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.

[205] 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 172, at 10.

[206] Bodiford, *supra* note 205, at §22.25.

[207] 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).

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