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.
On October 11, 1996, President Clinton signed The Economic Espionage Act of 1996 (“EEA”) into law. The EEA made theft of trade secrets a federal criminal offense. 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. 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. Senator Kohl and others read the 2008 article and proposed legislation to add a private civil cause of action to the Economic Espionage Act and to add ex parte provisions to the EEA. Various bills have been introduced in Congress in the

\[2\] Id. at sec. 101, 110 Stat. 3489 (codified at 18 U.S.C. § 1832(a) (2006)).
\[5\] 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
The John Marshall Review of Intellectual Property Law

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. Congress recognized that protecting U.S. trade secrets was necessary to "maintain our industrial and economic edge and thus safeguard our national security." 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 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 trade secrets. America leads the nation's [sic] of the world in developing new products and new technologies. Millions of jobs depend on the continuation of the productive minds of Americans, both native born and immigrants who find the freedom here to try new ideas and add to our economic strength."

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. Dept 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] Creativity 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").

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).
8 142 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.").
10 142 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.").
domestic competitors. Without freedom from economic sabotage, our companies lose [sic] their hard-earned advantages and their competitive edge.11

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.12 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.13 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.14 These structural changes have been accompanied by a computer revolution and transition to the Information Age.15 The power of computer technology has increased exponentially, resulting in more powerful means for the theft and transfer of proprietary information.16 The rapid growth of the Internet is a reflection of this boom.17 In fact, the corollary is also true: the Internet is now a tool for the destruction of trade secret assets.18

Computers facilitate the instant copying and transfer of proprietary information surreptitiously.19 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

14 See NIPLECC Report, supra note 4, at 45 (“Protecting IP . . . is crucial to increasing trade and competing in the global economy.”).
15 Brian M. Hoffstadt, The Voyeuristic Hacker, J. INTERNET L., July 2007, at 1, 1 (noting that the computer ushered in the Information Age).
16 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.”).
17 Id. (“Growth in use of the Internet has also offered inviting opportunities for intellectual property crimes.”).
18 Id. (“[T]he Internet has also been used as a vehicle to facilitate the theft of trade secrets.”).
19 Id.
purloined information anywhere in the world within minutes.\textsuperscript{20} The receiving party can do the same thing -- and the cycle can be repeated -- over and over again.\textsuperscript{21} Within days or even hours, a U.S. company can lose complete control over its trade secret assets forever.\textsuperscript{22}

Before the EEA, federal prosecutors relied primarily upon the National Stolen Property Act\textsuperscript{23} and the wire and mail fraud statutes to commence criminal prosecutions for trade secret theft. Both statutes were ineffective.\textsuperscript{24} On the day the EEA was enacted, President Clinton issued the following statement:\textsuperscript{25}

Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation’s national security and economic well-being.

Until today, federal law has not accorded appropriate or adequate protection to trade secrets, making it difficult to prosecute thefts involving this type of information. Law enforcement officials relied instead on antiquated laws that have


\textsuperscript{21} Id. (calling the internet the “world’s biggest copy machine.”).


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.


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.


\textsuperscript{24} See Rustad, supra note 4, at 465-66.

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.

The EEA is a watershed statute, recognizing U.S. national and economic interests in protecting the trade secret assets of U.S. companies. 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. ASIS has conducted seven Trends in Proprietary Information Loss Surveys over the past 17 years. "The resulting reports have been used by U.S. government agencies and private entities." 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.

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. The results confirm that proprietary information losses are continuing and increasing both in the United States and abroad. 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

26 Id.
27 142 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.").
30 Id.
31 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").
32 Id. at 1.
33 Id. at 11 ("Despite measures to ameliorate risk, U.S. companies continue to suffer losses").
respective companies in 2005.34 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.35 The top three foreign countries identified were China, Russia and India.36 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.37 These losses ranged from less than $ 10,000 to more than $ 5.5 million.38

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.39 Other credible sources estimated loss as high as $ 400 billion annually.40

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.41 There is a confluence of factors at work emanating from the digital environment in which we now live and work.42 Advancements in technology,

---

34 Id.
35 Id.
36 Id. at 24 (noting that "China, Russia, and India were identified as the top intended non-U.S. recipients of compromised information").
37 Id. at 3.
38 Id.
39 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.").
increased mobility, globalization and sophisticated cyber-tools and devices all contribute as catalysts for trade secret theft.43

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.”44 National Security Agency Director General Keith Alexander calls cyber-espionage “the greatest transfer of wealth in history.”45 Symantec places the cost of intellectual property theft for the U.S. economy at $250 billion a year.46 McAfee estimates global remediation costs at $1 trillion per year.47 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.48 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.49

IV. FEDERAL PROTECTION OF INTELLECTUAL PROPERTY ASSETS

U.S. law protects patents, copyrights, trademarks and trade secrets.50 There is a civil cause of action under federal law for patent infringement.51 There is a civil cause of action under federal law for copyright infringement.52 There is a civil cause of action under federal law for trademark infringement.53 There is not, however, a civil cause of action under federal law for trade secret misappropriation.54

43 Executive Office Trade Secret Summary, supra note 40 at 20.
The reasons for the step-child treatment of trade secrets are historical. Patents and trademarks are the by-products of the Industrial Revolution. Copyrights date back to the invention of the printing press, if not earlier. 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.

Even though the protection of confidential information dates back to Roman law, and even though the birth of every patent starts out as a trade secret, 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. Shortly thereafter, the Uniform Trade Secrets Act (UTSA) was promulgated by the National Conference of Commissioners on Uniform State Laws in 1979. The stage was now set. In 1984, the United States Supreme Court in Ruckelshaus v. Monsanto held that

55 See Katarzyna A. Czapacka, Antitrust and Trade Secrets: The U.S. and the EU Approach, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 207, 213-14 (2009) (“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 similar 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).


58 Milton E. Babirak, Jr., The Maryland Uniform Trade Secret Act: A Critical Summary of the Act and Case Law, 31 U. BALTIMORE 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 55, at 1142 (discussing trade secret law's evolution into something similar to contract law).


a trade secret asset was a property right protected by the United States Constitution.63

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.64 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.65 U.S. businesses are the victims of trade secret theft and foreign economic espionage.66 U.S. businesses have the fiduciary and statutory obligation to protect trade secret assets;67 finally, U.S. corporations have the financial means and financial incentive to protect trade secret assets.68 The legislative history of the EEA recognizes that

63 467 U.S. 986, 1002 (1984) (stating that a government taking of a trade secrets is governed by the Fifth Amendment).
64 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.

65 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).

66 142 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).

67 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).

68 Czapracka, supra note 55, at 211 (“Trade secrets provide an economic incentive for private investment in knowledge production by giving the means to exclude others from using that
the protection of trade secret assets is in the national interest of the United States. 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.

Trade secret assets are the backbone of an information-based economy. Trade secrets no longer comprise some paper files locked in a file cabinet in technology departments. 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.

Trade secret assets are critical to the competitiveness of companies creating jobs in the United States and abroad. The creation of trade secrets means the creation of jobs; conversely, the loss of trade secret assets means the loss of jobs. 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.

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.
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 these two critical amendments must be enacted to protect U.S. companies and U.S. economic interests. 77

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. 78

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.” This section provides that if a claim of misappropriation is made in bad faith, the court may award reasonable attorney's fees. The courts have 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. 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.

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). 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;"

. "[W]ithout authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;"

. "[R]eceives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization."

79 Id. § 4.
80 Id.
81 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.").
82 See TSPA, supra note 76.
84 18 U.S.C. § 1832(a)(1).
The EEA does not prohibit legitimate means of obtaining information, such as reverse engineering or independent development.\textsuperscript{87} Moreover, the EEA was not 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.\textsuperscript{88}

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.\textsuperscript{89}

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:

[\textit{\textbf{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.\textsuperscript{90}

\textsuperscript{86} 18 U.S.C. § 1832(a)(3).

\textsuperscript{87} See 142 CONG. REC. S12,213 (1996) (Manager's Statement for H.R. 3723, The Economic Espionage Bill) ("[I]f 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."). 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."). \textit{But see James H.A. Pooler, 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)(3)], 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).

\textsuperscript{88} See 142 CONG. REC. S12,213 (1996) (Manager's Statement for H.R. 3723, The Economic Espionage Bill) ("[T]he government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company."); id. at H10,462 (statement of Rep. Schumer) ("[S]ome Members thought that this legislation might inhibit common and acceptable business practices. For example, employees who leave one company to work for another naturally take their general knowledge and experience with them and no one, no one wishes to see them penalized as a result."); see also Tucker, supra note 87, at 1143.

\textsuperscript{89} 18 U.S.C. § 1831(a)(3); id. § 1832(a)(3).

Conspiracies and attempted thefts are also proscribed by the EEA.\textsuperscript{91} The same types of penalties apply with increased penalties imposed if the trade secret misappropriation benefits a foreign government, foreign instrumentality or foreign agent.\textsuperscript{92}

The EEA also provides for forfeiture to the United States of any property constituting or derived from the proceeds of violations of the act and the forfeiture of any property used or intended to be used, in any manner or part, to commit or facilitate a violation of the act.\textsuperscript{93}

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.\textsuperscript{94} These are the same investigative tools available in other federal criminal prosecutions.\textsuperscript{95}

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.\textsuperscript{96} 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.\textsuperscript{97} 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.\textsuperscript{98}

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.

\textsuperscript{91} 18 U.S.C. § 1831(a)(5); id. § 1832(a)(3).
\textsuperscript{92} 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).
\textsuperscript{93} 18 U.S.C. § 1834(a).
\textsuperscript{94} Id. § 2516(1)(a).
\textsuperscript{95} 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).
\textsuperscript{96} 18 U.S.C. § 1837.
\textsuperscript{97} 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.
\textsuperscript{98} Id. § 1836.
required by law or necessary actions by a government entity of the United States, a state or political subdivision or a state.99

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.100 Most of these prosecutions were filed in the Northern District of California.101 In fact, Justice Department statistics confirm that approximately 80% of the eighty six federal judicial districts nationwide have had no EEA prosecutions.102

Recently, Peter Toren went back and collected updated statistics for the 16-year period from 1996 to 2012.103 During this period, the total number of EEA indictments comes to only 124—less than 8 indictments a year on average.104 The statistics reveal that the number of indictments has remained relatively flat with no dramatic increases since the enactment of the EEA.105

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.106 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.107 In fact, just the opposite has occurred. Trade secret theft and economic espionage are

99 Id. § 1838.
100 Susan W. Brenner & Anthony C. Crescenzi, State Sponsored Crime: The Futility of the Economic Espionage Act, 28 HOUS. J. INTL 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).
102 See id. (listing only sixteen different federal circuit courts handling cases involving the EEA).
104 Id.
105 Id.
106 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.”).
crippling the U.S. economy and causing the loss of jobs, inhibiting employee mobility, and unfair competition in the marketplace.108

The reality is that the EEA as solely a criminal statute has not deterred theft and foreign economic espionage.109 The Computer Crime and Intellectual Property Section 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.110 Once again, academics and others have confused this critical jurisdictional issue.111 The law of trade secrets can be traced back to Roman times.112 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.113

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.114 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.115 The case involved the misappropriation of Amsted’s trade secrets used to

---

108 See generally, PwC Report, supra note 49.
110 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).
114 Savor, Inc. v. FMR Corp., 812 A.2d 894, 897 (Del. 2002).
115 661 F.3d 1322, 1337 (Fed. Cir. 2011).
manufacture cast steel railway wheels.116 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.117 The ITC issued a Section 337 limited exclusion order and the Federal Circuit affirmed the ITC.118

During the ITC proceedings, the ITC relied on the Illinois Uniform Trade Secrets Act for the adjudication of the “trade secret” and “misappropriation” claims.119 On appeal, TianRui argued that state trade secret law should not apply to an ITC section 337 proceeding.120 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.121 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.122 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.123 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.124

---

116 Id. at 1324.
117 Id. at 1325.
118 Id. at 1326.
119 Id. at 1328.
120 Id. at 1326-27.
121 Tianrui Group Co., 661 F.3d at 1327.
122 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.
IX. NATIONAL SERVICE OF PROCESS

The federal courts provide for national service of process.125 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.126

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 discovery anywhere in the country.127 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. § 1367.128 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.129

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.130 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.131 The whole process can take months with briefings both in the Illinois courts and the California courts.132

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.133 Trade secret cases are time sensitive -- "[a]
trade secret once lost is, of course, lost forever.” 134 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. 135 Once again, in today’s environment, trade secrets can be transferred to foreign countries and other parts of the world in seconds. 136 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. 137 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. 138 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. 139

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. 140 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 United States Constitution 141 reigning in (1) offenders committing wrongful acts outside


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

135 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-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).

136 See WIPO Report, supra note 20.

137 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).

138 See TSPA, supra note 76.

139 Id.


141 Id. at 761-62.
the United States if they are citizens, permanent resident aliens, or entities organized under the law of the United States142 and (2) wrongful conduct if any acts in furtherance of the offense occurred in the United States.143

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.

XII. UNIFORMITY

There has been much discussion regarding the lack of uniformity in state trade secret laws.144 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;145 what constitutes "misappropriation" is now defined by statute;146 there is a uniform statute of limitations;147 statutory standards for injunctive relief;148 statutory provisions for compensatory damages149 110 and so on.150

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

---

143 18 U.S.C. § 1837(2); Ballon, supra note 140, at 761-62.
146 Id. § 1(2).
147 Id. § 6.
148 Id. § 2.
149 Id. § 3.
150 See id. §§ 1-12.
151 See Pace, supra note144, 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).
152 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 144, at 443 (noting that New York continues to prefer the Restatement approach to trade secret misappropriation).
153 See Hutter, supra note 152, at 6-8; Pace, supra note 144, at 443; Allyson A. McKenzie, United States v. Kai-Lo Hsu: An Examination of the Confidentiality Provision in the Economic
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.

**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.

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

Both NAFTA and the TRIPS Agreement require national standards for trade secret protection. 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

---

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 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).


158 TRIPs, supra note 157; NAFTA, supra note 156; see Pace, supra note 144, at 450.
state trade secrets statute.159 So the prevailing argument in the international community goes something like this: if the United States does not have a federal civil statute to protect trade secrets, why should we be held to a higher standard in our respective countries? 122 This argument is well taken; although the US recognized the important national interest in the protection of trade secret assets with the passage of the EEA in 1996; we are long overdue for the enactment of a federal trade secrets statute. These goals can be accomplished quickly and efficiently by enacting the proposed amendments to the EEA. The United States leads the world in research and development. Historically, this has been due to a strong patent system.160 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.

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.161 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.162

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.163 Trade secrets and economic espionage are also intertwined in the TPP and TTIP negotiations.164 The Trans-Pacific Partnership (TPP) is a proposed regional regulatory and investment treaty.165 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

159 See McKenzie, supra note 153, at 314; Pace, supra note 144, at 443, 451-52.
161 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).
165 See TPP Outlines, supra note 164.
States and Vietnam.\textsuperscript{166} In turn, the Trans-Atlantic Trade and Investment Partnership (TTIP) involves EU-US negotiations.\textsuperscript{167} In both negotiations, there have been discussions about protecting trade secrets in computer systems.\textsuperscript{168}

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.

**XIV. MORE EFFECTIVE PROTECTION OF TRADE SECRET ASSETS**

There were many fears when the EEA was enacted.\textsuperscript{169} A major concern was that aggressive business competition would be exposed to EEA criminal indictment.\textsuperscript{170} This has not happened.\textsuperscript{171} 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.\textsuperscript{172} EEA prosecutions have been

\begin{itemize}
  \item Id.
  \item See TTIP Factsheet, supra note 164.
  \item Id.; TPP Outlines, supra note 164.
  \item Id.
    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.
  \item Id.
  \item 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*, 28 SETON HALL LEGIS J. 239 (2001) (discussing concerns surrounding this legislation).
  \item See Brenner \\ & Crescenzi, supra note 100, at 433 n.184 (noting the number of prosecutions under the EEA is small compared to other intellectual property violations).
    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.
\end{itemize}
targeted only to egregious and "open-and-shut" cases.173 Most indictments involve "offers to sell" or "offers to buy" purloined trade secrets.174

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.175 Trade secrets thefts are no longer a high priority.176 The perception exists that these are business crimes that U.S. companies can litigate in the civil courts.177 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.178

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 EEA179 or limited to the vagaries and procedural disadvantages of state court litigation.180 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

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. 173 Van Arnam, supra note 169, 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).

174 See generally Hosteny, supra note 173, at 10 ("Cases brought thus far under the Economic Espionage Act appear consistent with the notion that egregious criminal activity will be required to justify a prosecution, and that foreign involvement enhances the chances of prosecution. All cases brought thus far comprise incidents of outright bribery and payments for tangible property."); Rowe, supra note 58, at 1-5 (discussing an example of employees misappropriating trade secrets and attempting to sell them on the Internet).

175 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).

176 Rustad, supra note 4, at 479 n.119. See Hosteny, supra note 173173, 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.

177 Hosteny, supra note 173, at 8.


179 Hosteny, supra note 173, at 10.

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. Like the EEA, the CFAA is a criminal statute. The difference: the CFAA provides a civil cause of action: "Any person who suffers damage or loss may maintain a civil action against the violator...."

Since most trade secrets now reside in an electronic environment, it was not surprising that there was an upsurge in CFAA actions. 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." 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." 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.

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

---

182 Id. § 1030(c) (setting forth punishments ranging from a fine to up to 20 years of imprisonment).
183 Id. § 1030(g) (allowing causes of action can be maintained for compensatory damages or equitable relief, such as an injunction).
189 440 F.3d 418 (7th Cir. 2006).
190 Id.; Shurgard, 119 F. Supp. 2d at 1121.
In Shurgard, employees accessed plaintiff's computer to transmit trade secrets to the new employer.\textsuperscript{191} The district court rejected the argument that these employees had authorized access to Shurgard's computer system because they were still employed at Shurgard. \textsuperscript{192} 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.\textsuperscript{193}

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.\textsuperscript{194} Once again, the facts involved a disloyal employee who decided to quit and start up his own competing business.\textsuperscript{195} Before he quit, however, Citrin deleted all the data that he had collected on potential acquisition targets for the benefit of IAC.\textsuperscript{196} The issue was whether such pre-termination activities violated the CFAA because Citrin was authorized to use the laptop computer.\textsuperscript{197} 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.\textsuperscript{198}

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.\textsuperscript{199} 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.\textsuperscript{200}

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.\textsuperscript{201} The CFAA is a patchwork of amendments dating back to 1984 and reflect the attempts by the Congress to prohibit Internet computer crimes.\textsuperscript{202} In

\textsuperscript{191} 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.

\textsuperscript{192} Id. at 1129 (denying defendant's motion to dismiss).

\textsuperscript{193} Id.

\textsuperscript{194} Citrin, 440 F.3d 418.

\textsuperscript{195} Id. at 419. The trade secrets at issue were data collected that identified potential acquisition targets in the real estate industry. Id.

\textsuperscript{196} Id.

\textsuperscript{197} Id. at 420.

\textsuperscript{198} Id. at 421.


\textsuperscript{200} Id. (analyzing the way different courts have interpreted the CFAA).


\textsuperscript{202} See Gozdecki, supra note 201201; 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).
recent years, the CFAA has been under attack for overzealous prosecutions of alleged CFAA violations.203

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.

The primary obstacle is the high burden of proof to obtain a criminal conviction requiring proof beyond a reasonable doubt.204 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.205

Invocation of the Fifth Amendment privilege against self-incrimination also hampers EEA prosecutions.206 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.207

Finally, adding a civil cause of action to the EEA will lower the burden of proof standard to the "preponderance of the evidence".208 This is the same burden of proof standard for UTSA actions in state court.209 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.

---

203 See Boyer, supra note 123.
205 Hosteny, supra note 173, at 9-10; see Rustad, supra note 4, at 458.
206 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.
207 Id.
208 See Bodiford, supra note 206, at §22.25.
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 Trade Secrets Protection Act of 2015.