Statement of

Mark L. Krotoski

Submitted to the

U.S. Senate Judiciary Committee

For the Hearing on

"Protecting Trade Secrets:

The Impact of Trade Secret Theft on American Competitiveness

and Potential Solutions to Remedy This Harm"

December 2, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for focusing on the important issue concerning the protection of trade secrets which impacts national and economic security matters. I appreciate the opportunity to submit this statement and I remain available to assist on any issues or questions that may arise.

I am a partner in the law firm of Morgan, Lewis & Bockius LLP in Silicon Valley, California, and in Washington, D.C. My practice focuses on assisting clients on trade secret, economic espionage, cybersecurity, and antitrust cartel enforcement cases and issues.[1]

For nearly 20 years, I was privileged to serve as a federal prosecutor in the U.S. Department of Justice (DOJ) including leadership positions in the U.S. Attorney's Office for the Northern California and in the Criminal and Antitrust Divisions of the U.S. Department of Justice in Washington, D.C. Since first starting as a Computer Hacking and Intellectual Property (CHIP) prosecutor in the late 1990s, I had the chance to prosecute nearly every type of computer intrusion, computer crime, and intellectual property offense.

In Silicon Valley as a CHIP prosecutor, and later for nearly four years as the National Coordinator of the CHIP Program,[2] I focused on prosecuting foreign economic espionage and trade secret cases and serving as a DOJ leader on litigation and investigative issues under the Economic Espionage Act of 1996 (EEA).[3] Of the eleven foreign economic espionage cases that have been authorized by the DOJ since 1996,[4] I was fortunate to be involved in the successful prosecution of two of those cases. Both cases involved the misappropriation of trade secrets with the intent to benefit the government of the People's Republic of China (PRC). *See* Appendix A (summarizing the eleven foreign economic espionage cases during 1996 through 2015).

The first foreign economic espionage case that I participated in involved the misappropriation of a visual simulation software program trade secret used for training military fighter pilots and the export of a prohibited munitions list item that were brought to the PRC. The case was opened after a trade secret was displayed at a demonstration project at the PRC Naval Research Center in Beijing.[5] Following an extensive investigation, defendant Xiaodong Sheldon Meng was charged with three Section 1831 foreign economic espionage counts involving multiple foreign government entities, including the Thai Air Force, Malaysian Air Force, and various PRC instrumentalities, and other counts.[6] While preparing for a jury trial, defendant Meng ultimately pled guilty to two national security violations: committing foreign economic espionage with the intent to benefit the PRC Navy Research Center and violating the Arms Export Control Act and the International Traffic in Arms Regulations.[7] The case was the second conviction and first sentencing for foreign economic espionage and the first conviction involving "source code" under the Arms Export Control Act.[8]

The second foreign economic espionage case I worked on involved the misappropriation of proprietary insecticide trade secrets and transfer of that information to the PRC and Germany for further development.[9] I served as a member of the prosecution team with two other dedicated federal prosecutors and two FBI agents. The team successfully recovered some trade secrets in Germany through a Mutual Legal Assistance Treaty request for German law enforcement officials to obtain evidence.[10] The investigation revealed that defendant Kexue Huang had traveled to the PRC as a part-time professor at Hunan Normal University, where he directed the

development of the misappropriated trade secrets. The PRC government had granted funding for further research.[11] Following an investigation, Huang was charged with twelve counts of foreign economic espionage and five counts of transportation of stolen property.[12] A few weeks before the scheduled trial, Huang pled guilty to one count of foreign economic espionage under Section 1831 involving Dow AgroSciences' trade secrets in the Southern District of Indiana, and to one count of the theft of Cargill's trade secrets under Section 1832 based on charges filed in the District of Minnesota.[13] Huang was sentenced to 87 months in prison – the highest sentence for a negotiated plea agreement for foreign economic espionage to date.

Other trade secret cases I prosecuted involved cyber espionage of source code which was traced to a hacker outside the United States.[14] I have also successfully handled more traditional trade secret cases.

Based on my experience gained when prosecuting these cases, I led the development of the DOJ's first training on economic espionage and trade secret cases for prosecutors and agents, and served as an instructor on cybersecurity and other law enforcement issues at the DOJ National Advocacy Center. I also served as the primary author to update the Theft of Commercial Trade Secrets chapter in the DOJ Prosecuting Intellectual Property Crimes Manual (Fourth Edition 2013).

Now in the private sector, I counsel clients on trade secret protection and cybersecurity measures, and represent them in trade secret cases. Given my background, I have firsthand experience in prosecuting foreign economic espionage and trade secret cases and in assisting trade secret owners in protecting their trade secrets. I have seen the intersection of criminal and civil cases and the challenges confronted under current law in obtaining adequate remedies under current state trade secret laws. Trade secret theft has also emerged as an important cybersecurity issue. Based on my practitioner's viewpoint, I have concluded that it is important for Congress to strengthen and modernize trade secret law to promote and protect trade secrets in the innovation process.

I. Overview

Because of the tremendous value of trade secrets in our economy, they remain a target for theft and misappropriation. State legislatures first addressed the problem of trade secret theft by enacting state trade secret laws. In 1979, the Uniform Trade Secret Act (UTSA) was first promoted, and then modified in 1985.[15] Currently, 47 states have adopted some form of the UTSA. In 1996, Congress enacted the EEA to authorize federal criminal prosecution of foreign economic espionage and trade secret theft. The EEA was also largely premised on the UTSA.

Many of the technological issues today were not contemplated when the trade secret statutes were first enacted decades ago. No one could conceive that in only a few minutes valuable trade secrets could be emailed or transmitted to other jurisdictions or outside the country. Issues about cyber espionage were not a major concern.

The time has come to modernize and strengthen trade secret laws to address the unique challenges of today. State civil trade secret laws should be reinforced with the option to use a

strong and effective federal civil trade secret statute. Trade secret owners should have a choice on how best to obtain relief. For local trade secret theft, state laws can be effective. Once trade secrets are removed to other jurisdictions, and state laws may be less effective, trade secret owners should be able to rely on federal law to seek relief.

The bipartisan Defend Trade Secrets Act (DTSA) will modernize and strengthen trade secret law and resolve a number of deficiencies under current law. This statement reviews the role of trade secrets to innovation and our economy. The challenges under current law in obtaining meaningful remedies and the benefits of DTSA are noted. Finally, two suggestions are offered for consideration in addressing trade secret reform.

II. Significant Contributions of Trade Secrets to Innovation and the National Economy and Security

A. Many Products and Services in Many Industries

Trade secrets, as one form of intellectual property, serve a unique role in the innovation process and in our economy. Trade secrets can create new products, generate jobs, and lead to new consumer benefits and economic or technological advancements.

Trade secrets touch nearly every industry. Demonstrating the breadth of affected industries, recent cases have addressed trade secrets in industries such as agriculture, airplane parts, automobile, beverage, chemical, construction, executive recruiting, financial institution, fireworks, gas and oil, greeting cards, insurance, medical devices, paint, nutritional supplements, railroad, semiconductor manufacturing, toys, and wind turbine. *See* Appendix B (listing examples).

Trade secrets benefit companies of all sizes, including small businesses, and companies yet to be formed. The EEA has been successfully used to prosecute trade secret misappropriation for all types of businesses and organizations. Trade secrets may be developed by small companies that grow to be very large, which is consistent with the innovation process.

Trade secrets contribute tremendous value for consumers, their owners, employees, an industry and the economy. Consider, for example, the economic impact and many products generated by the Coca Cola formula trade secret or the Google search algorithm trade secret.

The benefits from trade secrets can be considered from macro and micro perspectives. At the macro level, trade secrets serve a fundamental role in advancing our national and economic security. One trade secret can help launch and generate numerous products or a new industry. On a micro level, trade secrets can foster economic growth for a company and generate jobs for its employees.

Trade secrets can take many forms and may include “financial, business, scientific, technical, economic, or engineering information” and can take many forms such as tangible or intangible plans, compilations, formulas, designs, prototypes, methods, techniques, processes, programs, and codes.[16] Trade secret examples from recent civil and criminal cases show a

diverse range of trade secrets such as corn seed information; proprietary organic insecticides; brake pad specifications; Kevlar® technology used for body armor; fiber optic cables; high frequency trading strategy and infrastructure source code; information regarding gas and oil wells, including seismic data, geological maps, and reserves reports; information regarding the design and manufacturing of a disposable pen injector; an epoxy-based intumescent fireproofing material used in paint products; semiconductor manufacturing methods; designs of memory macros for computer chips; algorithm outlining how to implement a solution to compare different vehicles with different name features; design for computer memory chips; and wind turbine technology used to regulate the flow of electricity. *See* Appendix B (listing 35 trade secret examples from civil and criminal cases).

Trade secrets can also impact national security. In business, trade secrets provide a competitive advantage to their owners. When military application trade secrets are stolen, more than the loss of a competitive advantage is at risk. Instead, military or tactical advantages may be foregone. *See* Appendix C (listing examples).

B. The Costs from Trade Secret Theft

With the theft of a trade secret, the thief can reap the benefits of the investment in the trade secret, leap frog over generations of research and development, and destroy the competitive advantages maintained by the confidentiality of the trade secret. The cost of trade secret theft can be considered from both macro and micro perspectives.

On a macro level the cost of trade secret theft has been estimated to be "from one to three percent of the Gross Domestic Product ('GDP') of the United States and other advanced industrial economies."[17] The current U.S. GDP exceeds $18 trillion.[18]

On a micro level, the theft of a single trade secret can adversely impact a company and jobs. Part of the trade secrets' value is based on the investment of time and money in developing them. Many trade secrets represent the culmination of millions of dollars of investment and thousands of hours of research and development. In criminal cases, development costs have been considered as one measure of valuing loss from trade secret misappropriation.[19]

The true costs from trade secret theft remain difficult to measure adequately for a variety of reasons. The loss of the trade secret may be undiscovered for several years, and the loss as a result of the trade secret theft may be unknown or difficult to calculate. The scope of the trade secret loss may not be known. The loss may not be reported by the trade secret owner. Some trade secrets may lack valuation measures since they will launch new products and services.

A few recent civil and criminal individual cases provide examples on the value assigned to trade secrets in the litigation process:

- $275 million loss estimated for the intended theft of trade secrets involving Kevlar® body armor technology from E.I. DuPont de Nemours & Co. with the intent to benefit the defendant company's own product;[20]

- $40 million loss estimated for misappropriating hybrid motor technology from General Motors, with the intent to use said technology in a joint venture with an automotive competitor in China;[21]
- $30.5 million awarded in damages by a jury for misappropriation of computer chip design memory macro trade secrets and breach of nondisclosure agreements;[22]
- More than $20 million loss estimated for misappropriating restricted technology and trade secrets related to the space shuttle program and Delta IV rocket;[23]
- $15.5 million loss estimated for the theft of more than 100 confidential chemical formulas used in the manufacture of silicone-based and rubber products;[24]
- Stipulated value between $7 million and $20 million for misappropriating trade secrets involving proprietary organic insecticides from Dow AgroSciences with the intent to benefit the People's Republic of China and its foreign instrumentalities, and involving novel ingredients and process for a food product from Cargill;[25] and
- More than $1.5 million loss for the theft of Coca-Cola trade secrets involving marketing information and product sample.[26]

C. Forms of Trade Secret Theft and Misappropriation

Because of their tremendous value, trade secrets are the target of theft and cyber espionage. Trade secret owners confront both internal and external threats.

A common scenario involves an insider who has trusted access to valuable trade secrets and other confidential information and decides to steal them for his own benefit or for the benefit of others. The motives for this insider theft can vary. Some employees after years of service may become disgruntled. Some may be enticed to a new position with a competitor. Some may decide to start a new company using the stolen trade secrets and other information. Regardless of the circumstances, the trade secret owner is often surprised by the theft and typically feels betrayed.

An emerging area of concern involves cyber espionage. Recent developments confirm how these external cyber attacks present a serious threat to obtain trade secrets and other information. Cyber espionage may be directed by state actors or committed by hackers and organized groups focused on obtaining trade secrets and other information of value. A few cyber espionage examples are noted in reverse chronological order:

- On April 1, 2015, as part of an effort to develop new tools to address this problem, the White House issued an Executive Order declaring that cyber espionage has become a "national emergency." The Executive Order authorizes the sanctions in appropriate cases against individuals and entities engaged in "malicious cyber-enabled activities," including for "causing a significant misappropriation of … trade secrets."[27]

- In December 2014, the FBI announced that it had attributed recent cyber attacks on Sony Pictures Entertainment to the North Korean government.[28] While this case did not involve trade secrets, it highlights the concerns raised by cyber espionage committed by state actors.

- In September 2014, an "international hacking ring" was indicted for stealing "trade secret data used in high-tech American products, ranging from software that trains U.S. soldiers to fly Apache helicopters to Xbox games that entertain millions around the world," Assistant Attorney General Leslie Caldwell announced.[29]

- In May 2014, five members of the Chinese military were charged with computer hacking, foreign economic espionage, and several other offenses in targeting six companies in the U.S. nuclear power, metals and solar products industries.[30]

- In May 2009, in a case I prosecuted, a hacker from Sweden was indicted for hacking and copying source code of a leading network equipment provider and for hacking into National Aeronautics and Space Administration. Because there was no extradition treaty with the Kingdom of Sweden, the case was transferred for final prosecution to Sweden.[31]

- Other reports have traced state-sponsored hacking and the misappropriation of intellectual property to Chinese and Russian government groups.[32]

III. Trade Secret Remedy Options Under Current Law

Since 1996, federal law only provides for the prosecution of criminal trade secret theft under the EEA. Consequently, the civil remedy for trade secret theft is based on local state laws.

Under current law, generally there are three avenues to seek remedies for trade secret theft:

(A) Persuade the U.S. Department of Justice to investigate and prosecute a federal criminal case under the EEA;
(B) File a civil case in state court; or
(C) Try to establish federal jurisdiction based on either (a) diversity of citizenship jurisdiction relying on state legal theories, or (b) federal question jurisdiction by piggybacking the case onto another federal statute.

Each avenue presents challenges and limitations. On the first avenue, realistically, only a few trade secret cases qualify for federal criminal prosecution under the EEA. Not many trade secret cases are prosecuted by state prosecutors, and some penalties for state trade secret violations are relatively modest.

On the second course, state law may be effective at addressing local harms, but is less adept in redressing national or international theft of trade secret cases. Finally, efforts to stretch a trade secret case to satisfy current federal jurisdiction standards under other statutes often results in a poor fit for the case. These complications interfere with the ability for trade secret owners to obtain meaningful remedies under current law.

A. The Intersection of Criminal or Civil Remedies

As a federal prosecutor handling a variety of trade secret cases under the EEA, I was often asked to decide whether to open a trade secret case. I was able to see firsthand the intersection of criminal and civil trade secret remedies.

In deciding whether a trade secret case may be prosecuted as a criminal case under the EEA, prosecutors apply certain relevant "discretionary factors" under the U.S. Attorney's Manual. These factors include:

- the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality;
- the degree of economic injury to the trade secret owner;
- the type of trade secret misappropriated [i.e., did it involve sensitive technology or implicate national security];
- the effectiveness of available civil remedies;[33] and
- the potential deterrent value of the prosecution.[34]

Other relevant factors may include:

- What was the manner of the misappropriation (e.g., criminal circumstances of theft, substantial planning and preparation for the misappropriation, or fraud)?
- Was the misappropriated trade secret used or what specific plans were made to use it?
- What steps were taken to disclose the trade secret to a foreign government or competitor?
- What evidence establishes the elements of the offense including criminal intent?
- What steps were taken for the trade secrets to leave the jurisdiction or country?

Under these factors, the U.S. Department of Justice has successfully prosecuted several significant foreign economic espionage and trade secret cases through the years.

As a practical matter, however, only a handful of trade secret theft cases will result in federal criminal prosecution. One key issue in all cases, including trade secret cases, is evidence to prove criminal intent. Even where the foregoing factors are met, the case may be declined for other reasons such as insufficient investigative resources. The criminal trade secret cases can be labor intensive depending on the circumstances. Some cases may take a few years to investigate and prosecute.

Apart from federal criminal prosecution, a few states have criminal statutes for the misappropriation of trade secrets. Some of the penalties, are generally modest.[35] The ability to bring state criminal trade secret cases is also a function of limited resources. State prosecutors are challenged when it comes to prosecuting international trade secret theft cases given limited resources and other limitations.

When trade secret cases were declined for criminal prosecution, the trade secret owner is left with civil remedies. On a number of occasions, the trade secret owners described their

concerns about whether they could obtain meaningful relief based on state law particularly for cases where the trade secrets were misappropriated to other states or outside the United States.

For me, these cases demonstrated the need for meaningful federal civil remedies to protect trade secrets. From my perspective, if the federal government declined criminal prosecution for appropriate reasons, policies to encourage intellectual property in the form of trade secrets are undermined if trade secret owners are unable to obtain effective relief.

B. Cumbersome and Costly State Law Process When Trade Secrets Are Transferred To Other Jurisdictions

State law may be useful for local misappropriation cases. As an example, if an employee steals an employer's trade secrets and brings them to a competitor across town or in another part of the same state, the same state judicial process and rules can be used to consider the misappropriation.

However, efforts to obtain remedies for the stolen trade secrets taken to other jurisdictions under state law can be cumbersome, costly and ineffective. Once trade secrets are stolen and removed to another state or outside the country, the legal options generally become more costly and complicated. The mere act of obtaining a deposition of a witness in another state can require multiple court orders and unacceptable delays.[36] Multiple court systems may also be necessary to subpoena records.

Instead, federal jurisdiction offers nationwide subpoena service power.[37] The ability to obtain one federal court order or issue one federal subpoena results in less delay and typically less cost than seeking the same or similar records or process through multiple state court systems. The cumbersome process and delays for interstate trade secret theft in state cases can serve as a significant disincentive to use an overburdened state court system.

C. Limited Options for Federal Court Jurisdiction

In order to seek relief, and avoid state court delays and challenges, trade secret owners may try to vindicate their rights in federal court. Although successful trade secret cases have been brought in federal court, obtaining federal jurisdiction is not always possible or a natural fit for the facts of the case. Current law provides two primary paths for federal court jurisdiction: (1) diversity jurisdiction or (2) federal question jurisdiction.[38]

Diversity of Citizenship jurisdiction is available in limited circumstances where the "matter in controversy" exceeds $75,000 and there is diversity of citizenship among the parties. This requires that the parties be from different states or involve a state citizen and non-citizen.[39] If diversity of citizenship is established, the federal court applies state law. This is the same state law that the state court would apply.

Diversity jurisdiction is not always available. It is nonexistent when the parties are from the same state even if the trade secret was removed to another state or outside the country. Even in those circumstances where diversity jurisdiction can be met, since the federal legislation

provides for greater protections of trade secrets than state law, trade secret owners will likely prefer the federal law. As noted in Section V(E), enhanced protections under the federal legislation include stronger protective order measures, a five-year statute of limitations, a broader definition of trade secrets, and an extraterritorial provision which applies to conduct outside the United States.

Where diversity jurisdiction is unavailable, trade secret owners may seek federal question (or subject matter) jurisdiction by using another federal statute.[40] In some cases, the Computer Fraud and Abuse Act (CFAA), may be an option.[41] However, there are two significant restrictions. First, the CFAA does not apply where a computer was used and its other statutory requirements are not met. Second, even if a computer was used (for example to download or transfer the misappropriated trade secret), there is a significant circuit split on whether an insider or employee acting with the intent to steal the company's trade secrets and information with the company's computer violates the CFAA.[42] Until this division among the courts is addressed, whether the CFAA may be used depends on which jurisdiction the misappropriation occurred.

Other federal statutes may be considered for federal question jurisdiction. However, the state trade secret claim would be considered under pendant or supplemental jurisdiction.[43] State law will still govern the trade secret misappropriation claim. The state trade secret claim may be weaker than the federal legislation, which fails to provide the most effective remedies and protection for trade secrets. Further, federal jurisdiction will be based on another statute (such as a trademark violation) that likely is not the primary basis for filing the case. Stretching the case as a means to enable jurisdiction often does not best fit the core facts of the case. The federal statute used for jurisdiction becomes the tail wagging the proverbial dog to obtain federal court review of the dispute. As with diversity jurisdiction, a federal trade secret statute, if enacted, would be preferable since it would provide more protections to trade secrets than current state law, as noted in Section V(E).

Consequently, because few trade secret cases rise to the level of a federal criminal prosecution, current law is dependent on state trade secret laws. Unless the trade secret theft is a local matter, state law is not effective to remedy trade secret theft in cases where the trade secrets are removed to other jurisdictions.

IV. Other Challenges in Obtaining Meaningful Remedies

Policies to encourage and promote trade secrets are undermined by an inability to obtain meaningful remedies resulting from the theft of trade secrets. When the entrepreneurial risks in time, effort, and money can be stolen without an effective remedy, innovation becomes stifled. The risks for innovation should be worth the unrealized reward.

There are a number of unique challenges in finding sufficient remedies for trade secret theft. In cases I have handled, certain challenges commonly arise in investigating and litigating trade secret theft cases. These challenges include:

(1) The "misappropriation gap" advantage that a trade secret thief has in planning and stealing the trade secrets until the full scope of misappropriation is discovered;

(2) The ease by which trade secrets can be transferred or transported to other jurisdictions in our global economy; and

(3) The need to narrow the "recovery gap," which is the time to recover the trade secrets after their misappropriation is discovered, and maintain the competitive advantage from the trade secrets for the owner and prevent their use and copying.

A. Overcoming the "Misappropriation Gap" Advantage During the Planning, Theft and Discovery Stages

Today trade secret thieves benefit from a "catch me if you can" environment. Under a risk-reward analysis, there is tremendous potential reward that can result from stealing trade secrets, measured against a lower risk of getting caught, recovery of the stolen trade secrets, and being held accountable in either a civil or criminal case. Recovery becomes more difficult in our legal system if the trade secrets are removed and transferred to other states or outside the United States. State law can be effective in addressing local misappropriation, but is less effective in dealing with the misappropriation of trade secrets to other jurisdictions or outside the United States.

Many trade secret cases involve what I have characterized in my cases as a "misappropriation gap." This gap describes the time between the planning, preparation and actual theft of the trade secrets to the time of the discovery of the theft. The significance of this gap is that the trade secret thief maintains an advantage at this stage until full discovery of the theft. The reality is that it can take anywhere from a few months to a few years to learn about, investigate and uncover the full scope and manner of the misappropriation.

Significantly, the "misappropriation gap" advantage that the thief has often extends beyond the initial discovery. Often the full scope of the theft, including the number of stolen trade secrets, will not be known for a substantial amount of time.

The reality is that trade secret theft is often a highly reactive event for the trade secret owner.[44] The owner is usually surprised and caught off guard by the theft.

In trade secret cases, it is essential to uncover this "misappropriation gap" to learn about the scope of the trade secret theft. The sooner the misappropriation is discovered, the greater the chance to prevent loss of the trade secret including investments in research and development, and stop the use and copying of the trade secret.

Given the challenge of the "misappropriation gap," based on my experience handling a variety of trade secret cases, the law needs to provide effective tools that promote the prompt seizure and recovery of trade secrets.

B. Ease of Misappropriating Trade Secrets to Other Jurisdictions

Today, our economy relies on information and technology in new ways that were unforeseeable when either the EEA was first enacted nearly 20 years ago, or the UTSA was adopted more than 35 years ago.

The ability to quickly transfer trade secrets to other jurisdictions has increased.[45] In today's global economy, within hours or a few days of the initial theft, the trade secret can be transferred or transported to other states or other countries. Once the secret is disclosed, the competitive value of the trade secret dissipates. The stolen trade secrets may never be recovered.

A common means to transfer and misappropriate trade secrets is by email. Consider a few case examples:

- After a defendant informed his employer "that he was going to remain with the company," on the next day he "emailed a Microsoft Word document to his PKU [Peking University, College of Engineering, Department of Nanotechnology] email account which contained, embedded on the second page of an unrelated document, the protected chemical process."[46]
- Defendants were convicted for obtaining cell phone photographs of trade secret information and emailing the photographs to others.[47]
- Trade secrets have been transmitted by email including to others outside the United States.[48]

These are only a few examples but they demonstrate how quickly trade secrets can be removed from one jurisdiction and transmitted around the world. Given these challenges, the trade secret law should be modernized to address these electronic realities.

C. Narrowing the "Recovery Gap"

In addition to the "misappropriation gap," which provides the trade secret thief with a substantial advantage until full discovery of the misappropriation, another important gap in these cases involves what is best described as the "recovery gap" which concerns the amount of time it may take to recover stolen trade secrets after discovery.

Time is certainly of the essence when it comes to recovering stolen trade secrets. Normally there is a small window of opportunity to recover stolen trade secrets. The best time to recover trade secrets is as close in time to the actual theft.

In each trade secret misappropriation case, one of the first requests and highest priorities of the trade secret owner is to recover the stolen trade secrets and prevent any copying or use. Often the stolen trade secrets can never be recovered. Current law lacks an effective mechanism to provide for the prompt trade secret recovery.

Any remedy that fails to address the "recovery gap" may fall short of meaningful relief. In criminal cases, search warrants can be used to seize trade secrets if their location can be identified. In civil cases, an appropriate mechanism with judicial oversight is needed to protect and recover trade secrets.

V. Modernizing and Strengthening Trade Secret Law and Establishing Effective Trade Secret Remedies

The bipartisan Defend Trade Secrets Act (DTSA) will modernize and strengthen trade secret law and resolve a number of deficiencies under current law. The legislation (S. 1890 and H.R. 3326) has been introduced by Senators Orrin Hatch (R-UT) and Chris Coons (D-DE) and Representatives Doug Collins (R-GA) and Jerrold Nadler (D-NY).

Based on the increasing importance of trade secrets to our economy, the legislation will help implement the original EEA objectives to promote national and economic security.[49] The legislation strengthens and modernizes trade secret law in a number of respects, noted below:

A. New Federal Private Right of Action

For the first time the legislation establishes a federal civil private right of action for trade secret misappropriation. Today, the only basis for a civil remedy of the misappropriation of trade secrets is under state and not federal law. While many states have adopted some version of UTSA, there are modifications and variations.

In limited circumstances, federal courts may apply state trade secret law where jurisdiction is based on diversity of citizenship, as noted in Section III(C). Under this jurisdiction, the federal court is applying state and not federal trade secret law. However, diversity jurisdiction is not available where the parties are from the same state, even if the trade secret has already been removed to another state or outside the country. DTSA would establish federal trade secret law. Under DTSA, trade secret owners would have a choice of seeking relief in either federal or state court where the jurisdictional requirements are met.

A federal private right of action will provide trade secret owners with meaningful remedies, particularly where trade secrets are removed from the original location and taken out of the state.

B. Filling a Gap in Federal Intellectual Property Law

The legislation fills a gap in current law by ensuring a federal private cause of action is available for all four intellectual property forms. Under current law, federal courts can hear claims of infringement in copyright,[50] trademark,[51] and patent cases.[52] However, civil trade secret misappropriation is based only on state law civil remedies.[53] Given the importance of trade secrets as intellectual property and to the role of innovation, there is no policy reason why trade secrets should not have similar federal protection. Federal law should encourage and promote the development of trade secrets just as it fosters other forms of intellectual property development.

Each type of intellectual property advances distinct objectives. Trade secret law protects information which provides a commercial advantage to its owner. Copyright law protects original creative works of authorship which may include computer software, motion pictures and sound recordings, and literary, musical, dramatic, choreographic, architectural, pictorial, graphic, and sculptural works.[54] Trademark law protects “any word, name, symbol, or device, or any

combination thereof" that identifies and distinguishes the source of goods.[55] Patent law protects inventions that are publicly filed and provides a "right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States."[56]

The different intellectual property forms can be interrelated. Trade secrets often serve as a precursor to patents. After initial development, the trade secret owner may decide to obtain protection under patent law by publicly filing the invention.

One trade secret may lead to other forms of intellectual property protection for related products. Consider for example the many products generated by the original Coca-Cola trade secret formula.[57] The words ("Coca-Cola"® and "Coke" ®),[58] logo,[59] and bottle design have received trademark protection.[60] Design patents have also been issued on the bottle shape.[61] Songs promoting the products, and advertising have copyright protection. These examples illustrate how one innovation can result in multiple forms of intellectual property protection.

Claims for the infringement of other forms of intellectual property, including copyrights, trademarks, and patents, are heard in federal court. There is no reason why this same option should not be extended to trade secrets as one of four intellectual property rights. National policy should encourage the development of all forms of intellectual property.

C. Reasonable, Balanced Mechanism to Recover Misappropriated Trade Secrets

The legislation addresses the "recovery gap" problem involving the need to promptly recover trade secrets and prevent any copying or use. The best time for recovery is as close in time to the theft. Prompt recovery minimizes the risk of unauthorized copying and use of the stolen trade secret.

Under the legislation, a federal court, under limited circumstances, can order the seizure of the trade secrets, bring them within the jurisdiction of the court, and hold a hearing to determine the appropriate response. The legislation is effective, reasonable and balanced in its approach and includes a number of safeguards to prevent potential abuse.

The legislation would provide a federal court the authority to issue a short-term, ex parte civil seizure order, upon a sufficient showing, to seize allegedly stolen trade secrets and prevent their transfer. A full hearing would be held within seven days with all parties. This part of the legislation contains a number of safeguards to balance the need for immediate action against the potential harm to a defendant.

The following six requirements ensure that the ex parte seizure order is limited to appropriate circumstances:

First, in seeking relief, the applicant must make a proper showing based on an affidavit or verified complaint.[62] Specifically, the applicant must allege "specific facts" that demonstrate (1) a temporary restraining order under Rule 65 would be inadequate "because the party to which the

order would be issued would evade, avoid, or otherwise not comply with such an order;" (2) an "immediate and irreparable injury will occur" in the absence of seizure; (3) the harm in denying relief outweighs any harm to others; (4) the applicant is likely to succeed in showing the information is a trade secret and the person who is the subject of the order misappropriate or conspired to misappropriate the trade secret; (5) the matter to be seized is described with "reasonable particularity" and the location is identified; (6) the person subject to the order "would destroy, move, hide, or otherwise make such matter inaccessible to the court" if notice were provided; and (7) the requested seizure has not been publicized by the applicant.[63] Under this threshold step, no seizure order will issue absent a sufficient showing.

Second, in considering the application, the court must make certain findings and conclusions before issuing a seizure order. The seizure order shall (1) set forth findings of fact and conclusions of law required for the order; (2) provide for the "narrowest seizure of property" in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate, unrelated business operations of the person accused of misappropriating the trade secret; (3) be accompanied by an order protecting the seized property from disclosure by restricting the access of the applicant and prohibiting any copies of the seized property; (4) set a prompt hearing within seven days after the order has issued; and (5) require the applicant to provide the security determined adequate by the court for payment of such damages as a person may be entitled to recover as a result of a wrongful or excessive seizure.[64] No seizure order will issue absent the required court findings are not made. Also, if the applicant cannot post the required security, the order will not issue.

Third, a neutral law enforcement official serves the seizure order and the "submissions of the applicant to obtain the order."[65] This ensures that an experienced and unbiased professional executes the court's order. By comparison, under current law a temporary restraining order may be served by an attorney or agent of a party, who may hold an interest in the outcome.

Fourth, any materials seized are retained into the custody of the court.[66] The court is required to secure the material from physical and electronic access.[67] Additionally, the court may take protective steps to verify that any electronic medium containing the trade secret is not "connected to an electronic network or the Internet without the consent of both parties, until the hearing" with all parties present. The seized material remains secure within federal court control.

Fifth, the court must hold a seizure hearing within seven days.[68] At the hearing, the court can consider the arguments from the parties. If the applicant is unable to meet its burden to establish sufficient facts to support the order, "the seizure order shall be dissolved or modified appropriately."[69]

Sixth, the legislation includes various safeguards against an improper ex parte seizure order. A motion to dissolve or modify the seizure order may be filed "at any time" by "any person harmed by the order."[70] A person who suffers damage as a result of a wrongful or excessive seizure may bring a cause of action against the applicant to recover damages including punitive damages and a reasonable attorney's fee.[71] These statutory sanctions are in addition to general sanctions that the court may issue under Federal Rule of Civil Procedure 11.[72] For any

claim of misappropriation that is made in bad faith, the court may award reasonable attorney's fees.[73]

This balanced approach provides a new necessary tool to overcome the "misappropriation gap" and narrow the "recovery gap." The provision increases the chances that trade secrets may be seized by a law enforcement official and maintained in the custody of the court pending a hearing involving all parties. The safeguards protect against potential abuse and provide the court with a variety of options to address any abuse. Because the recovery of trade secrets, particularly before any use or copying, may be the most important step following any misappropriation, the legislation enhances the chance for meaningful remedies.

D. Tools to Address Digital Era Issues

The legislation includes new provisions that recognize the realities of trade secret theft in the digital era. For example, the court can "secure the seized material from physical and electronic access during the seizure and while in the custody of the court."[74] For information on an "electronic storage medium," the court can protect the seized material by "prohibiting the medium from being connected to an electronic network or the Internet without the consent of both parties, until the hearing."[75] A party can request that any seized materials be encrypted.[76]

These provisions will help modernize trade secret law. Courts will be empowered to take appropriate steps to safeguard trade secrets during the litigation process.

E. Drawing Upon Meaningful Experience and Adopting Proven EEA Standards

Another benefit of the legislation is that it amends the current EEA statute by adding provisions for a civil remedy. In doing so, the legislation adopts and draws upon some of the stronger and effective standards that have been used in federal criminal cases. By amending the existing EEA, the legislation benefits from the practice and experience of a statute that has been used effectively for criminal cases. Some of these benefits include: (a) fostering employee mobility while prohibiting trade secret misappropriation; (2) using stronger standards to protect trade secrets during litigation; (3) using the broader definition of trade secrets covering intangible information; and (4) applying the extraterritorial provision.

A number of states which have adopted versions of the UTSA have also added criminal remedies as part of their trade secret laws.[77]

1. Prohibiting Trade Secret Misappropriation While Fostering Employee Mobility

In amending the EEA to add the civil provisions, the legislation draws upon existing federal standards to promote employee mobility. For nearly 20 years the EEA has prohibited the misappropriation of a trade secret yet permitted the use of "general knowledge and skills developed while employed."[78] In this manner, the EEA does not restrict employee movement; it only bars trade secret misappropriation.

During the House EEA debate 19 years ago, then-Representative Charles E. Schumer specifically addressed this issue:

> [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.[79]

During the Senate debate, Senator Herb Kohl also clarified:

> [T]rade secrets are carefully defined so that the general knowledge and experience that a person gains from working at a job is not covered.
>
> Mr. President, we do not want this law used to stifle the free flow of information or of people from job to job. But we built in a number of safeguards to prevent exactly these problems. They are elaborated on in the managers' statement and our committee reports.[80]

The Managers' Statement further added:

> This legislation does not in any way prohibit companies, manufacturers, or inventors from using their skills, knowledge and experience to solve a problem or invent a product that they know someone else is also working on. Thus, parallel development of a trade secret cannot and should not constitute a violation of this statute.
>
> …
>
> In addition, a prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated. It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was merely exposed to a trade secret while employed. A prosecution that attempts to tie skill and experience to a particular trade secret should not succeed unless it can show that the particular material was stolen or misappropriated. Thus, the 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. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior.[81]

This distinction was further made in defining a trade secret:

> In the course of reconciling the Senate and House versions of this legislation, we eliminated the portion of the definition of trade secret that indicated that general knowledge, skills and experience were not included in the meaning of that term. Its elimination from the statutory language does not mean that general knowledge can be a trade secret. Rather, we believed that the definition of trade secrets in itself cannot

include general knowledge. Thus, it was unnecessary and redundant to both define what does and what does not constitute a trade secret.[82]

By amending the EEA, the legislation adopts and incorporates this line which bars trade secret misappropriation yet allows employees to use their general skill and knowledge.

2. Stronger Standards to Protect Trade Secrets During Litigation

Because the value and competitive advantages of a trade secret can be lost upon disclosure, it is essential to preserve the confidentiality of trade secrets during litigation. EEA Section 1835 contains effective standards to protect trade secrets during the litigation process. This provision has successfully safeguarded a wide variety of trade secrets and is stronger than comparable provisions under the UTSA or state law.

The UTSA recognizes that a court may issue a protective order.[83] However, the UTSA fails to address the situation in which a trial court orders the disclosure of trade secret information. This remains as an occasional risk during litigation process.

The EEA contains a stronger mechanism to safeguard trade secrets during litigation. EEA Section 1835 allows for an interlocutory appeal for review of an adverse disclosure ruling.[84] Without this statutory protection, an adverse ruling may not be appealable until after the conclusion of the entire case.[85] The legislation addresses this deficiency by using the stronger EEA protective order provision in civil cases.

Based on my experience prosecuting EEA cases, and in working closely with other prosecutors on EEA issues, the federal protective order provision has worked well to safeguard a wide variety of trade secrets. Since the EEA was enacted 19 years ago, only twice has an interlocutory appeal been sought under Section 1835. Both times the appellate court agreed with the government on the need to safeguard the trade secrets.[86] These cases demonstrate the importance of the shadow of potential and immediate appellate review. The legislation extends this protection to civil cases.

3. Broader Descriptive Definition of Trade Secrets Covering Intangible Information

The legislation uses the more descriptive and broader definition of trade secret information under the EEA.[87] In this manner, stronger protection is provided to trade secrets than under state law.

The trade secret definition under the EEA is based on the UTSA.[88] However, the EEA definition is broader than the UTSA in two areas. First, the federal definition is more descriptive in terms of what is covered. Second, the federal definition expressly applies to intangible information. In construing a statute, courts first consider the plain meaning of the statutory language to determine legislative intent.[89]

Under the UTSA, a "trade secret" is defined as "information, including a formula, pattern, compilation, program, device, method, technique, or process."[90] In contrast, the broader federal definition applies expressly to "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[91] In 1996, Congress intended the federal definition to be broadly applied.[92]

One of the objectives of the EEA was "to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished." [93] Congress explicitly included intangible information in the definition of a trade secret. Consequently, the legislation provides stronger protection for trade secrets than under state law based on UTSA.

4. Extraterritorial Provision

In our global economy, many trade secrets are taken outside the United States. The EEA includes a specific extraterritorial provision which extends to the misappropriation of trade secrets outside the country.[94] By amending the current EEA, the legislation applies the extraterritorial provision to civil cases.

Because the UTSA does not include an extraterritorial provision, the general presumption against coverage of extraterritorial conduct applies in UTSA cases.[95] Federal law can best address this situation.

F. Longer Statute of Limitations

The legislation would establish a five year statute of limitations, which is longer than the three year statute of limitations under the UTSA[96] that is used by many states.

As noted, trade secret cases are often highly reactive. The period of the "misappropriation gap," measuring the time of the planning and theft to discovery, can vary significantly. The trade secret owner may not discover the theft until the trade secret has been removed to another jurisdiction.

Even after discovery, the scope and nature of the misappropriation may remain unknown for some time. It is not uncommon for more trade secrets to have been stolen than initially realized. In some cases, it is not possible to determine how the trade secrets were stolen. The longer statute of limitations period recognizes these realities, provides a more realistic amount of time to seek relief, and increases opportunities to obtain meaningful relief.

G. Non-Preemption of State Remedies

The legislation does not preempt state law remedies. It therefore promotes remedies for trade secret theft by giving trade secret owners a choice to rely on either state or federal law as appropriate under the circumstances. The non-preemption also promotes greater deterrence

because trade secret owners can best decide whether relief is more appropriate in federal or state court. Trade secret thieves will risk the broader reach of federal law when trade secrets are removed to other jurisdictions. This approach is consistent with EEA Section 1838 which provides that the statute does not "preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret."[97]

Under our federal system, the dual option for state or federal remedies is common. For policy reasons, each jurisdiction may vindicate its interests. In other circumstances, federal and state law may overlap and reinforce common policies. For example, the Uniform Securities Act (USA) is used as a model for state securities law to cover "fraudulent activity … at a level that eludes the applicability of federal law and, even when federal law applies, eludes the capacity of federal enforcement. Without state regulation accompanied by civil and criminal enforcement of the law in state courts, there would be no hope of redress for many victimized investors."[98]

As another example, a federal statute prohibiting age discrimination,[99] is supplemented by many state age discrimination statutes. Similarly, while most crimes are local, there is a benefit to allow prosecution of fraud at both the local and federal levels. As another example, many states have enacted laws prohibiting computer intrusions or unauthorized access to computers,[100] which supplements the Computer Fraud and Abuse Act which has both civil and criminal remedies.[101]

There may be a variety of reasons that a trade secret owner may select a federal or state forum. The owner may conclude that a local misappropriation is appropriate for resolution in state court. However, if the trade secret leaves the local jurisdiction, the trade secret owner may decide that a federal court provides a more effective chance to pursue relief. The owner may conclude that a remedy may be quicker in federal court particularly where many state courts are suffering from substantial civil case delays. The owner may conclude that litigation and other costs may be lower in federal court.

VI. Responding to Some Recent Questions About the Legislation

Some questions about the legislation have been raised. In reviewing the responses to these questions, in my view the benefits of the legislation are reinforced.

A. Promoting Litigation and Other Costs Savings

Some critics have suggested that a federal cause of action for trade secret misappropriation will adversely increase the length and cost of trade secret litigation. On the contrary, the legislation will result in significant cost reductions in a number of key respects and provide more options to reduce costs in trade secret cases. First, on those occasions in which the ex parte seizure order results in the recovery of stolen trade secrets, the cost savings will be tremendous. The timely recovery of the trade secrets will salvage the original investment in research and development of the trade secrets. It will also avoid the unauthorized copying and use of the trade secrets by others. This mechanism will minimize the costs and losses caused by

trade secret misappropriations and will address one of the paramount concerns of trade secret owners when their trade secrets are stolen.

Current law lacks this option. The inability to recover the stolen trade secrets in state court means the trade secrets may be used by others. Without the recovery of the stolen trade secrets, the thief reaps a windfall from the prior research and development invested in the trade secrets. The trade secret owner loses the competitive advantages from the confidentiality of the trade secret.

The legislation will also promote litigation costs savings. The costs of litigation will certainly turn on the facts and circumstances of the case and the jurisdiction in which the case is filed. In general, it takes longer, and there are more delays in state court. In many jurisdictions, it can take longer to obtain a trial in state court than federal court.[102] Delay in obtaining a remedy is a significant cost by itself.

Once evidence crosses state lines, depositions or other discovery likely will fall outside of the court's jurisdiction and can only be reached with additional costs, expenses, and time. Under these circumstances, the state court process is usually cumbersome and more costly to obtain relief. The costs of litigation will be lower in federal court as a federal judge can order discovery and depositions, and enforce a judgment more efficiently and effectively than state courts.

Further cost savings will result from choices given to the trade secret owner by the legislation. The owner will be given a choice to pursue state or federal remedies depending on the circumstances. The owner may decide that a local misappropriation may be best for state court. To the extent cost may make a difference, the trade secret owner could pursue the least costly litigation option. So in a number of respects, the legislation will promote significant savings.

B. The Impact Of The New Seizure Order On Small Companies

Some have questioned the impact the court's seizure authority will have on small companies. First, the legislation will promote and protect trade secrets regardless of whether they are owned by small, medium and large companies as well as start-ups and individual. Small companies, like other entities will benefit from the ability to use the new seizure order provision. Many trade secrets are first developed in a small company or by individuals who have yet to form a company. In the event of trade secret theft, the small company can benefit by using the ex parte seizure provision to recover them through the federal court.

Second, the legislation contains several safeguards to prevent and address any abuse from the seizure provision. A court order will not issue unless the applicant makes the required showing to the satisfaction of the federal judge. The court, not a party to the action, takes custody of the trade secrets. The legislation includes restrictions about the publicity of the seizure which benefits those who might be unfairly targeted. Among other protections, the legislation establishes a private right of action for a person who suffers damage by a wrongful or excess seizure. The court can also award reasonable attorney's fees if it determines that a

misappropriation claim was made in bad faith. These protections will protect all companies or individuals.

C. "De-Harmonizing" State Trade Secret Law

Some have asked whether the federal legislation will "de-harmonize" state trade secret laws. The question misplaces the appropriate focus. The key issue is whether current law, which is based largely on a more-than-30-year-old statute, remains sufficient to address trade secret theft and misappropriation today. There is no reason trade secret law should be anchored to the past.

The federal legislation strengthens and modernizes trade secret law by addressing the technological realities and other challenges of today. The current federal criminal statute, the Economic Espionage Act of 1996, was originally based in large part on UTSA, which is the same model statute that 47 states have adopted in some form. UTSA was first promoted in 1979 and modified in 1985.

Many states have adopted variations to the UTSA model. For example, some states have criminal trade secret provisions and others do not. One challenge is that UTSA is now outdated in some key respects. A more-than-30-years-old statute model statute has not kept up with the technological advances and other challenges confronting trade secret law today particularly in our global and national economy. The legislation builds upon the UTSA framework to modernize and strengthen trade secret law. The failure to do so will allow the challenges in obtaining meaningful remedies under current law to persist, which is not acceptable.

Significantly, the legislation will not displace any state laws. There is no federal preemption. Instead, the legislation will provide another option to obtain remedies for trade secret misappropriation in federal court. In our global economy, the federal legislation is important given the role of trade secrets to commerce and because current state laws are often inadequate to address common challenges.

VII. Other Legislative Considerations

Two other issues deserve noting in considering the legislation.

A. Jurisdiction Also Based On Conduct

First, consideration should be given to including jurisdiction based on the interstate conduct related to the trade secret misappropriation.

The legislation provides federal jurisdiction based on "a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce."[103] This language is based on the recent amendment to the EEA, under the Theft of Trade Secrets Clarification Act of 2012,[104] which was enacted to correct the limitations imposed under the *United States v. Aleynikov* Second Circuit case.[105]

The current interstate standard can be augmented by a provision that clarifies that federal jurisdiction may be based on the transfer, in any manner, of a trade secret from one state to another state or outside the United States. Jurisdiction would then be based on either (a) the product or service intended for interstate or foreign commerce or (b) the interstate conduct in the case. The second option is similar to wire fraud,[106] which requires an interstate wire, and is based on the need for federal legislation to protect trade secrets removed from one state or the country. The current standard should cover most situations; language related to the transfer of the trade secret will remove any uncertainty and be consistent with the need for federal legislation.

B. Related Issue: Resolving The Circuit Split Under The Computer Fraud and Abuse Act

There is another issue that often arises in trade secret cases concerning the theft of confidential business information that is not a trade secret. In both criminal and civil cases, the defendant often misappropriates trade secrets along with other confidential business information. For example, the misappropriation may include financial, strategic and marketing information that may be useful to use and develop the stolen trade secrets. This information may not constitute trade secrets as defined under the EEA.

The Computer Fraud and Abuse Act (CFAA), first enacted in 1984,[107] is the primary federal computer statute that applies to the unauthorized obtaining or theft of information from a computer, along with related offenses. The CFAA provides for a civil private right of action for damages or equitable relief, along with potential criminal penalties.[108]

The courts are presently divided on whether the CFAA applies when a trusted employee steals the company's confidential information using the company's computer.[109] The court split has persisted for more than six years.[110] Consequently, the availability of a remedy depends on whether the jurisdiction applies a narrow or broad construction of the CFAA. Three circuits, including the First, Fifth and Eleventh Circuits, apply a broad construction which provides for a remedy for the theft of information by a computer.[111] However, two circuits, including the Fourth and Ninth Circuits, use a narrow interpretation and have held the CFAA does not cover this conduct.[112]

Because of the importance of confidential computer information, there should be a remedy when a trusted employee uses company computers to download, steal and transfer confidential business information either to start his own company or provide it to a competitor. The availability of a remedy for this theft should not turn on which jurisdiction the theft occurred.

In eventually addressing this problem, as part of a separate legislative reform apart from the current trade secret reform legislation, Congress has some options:

First, Congress can substitute a new standard which does not rely on "authorization" but instead focuses on the "use" or "purpose" to misuse the information. Several courts have considered this approach.

Second, Congress can use a misappropriation standard which would focus on whether the information was misappropriated or stolen. Initial authorized or unauthorized access to the information would not be dispositive. Instead, the facts concerning the intent and circumstances of the theft would determine whether the statute was violated.

Finally, if Congress is determined to retain the "authorization" standard, Congress should redefine the terms "without authorization" and "exceeds authorized access" to clarify that the statute applies when initial permitted access to information is later rescinded or abused. The current lack of clear guidance has resulted in disparate standards developed by the courts.

Insider theft of computer information should be covered under the CFAA. This type of conduct should not be subject to varying interpretations by the courts. Eventually this issue will need to be confronted. The problem arises in many trade secret cases but other cases too. I do not suggest that this issue be considered with the current legislation.

VIII. Reinforcing the Original Objectives of the EEA to Promote and Protect National and Economic Security

The EEA was enacted in 1996 to promote and protect national and economic security.[113] As part of a bipartisan effort, the statute was enacted to fill in gaps under the law which previously allowed this conduct to go unpunished.[114]

In signing the EEA into law, President William J. Clinton noted:

> 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.[115]

The original objectives remain but in many respects, there are new risks and challenges to protect trade secrets. Since 1996, the role of trade secrets and information has expanded in ways that could not have been envisioned. In our global economy, trade secrets continue to play a vital role in the development of new products and services. However, without a meaningful ability for trade secret owners to recover their stolen trade secrets and obtain an adequate remedy, this key aspect of innovation is undermined.

The legislation will help modernize and strengthen trade secret law. It builds on the traditions of UTSA and addresses current issues and challenges. In my view, the legislation has strong bipartisan support and should be enacted.

Thank you for the opportunity to share my views on this important issue.

Endnotes:

[1] My statement is offered in my personal capacity based on my experience handling trade secret and foreign economic espionage cases and not on behalf of any organization or client. My views do not necessarily reflect the views of my firm, its clients, or my former employer, the U.S. Department of Justice.

[2] The National CHIP Program involves more than 250 federal prosecutors specially trained to prosecute cybercrime and intellectual property enforcement cases. For more on the history of the CHIP Program and DOJ cybercrime efforts, *see* Mark Krotoski, DOJ Cybercrime Efforts That Led To New Cybersecurity Unit, Law360 (Jan. 7, 2015), http://morganlewis.com/~/media/law360_dojcybercrimeeffortsnewcybersecurityunit_07jan15.ashx.

[3] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended in 18 U.S.C. §§ 1831–1839).

[4] *See* U.S. Attorney's Manual § 9-59.100 ("The United States may not file a charge under 18 U.S.C. § 1831 of the Economic Espionage Act (hereinafter the 'EEA'), or use a violation under § 1831 of the EEA as a predicate offense under any other law, without the approval of the Assistant Attorney General for the National Security Division . . . ."), http://www.justice.gov/usam/usam-9-59000-economic-espionage.

For a summary of the first eleven foreign economic espionage cases, *see* Appendix A; *see also* Mark L. Krotoski & Jenny Harrison, *Reviewing the First Foreign Economic Espionage Cases*, BNA'S PATENT, TRADEMARK & COPYRIGHT JOURNAL, 90 PTCJ 1951 (May 8, 2015) (summarizing the facts and proceedings for the first ten foreign economic espionage cases), http://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bbnainsight_foreigneconomicespionage.ashx.

[5] Redacted Plea Agreement at ¶ 2, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Aug. 29, 2007, ECF Nos. 76, 77); Meng Government's Sentencing Memorandum at 5, 10–11 (June 11, 2008) (ECF No. 94).

[6] Superseding Indictment at ¶¶ 28, 40, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Dec. 17, 2004, ECF No. 57; Meng Redacted Plea Agreement at ¶ 2 (Aug. 29, 2007), ECF Nos. 76, 77); Meng Government's Sentencing Memorandum at 8 (June 11, 2008), ECF No. 94); Press Release, U.S. Dep't of Justice, Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China (Dec. 14, 2006), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/mengCharge.htm.

[7] Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), 22 U.S.C. §§ 2778(b)(2), 2778(c), and 22 C.F.R. § 120.2.

[8] Meng Redacted Plea Agreement at ¶ 2 (Aug. 29, 2007), ECF Nos. 76, 77; Meng Judgment (June 24, 2008), ECF No. 103; *see generally* Press Release, U.S. Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html; Press Release, U.S. Dep't of Justice, Chinese National Sentenced For Committing Economic Espionage with the Intent to Benefit China Navy Research Center (June 18, 2008), http://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/mengSent.pdf. According to court records, the sentence included a reduction based on substantial assistance provided under U.S.S.G. § 5K1.1. *See* Meng Sentencing Hearing Transcript at 10–11, 17–18 (June 18, 2008).

[9] Huang Sentencing Hearing Transcript at 17, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Dec. 22, 2011) (testimony of Dow AgroSciences managing counsel summarizing investigation); *see also* Press Release, U.S. Dep't of Justice, Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets (Dec. 21, 2011), http://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets.

[10] *See* Huang Plea Hearing Transcript at 41–43 (Oct. 18, 2011); Huang Sentencing Hearing Transcript at 18, 25 (Dec. 22, 2011); and Huang Plea Agreement ¶ 8(D).

[11] Defendant's Memorandum of Law in Support of Motion for Revocation of Detention at 6–7, *United States v. Kexue Huang*, No. 10-CR-0163 (S.D. Ind. Sept. 23, 2010), ECF No. 42; Huang Plea Agreement ¶ 8(A); Huang Government's Sentencing Memorandum at 10–11 (Dec. 12, 2011), ECF No. 91; Huang Sentencing Hearing Transcript at 23 (Dec. 22, 2011).

[12] Press Release, U.S. Dep't of Justice, Chinese National Charged with Economic Espionage Involving Theft of Trade Secrets from Leading Agricultural Company Based in Indianapolis (Aug. 31, 2010), http://www.justice.gov/criminal/cybercrime/press-releases/2010/huangChar.pdf.

[13] Huang Plea Hearing Transcript (Oct. 18, 2011); Huang Plea Agreement; Order (March 8, 2011), ECF No. 72; *see also* Press Release, U.S. Dep't of Justice, Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets (Oct. 18, 2011), http://www.justice.gov/opa/pr/chinese-national-pleads-guilty-economic-espionage-and-theft-trade-secrets.

[14] *See* note 31, *infra*, for further information concerning *United States v. Philip Gabriel Pettersson aka "Stakkato"*, No. 09-CR-00471-RMW (N.D.Cal. May 5, 2009).

[15] 14 U.L.A. 438 (1990). For the UTSA, *see* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf. For UTSA jurisdictions, see http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade Secrets Act.

[16] 18 U.S.C. § 1839(3) (trade secret definition).

[17] Center for Responsible Enterprise And Trade (CREATe.org) and PricewaterhouseCoopers LLP, Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats, 3 (Feb. 2014), https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.

[18] U.S. Bureau of Economic Analysis, National Income and Products Accounts, Gross Domestic Product: Third Quarter 2015 (Second Estimate), http://www.bea.gov/newsreleases/national/gdp/gdpnewsrelease.htm.

[19] Under the Sentencing Guidelines, a variety of factors and measures may be considered such as the "reasonably foreseeable pecuniary harm"; the "fair market value of the property unlawfully taken, copied, or destroyed" or "the cost to the victim of replacing that property"; "the cost of developing that information or the reduction in value of that information that resulted from the offense." U.S.S.G. § 2B1.1 cmt. n.3(A)(i), 3(C)(i), (ii).

[20] Restitution Order, *United States v. Kolon Industries, Inc.*, No. 12-CR-00137 (E.D. Va. April 30, 2015), ECF No. 194); Plea Agreement at ¶¶ 19–20 (E.D. Va. April 30, 2015) (restitution & fine), ECF No. 191; Judgment (E.D. Va. May 1, 2015), ECF No. 196; *see also* Press Release, U.S. Dep't of Justice, Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology (Apr. 30, 2015), http://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

[21] Government Sentencing Memorandum, at 22, 29-30, *United States v. Shanshan Du & Yu Qin*, No. 10-CR-20454 (E.D. Mich. April 25, 2013) (ECF No. 185).
Government Sentencing Memorandum at 22, 29–30, *United States v. Shanshan Du & Yu Qin*, No. 10-CR-20454 (E.D. Mich. April 25, 2013), ECF No. 185.

[22] Entry of Judgment, *UniRAM Technology, Inc. v. Taiwan Semiconductor Manufacturing Co.* at *2–3, No. 04-CV-01268 (N.D. Cal. April 17, 2008), ECF No. 628 (Plaintiff's damages expert estimated Defendant generated over $185 million in profits off the accused products, while Defendant's expert used a different accounting method for calculating revenues and costs, arriving at a profit figure of $78.6 million, of which only a portion was attributable to the misappropriated memory macros.).

[23] Government's Sentencing Memorandum at 4, *United States v. Chung*, No. 08-CR-00024 (C.D. Cal. Feb. 11, 2010), ECF No. 156 (estimating the loss to be around $35 million based on Boeing's research and development expenditure of over $35 million to develop the trade secret and noting the Probation estimate of over $20 million); *see also* Memorandum of Decision, *United States v. Chung*, 633 F. Supp. 2d 1134 (C.D. Cal. 2009), *aff'd*, 659 F.3d 815 (9th Cir. 2011) (affirming conviction and sentence).

[24] *See* Defendant's Sentencing Memorandum at 3, *United States v. Agodoa*, No. 13-CR-20525 (E.D. Mich. Jan. 14, 2014), ECF No. 27 (agreeing with loss estimate obtained from Wacker Chemical Corporation grand used by probation for the recommended sentence).

[25] Plea Hearing at *33, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Oct. 18, 2011), 11-CR-00163 (D. Minn. Dec. 21, 2011); Sentencing Hearing at *7, 32, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Dec. 21, 2011), 11-CR-00163 (D. Minn. Dec. 21, 2011).

[26] *United States v. Williams*, No. 06-CR-313 (N.D. Ga. May 23, 2007) (intended loss of $1.5 million was determined to "under represent the seriousness of the offense"), *aff'd*; 526 F.3d 1312, 1321 n.2 (11th Cir. 2008) (affirming conviction and sentence; concluding "the district court did not err by considering" Coca-Cola's annual revenues "in deciding whether the $1.5 million intended loss calculated under the guidelines underrepresented the seriousness of the offense").

[27] Exec. Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 1, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[28] Press Release, Federal Bureau of Investigation, Update on Sony Investigation (December 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
[29] Press Release, U.S. Dep't of Justice, Four Members of International Computer Hacking Ring Indicted for Stealing Gaming Technology, Apache Helicopter Training Software (Sept. 30, 2014), http://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache.
[30] Indictment, *United States v. Wang Dong et al*. No. 14-CR-118 (W.D. Pa. May 2014), http://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf ; *see also* Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
[31] Indictment, *United States v. Philip Gabriel Pettersson aka "Stakkato"* No. 09-CR-00471-RMW (N.D. Cal. May 5, 2009), http://www.wired.com/images_blogs/threatlevel/2009/05/petterssonindictment.pdf; *see also* Dan Goodin, Sweden to Prosecute Alleged Cisco, NASA Hacker, THE REGISTER (Feb. 8, 2010), http://www.theregister.co.uk/2010/02/08/swedish_hacker_prosecution.
[32] *See, e.g.*, Mandiant: *APT1 Exposing One of China's Cyber Espionage Units* (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; FireEye, *APT28: A Window Into Russia's Cyber Espionage Operations?* at 3 (2015), https://www2.fireeye.com/apt28.html; Office of the National Counterintelligence Executive: Foreign Spies Stealing U.S. Economic Secrets in Cyberspace (Oct. 2011), http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
[33] On the civil remedies factor, U.S. Department of Justice policy clarifies that: "The availability of a civil remedy should not be the only factor considered in evaluating the merits of a referral because the victim of a trade secret theft almost always has recourse to a civil action. The universal application of this factor would thus defeat the Congressional intent in passing the EEA." U.S. Attorney's Manual § 9-59.100, http://www.justice.gov/usam/usam-9-59000-economic-espionage.
[34] U.S. Attorney's Manual § 9-59.100 (listing factors), http://www.justice.gov/usam/usam-9-59000-economic-espionage. *See also* Tom Reilly, Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and the "Foreign Instrumentality" Element, 57 UNITED STATES ATTORNEYS' BULLETIN 2, 12–13 (Nov. 2009) (describing review process), http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf.
[35] *See, e.g.*, Cal. Penal Code § 499c (trade secret theft may result in a criminal fine up to $5,000 and up to one year in jail); Nev. Rev. Stat.§ 600A.035 (trade secret theft is punishable by "a minimum term of not less than 1 year and a maximum term of not more than 10 years" in prison and "a fine of not more than $10,000''); RCW § 9A.56.010(6) (defining "deprive," under the theft and robbery statute, to include the "unauthorized use or an unauthorized copy of records, information, data, trade secrets, or computer programs"); Tex. Penal Code §31.05 (at least two years imprisonment and up to a maximum of 10 years and a fine of up to $10,000).
[36] States have recognized this problem. Several states have adopted the Uniform Interstate Depositions and Discovery Act. However, many states have not, including Texas and Florida. *See* Legislative Fact Sheet - Interstate Depositions and Discovery Act (listing states), http://www.uniformlaws.org/Act.aspx?title=Interstate%20Depositions%20and%20Discovery%20Act.
[37] Fed. R. Civ. P. 45(b)(2) ("A subpoena may be served at any place within the United States").
[38] *See* 28 U.S.C. §§ 1331 (federal question), 1332 (diversity of citizenship).
[39] *See also* U.S. CONST. art. III, § 2 ("The judicial power shall extend to all Cases, in Law and Equity . . . between Citizens of different States.").
[40] 28 U.S.C. §§ 1331 (federal question); *see also* U.S. CONST. ART. III, § 2 (federal courts can hear "all cases, in law and equity, arising under this Constitution, [and] the laws of the United States").
[41] 18 U.S.C. § 1030(g) (limited civil cause of action).
[42] Mark Krotoski, *Viewpoint: Time to Reform the Computer Fraud and Abuse Act*, THE RECORDER (Nov. 18, 2015) (noting circuit split and need for reform), http://www.therecorder.com/home/id=1202742832060/Viewpoint-Time-to-Reform-the-Computer-Fraud-and-Abuse-Act?slreturn=20151021171349; Mark Krotoski & Brock Dahl: *Stealing Trade Secrets and Confidential Information With Computers*, BNA'S PATENT, TRADEMARK & COPYRIGHT JOURNAL, 89 PTCJ 1142 (Feb. 27, 2015) (same).
[43] 28 U.S.C. § 1367 (supplemental jurisdiction).
[44] Mark Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 UNITED STATES ATTORNEYS' BULLETIN 2, 12–13 (Nov. 2009) (describing reactive nature of trade secret investigations), http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf.

[45] *See generally* Mark Krotoski, Identifying And Using Electronic Evidence Early To Investigate And Prosecute Trade Secret And Economic Espionage Act Cases, 57 UNITED STATES ATTORNEYS' BULLETIN 42-51 (Nov. 2009) (noting cases involving the use of computers and emails to obtain and transfer trade secrets), http://www.justice.gov/criminal/cybercrime/docs/prosecuting_ip_crimes_manual_2013.pdf.
[46] Press Release, U.S. Dep't of Justice, Former DuPont Chemist Sentenced to 14 Months in Prison for Stealing DuPont Trade Secrets (Oct. 21, 2010), https://www.fbi.gov/baltimore/press-releases/2010/ba102110a.htm.
[47] Press Release, U.S. Dep't of Justice, Two Engineers Found Guilty of Stealing Goodyear Trade Secrets (Dec. 9, 2010) (noting that "the defendants used a cell phone camera to surreptitiously take seven unauthorized photographs of a Goodyear swab down device" and "then emailed the unauthorized photographs to employees at a Wyko subsidiary located in Dudley, England"), http://www.justice.gov/opa/pr/two-engineers-found-guilty-stealing-goodyear-trade-secrets.
[48] Press Release, U.S. Dep't of Justice, Former Connecticut Resident Pleads Guilty to Attempting to Send Sensitive Military Documents to Iran (Feb. 25, 2015) (noting the defendant "corresponded by email with an individual in Iran to whom he attempted to send, and in some cases did send, documents containing trade secret, proprietary and export controlled material relating to the Joint Strike Fighter Program"), http://www.justice.gov/opa/pr/former-connecticut-resident-pleads-guilty-attempting-send-sensitive-military-documents-iran; Government's Sentencing Memorandum at 5–6, *United States v. David Kent Lewis*, No. 14-CR-00014 (E.D. Ky. Oct. 8, 2014), ECF No. 19; Judgment (E.D. Ky. Oct. 8, 2014), ECF No. 21; *see also* Press Release, U.S. Dep't of Justice, Former Winchester Brake Pad Engineer Pleads Guilty to Theft of Trade Secrets Charge (March 5, 2014) (noting the defendant "emailed trade secrets concerning the specifications of brake pads" and "was paid thousands of dollars by a Canadian company for this information"), http://www.justice.gov/usao-edky/pr/former-winchester-brake-pad-engineer-pleads-guilty-theft-trade-secrets-charge.
[49] 1996 House Report, at 4 (noting ''threats to the nation's economic interest are threats to the nation's vital security interests'').
[50] *See* 17 U.S.C. §§ 501 *et seq*.
[51] *See* Lanham Act, 15 U.S.C. §§ 1051–1127.
[52] *See* U.S. Patent Act, 35 U.S.C. §§ 1 *et seq*.
[53] Federal criminal statutes already apply to copyright and trademark infringement and trade secret misappropriation. Criminal copyright cases are authorized under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319; criminal trademark cases are provided for under 18 U.S.C. § 2320. Trade secret misappropriation is subject to criminal penalties under the Economic Espionage Act, 18 U.S.C. §§ 1831-1839.
[54] *See* 17 U.S.C. § 102(a) (subject matter of copyright).
[55] *See* 15 U.S.C. § 1127 (defining "trademark").
[56] 35 U.S.C. § 154(a) (contents and term of patent).
[57] *Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co.*, 107 F.R.D. 288, 289 (1985) ("The formula for Merchandise 7X has been tightly guarded since Coca-Cola was first invented and is known by only two persons within The Coca-Cola Company…. The only written record of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, Georgia, which can only be opened upon a resolution from the Company's Board of Directors.").
[58] *Coca-Cola Co. v. Koke Co. of America*, 254 U.S. 143, 145 (1920) (in trademark infringement action, summarizing prior trademarks); *United States v. Coca Cola Co. of Atlanta*, 241 U.S. 265, 272 (1916) (describing the registered trademark of "Coca Cola" in the 1890s); *Coca-Cola Company v. Gemini Rising, Inc.*, 346 F. Supp. 1183, 1186 (E.D.N.Y. 1972) (in injunction for "Coca-Cola" trademark, noting trademarks filed in 1893, 1905, and 1928).
[59] The Coca-Cola logo story, http://www.coca-cola.co.uk/stories/history/advertising/the-logo-story.
[60] U.S. Registration Number: 696147 (1960) (bottle), http://tsdr.uspto.gov/#caseNumber=72069873&caseType=SERIAL_NO&searchType=statusSearch ; *see also Qualitex Co. v. Jacobson Products Co.*, 514 U.S. 159, 162 (1995) (noting that the "courts and the Patent and Trademark Office have authorized for use as a mark a particular shape (of a Coca-Cola bottle), …."); *see generally* Coke Lore: Trademark Chronology, http://www.coca-colacompany.com/stories/coke-lore-trademark-chronology.
[61] *See* U.S. Design Patent No. 48160 (1915), http://www.google.com/patents/USD48160 ; *see also* The Story of the Coca-Cola Bottle (Feb. 26, 2015), http://www.coca-colacompany.com/stories/the-story-of-the-coca-cola-bottle.
[62] S. 1890 § 2 (proposed § 1836(b)(2)(A)(i)).
[63] *Id*. § 1836(b)(2)(A).
[64] *Id*. § 1836(b)(2)(B).
[65] *Id*. § 1836(b)(2)(E).

[66] *Id*. § 1836(b)(2)(D).
[67] *Id*. § 1836(b)(2)(D).
[68] *Id*. §§ 1836(b)(2)(B)(iv), (F)(i).
[69] *Id*. § 1836(b)(2)(F)(ii).
[70] *Id*. § 1836(b)(2)(F)(iii).
[71] *Id*. § 1836(b)(2)(G).
[72] *See, e.g., Homecare CRM, LLC v. Adam Group, Inc*., 952 F. Supp. 2d 1373, 1380 (N.D. Ga. 2013) (Rule 11 sanctions ordered when "the factual allegations in support of Homecare's trade-secrets claim do not, and did not at the time this action was filed, have evidentiary support…"); *see also Qad., inc. v. ALN Assoc., Inc*., 18 U.S.P.Q. 2d 1122 (N.D. Ill. 1990) (dismissing Qad's trade secret count and awarding Rule 11 sanctions to defendant based on Qad's persistent failure to identify a claim); *Robertshaw Controls Co. v. Weerstra*, 1990 U.S. Dist. LEXIS 17380 at *16 (W.D. Mich. 1990) (ordering Rule 11 sanctions when "[a]lthough the Court has concluded that it was at least reasonable to file the complaint, further investigation of the facts would have revealed that defendant never stole any confidential information or trade secrets").
[73] S. 1890 § 2 (proposed § 1836(b)(3)(D)).
[74] *Id*. § 1836(b)(2)(D).
[75] *Id*.
[76] *Id*. § 1836(b)(2)(H).
[77] *See, e.g.*, Cal. Penal Code § 499c (trade secret theft may result in a criminal fine up to $5,000 and up to one year in jail); Nev. Rev. Stat.§ 600A.035 (trade secret theft is punishable by ''a minimum term of not less than 1 year and a maximum term of not more than 10 years'' in prison and ''not more than $10,000''); RCW § 9A.56.010(6) (defining ''deprive,'' under the theft and robbery statute, to include the ''unauthorized use or an unauthorized copy of records, information, data, trade secrets, or computer programs''); Tex. Penal Code §31.05 (at least two years imprisonment and up to a maximum of 10 years and a fine of up to $10,000).
[78] 1996 House Report, at 7.
[79] 142 CONG. REC. H10462 (Sept. 17, 1996).
[80] *Id*. S12212 (daily ed. Oct. 2, 1996).
[81] *Id*. S12213 (daily ed. Oct. 2, 1996) (Manager's Statement).
[82] *Id*.
[83] UTSA, Section 5 provides that "a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval."
[84] 18 U.S.C. § 1835 provides: "In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret."
[85] *See generally Mohawk Industries, Inc. v. Carpenter*, 558 U.S. 100 (2009) (holding interlocutory appellate review of an adverse attorney-client privilege ruling was not available and reinforcing the role of one appeal following a final judgment in the case).
[86] *See United States v. Hsu*, 155 F.3d 189, 203-04 (3d Cir. 1998) (reversing disclosure order as the attempt and conspiracy offenses did not require actual proof of the trade secret); *see also United States v. Fei Ye*, 436 F.3d 1117, 1121 (9th Cir. 2006) (although the circuit lacked jurisdiction over the interlocutory appeal since "the district court's order does not direct or authorize the 'disclosure' of trade secrets as required by the plain language of § 1835," issuing a writ of mandamus to rescind the district court ruling mandating pretrial depositions concerning the trade secrets).
[87] 18 U.S.C. § 1839(3).
[88] 1996 House Report, at 12; *see also United States v. Chung*, 659 F.3d 815 (9th Cir. 2011) (noting that the EEA trade secret definition "is derived from the definition that appears in the Uniform Trade Secrets Act" and "we consider instructive interpretations of state laws that adopted the UTSA definition without substantial modification") (footnote omitted); *Hsu*, 155 F.3d at 196 ("The EEA's definition of a 'trade secret' is similar to that found in a number of state civil statutes and the Uniform Trade Secrets Act ('UTSA'), a model ordinance which permits civil actions for the misappropriation of trade secrets. There are, though, several critical differences which serve to broaden the EEA's scope.") (footnote omitted).

[89] *See generally Ratzlaf v. United States*, 510 U.S. 135, 147-48 (1994) ("we do not resort to legislative history to cloud a statutory text that is clear").
[90] UTSA, § 1(4).
[91] 18 U.S.C. § 1839(3).
[92] 1996 House Report, at 12 ("These general categories of information are included in the definition of trade secret for illustrative purposes and should not be read to limit the definition of trade secret. It is the Committee's intent that this definition be read broadly.").
[93] 1996 House Report, at 11; *see also id*. at 4 ("In the last few decades, intangible assets have become more and more important to the prosperity of companies…. As the nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow.").
[94] 18 U.S.C. § 1837 (applicability to conduct outside the United States); *see also* 1996 House Report, at 14 ("To rebut the general presumption against the extraterritoriality of U.S. criminal laws, this subsection makes it clear that the Act is meant to apply to the specified conduct occurring beyond U.S. borders.").
[95] *See generally Kiobel v. Royal Dutch Petroleum Co.*, 133 S.Ct. 1659, 1664-65 (2013) (applying presumption to the Alien Tort Statute); *Morrison v. National Australia Bank Ltd.*, 130 S.Ct. 2869, 2878 (2010) (noting "[w]hen a statute gives no clear indication of an extraterritorial application, it has none").
[96] *See* UTSA, § 6.
[97] 18 U.S.C. § 1838.
[98] Why States Should Adopt USA, Uniform Law Commission, National Conference of Commissioners on Uniform State Laws (last visited Dec. 1, 2015), http://www.uniformlawcommission.com/Narrative.aspx?title=Why%20States%20Should%20Adopt%20USA.
[99] Age Discrimination in Employment Act (ADEA), 29 U.S.C. §§ 621-634.
[100] *See* State Computer Crime Statutes, National Conference of State Legislatures (last updated June 12, 2015) (listing state statutes), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.
[101] 18 U.S.C. § 1030 *et. seq*.
[102] For example, fewer than 66% of California civil unlimited cases were disposed of in less than 12 months and 16% remained pending after 24 months for the financial year 2014. 2015 Court Statistics Report, Statewide Caseload Trends 2004-2005 Through 2013-2014, Judicial Council of California, page 71 (available at http://www.courts.ca.gov/documents/2015-Court-Statistics-Report.pdf). On the other hand, the average time from filing to disposition for civil cases in federal court for the year ending on June 30, 2015 was 8.8 months and only 8.9% of civil cases were over three years old. U.S. District Courts – Combined Civil and Criminal Federal Court Management Statistics, United States Courts (Dec. 31 2014) (available at http://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2015/06/30-3).
[103] S. 1890 § 2 (proposed § 1836(b)(1)).
[104] Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012), https://www.congress.gov/112/plaws/publ236/PLAW-112publ236.pdf.
[105] *United Staes. v. Aleynikov*, 676 F.3d. 71 (2d Cir. 2012).
[106] 18 U.S.C. § 1343 (wire fraud).
[107] 18 U.S.C. § 1030. Section 1030 was originally enacted in 1984. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified at 18 U.S.C. § 1030 *et seq*.).
[108] 18 U.S.C. § 1030(g) (civil private right of action). Congress added the private right of action in 1994. *See* Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097–2099.
[109] *See, e.g.*, M. Krotoski & B. Dahl, Stealing Trade Secrets and Confidential Information With Computers: Time to Resolve the Lingering Circuit Split, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 1142 (Feb. 27, 2015) (89 PTCJ 1142, 2/27/15) (reviewing circuit split).
[110] *See, e.g.*, *LVRC Holdings LLC, v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (noting disagreement with Seventh Circuit construction); see also United States v. John, 597 F.3d 263, 269 (5th Cir. 2010) (noting disagreement with Ninth Circuit construction of the CFAA); *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 & nn. 65-66 (S.D.N.Y. 2010) (noting the division among federal circuit and district court cases construing the CFAA).
[111] *See United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st 2001).

[112] *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 202 (4th Cir. 2012), *cert. dismissed*, 133 S.Ct. 831 (2013) (No. 12-518); *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).
[113] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended in 18 U.S.C. §§ 1831–1839).
[114] 1996 House Report, at 4 (noting "the nation's economic interests are part of its national security interests" and "threats to the nation's economic interest are threats to the nation's vital security interests"); *id*. at 6-7 (noting gaps under federal law); *see also United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998) (noting prior to the EEA "the absence of any comprehensive federal remedy targeting the theft of trade secrets, compelling prosecutors to shoehorn economic espionage crimes into statutes directed at other offenses").
[115] President William J. Clinton, Presidential Statement on the Signing of the Economic Espionage Act of 1996 (Oct. 11, 1996), available at 1996 Pub. Papers 1814 (Oct. 11, 1996), http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/pdf/WCPD-1996-10-14-Pg2040-2.pdf.

Appendix A

Summary of the First Eleven Foreign Economic Espionage Cases

Under 18 U.S.C. § 1831

(1996 – 2015)

Appendix A

Summary of the First Eleven Foreign Economic Espionage Cases Under 18 U.S.C. § 1831 (1996 – 2015)

Case	Case	Court; Case No.	Defendant: Disposition	Date of Misappro.	Date of Indictment	Date of Disposition	Trade Secret	Theft of Secret	Foreign Government Connection	Sentence
1	Okamoto	NDOH; No. 01-CR-00210	**Okamoto:** fugitive **Serizawa:** plea conviction: §1001 (1 count)	1999	May-01	NA	Trade secrets regarding DNA & cell line reagents	Employee stole trade secrets from his employer, sent them to Serizawa for holding, then took a new position at a state-funded research institute in Japan.	Japanese state-funded research institute	Okamoto: A fugitive Serizawa: 3 yrs probation, 150 hrs community service; $500 fine
2	Fei Ye	NDCA; No. 02-CR-20145	**Fei Ye**: plea conviction: §1831 (2 counts); acquittals: §1832 (3 counts); §371 (1 count); §2314 (2 counts) **Zhong:** plea conviction: §1831 (2 counts); acquittals: §1832 (4 counts); §371 (1 count); §2314 (2 counts)	2001	Dec-02	Dec-06	Trade secrets regarding the design and manufacture of computer microprocessors	Employees stole employer's trade secrets and planned to use them at their PRC-funded company, but were stopped at the airport with the secrets.	PRC state-funded private company	Both: 366 days in prison, 3 yr supervised release
3	Meng	NDCA; No. 04-CR-20216	**Meng:** plea: convictions: §1831 (1 count); 22 USC § 2778 (1 count); aquittals: §2314 (14 count); §371 (3 counts); §1831 (2 counts); §2778 (1 count); §1832 (12 counts); §1001 (3 counts)	2003	Dec-04	Aug-07	Trade secrets regarding visual simulation software program	Employee took employer's trade secrets to new job in the PRC. He was stopped at the airport with the secrets when traveling to the US on a business trip.	PRC Navy Research Cen	24 months + 1 day in prison, 3 yr supervised release; $10,200 fine
4	Lee	NDCA; No. 06-CR-00424	**Lee:** jury trial acquittal: §1831 (3 counts); §1832 (4 counts) **Ge:** jury trial acquittal: §1831 (3 counts); §1832 (4 counts)	2003	Sep-07	Dec-09	Trade secrets regarding computer chip designs and manufacturing information	Employees allegedly stole trade secrets from two former employers to use at their own company.	Private company seeking PRC state-funding	NA
5	Chung	CDCA; No. 08-CR-00024	**Chung:** bench trial conviction: §1831 (6 counts), §951 (1 count), §371 (1 count); §1001 (1 count); acquittals: §1831 (2 counts); §1512 (1 count); §1001 (2 counts)	2003-2006	Feb-08	Jul-09	Trade secrets regarding space shuttle and Delta IV rocket	Employee stole two former employers' trade secrets	PRC military	188 months in prison
6	Jin	NDIL; No. 08-CR-00192	**Jin:** bench trial conviction: §1832 (3 counts); acquittal: §1831 (3 counts)	2007	Apr-08	Nov-11	Trade secrets regarding iDEN mobile communications technology	Employee stole employer's trade secrets and planned to take them to the PRC to work for a company connected to the PRC military, but was stopped at the airport with the documents.	PRC military	4 years in prison; $20,000 fine
7	Huang	SDIN; No. 10-CR-0102	**Huang:** plea conviction: §1831 (1 count); acquittal: §1831 (11 counts); §2314 (5 counts)	2007-2010	Jun-10	Oct-11	Trade secrets regarding insecticides	Employee stole employer's trade secrets, transferred them to the PRC and Germany, and worked at a PRC university to further develop them.	PRC state-funded research institute	87 months in prison
8	Doxer	D.Mass; No. 11-CR-10268	**Doxer:** plea conviction: §1831 (1 count)	2006	Jul-11	Aug-11	Confidential company information (contractual papers, customer lists, and employee lists)	Employee stole documents he had access too. Only sting-operation case.	Israel	6 months prison; 6 months home confinement; $25,000 fine
9	Liew	NDCA; No. 11-CR-00573	**Liew:** jury trial conviction: §1831 (2 counts), §1832 (6 counts), §1512 (3 counts), §1004 (1 count), §152 (3 counts), §7206 (5 counts) **Maegerle:** jury trial conviction: §1832 (3 counts), §1512 (1 count) **Chao:** plea conviction: §1831 (1 count) **C. Liew:** pending trial	1998-2008	Feb-12	2014	Trade secrets regarding pigment manufacturing processes	Employees stole employer's trade secrets and used them to obtain contracts with PRC companies.	PRC state-funded company	Liew: 180 mths in prison; Maegerle: 18 mths; Both: forfeit $27.8M

Appendix A
Summary of the First Eleven Foreign Economic Espionage Cases Under 18 U.S.C. § 1831 (1996 – 2015)

Case	Case	Court; Case No.	Defendant: Disposition	Date of Misappro.	Date of Indictment	Date of Disposition	Trade Secret	Theft of Secret	Foreign Government Connection	Sentence
10	Dong	WDPA; No. 14-CR-118	All 5 defendants (Dong, Kailiang, Xinyu, Zhenyu, Chunhui) are fugitives and the 31-count indictment is pending	2006-2014	May-14	NA	Information including emails regarding business strategies, financial positions, and production capabilities	Cyber-espionage: alleged hacking of company computer systems through spear-phishing emails	PRC military	NA
11	Pang	NDCA; No. 15-CR-106	Hao Zhang: arrested on 5/16/2015 Remaining 5 defendants (Pang, Huisui Zhang, Chen, Gang, Zhou) are fugitives and the 32-count indictment is pending	2006-2015	Apr-15	NA	Confidential thin-film bulk acoustic resonator ("FBAR") technology	Employees allegedly stole employers' trade secrets and used them to obtain business with a PRC-sponsored university to further develop the technology.	PRC state-funded research institute	NA

Appendix B

Trade Secret Examples Based on Recent

Criminal and Civil Cases

Appendix B
Trade Secret Examples
Based on Recent Criminal and Civil Cases

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
1	"Inbred"or"parent" line of corn seed information	U.S.seed companies DuPontPioneer, Monsanto,and LG Seeds,located in Iowa, Missouri,and Indiana respectively and utilizingfacilities in Iowa,Illinois,and Indiana[1]	Agriculture	• *Criminal case* • *Alleged Conduct*:Third SupersedingIndictmentalleges the defendants conspired to stealtrade secrets of seed manufacturing companies,and transportthem to Chinato use in theirChina-based seed company • *Disposition*:Case remains pending[2]
2	Proprietary organic insecticides	Dow AgroSciences, headquartered in Indiana[3]	Agriculture	• *Criminal case* • *Conviction:* Defendantwho served as aresearchscientistand leaderfor strain developmentpled guilty to stealinghis employer's trade secrets and furtherdevelopingthem as his position as visitingprofessorat Hunan NormalUniversity in the PRC • *Disposition*:Sentenced to serve **87 months in prison**[4]
3	Computer-assisted drawingsoftware forairplane parts, includingaircraft brake assembly and specifications	ReplacementAircraft Parts C o.(RAP C O) located in Wisconsin	Airplane parts	• *Criminal case* • *Bench Trial Conviction:* Defendant convicted under18 U.S.C .§ 18 32 forstealinghis employer's dataand attemptingto sellitto acompetitor • *Disposition*:Sentenced to **30 months** in prison and **$2,500 fine**; conviction affirmed on appeal[5]
4	Hybrid motor technology	GeneralMotors located in Michigan[6]	Automobile	• *Criminal case* • *Jury Trial Conviction:* A former GeneralMotors engineer(Yu Q in) and herhusband (Shanshan D u) were convicted atajury trialfor copying16,000 GM computerfiles whichincluded trade secrets,with the intentto use them in ajoint venture withan automotive competitorin Chinaunder18 U.S.C .§ § 18 32(a)(3),(a)(5)and othercounts • *Disposition*:Q in was sentenced to **three years in prison** and a **$25,000 fine** and Du was sentenced to **a year and a day in prison** and a **$12,500 fine**[7] ;the trialconvictions and sentences were affirmed on appeal[8]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
5	Brake pad specifications	Brake Parts International,Inc., headquartered in Illinois,withproduction in Kentucky[9]	Automobile	• *Criminal case* • *Conviction:* Defendantpled guilty to one countof conspiringto committheftof trade secrets under 18 U.S.C .§ 18 32(a)(5)fore-mailingbrake pad formulations and providingtrade secretinformation to acompetitor • *Disposition*:Sentenced to **three years probation**,nine months home incarceration,and **$32,000 in restitution**[10]
6	CocaCola® marketing information,product sample	CocaCola, headquartered in Georgia	Beverage	• *Criminal case* • *Jury Trial Conviction:* Lead defendantemployee convicted in a jury trialformisappropriatingCoca Cola's trade secrets and attempting to sellthem forprofitto a competitor • Disposition:Sentenced to **96 months** in prison and ordered to pay **restitution of $40,000**[11] • *Other Convictions*:Co-defendants: *United States v. Dimson* (sentenced June 5,2007 ,to **60 months** and **$40,000 restitution** followingplea to conspiracy)[12];*United States v. Duhaney* (sentenced June 5,2007 , to **24 months** and **$40,000 restitution** followingpleato conspiracy and included a downward departure forsubstantial assistance underU.S.S.G.§ 5K1.1)[13]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
7	Kevlar® technology used forbody armor,fiberoptic cables,automotive and industrial products	E.I.DuPontde Nemours & Co., headquartered in Delaware,and manufactured in Virginia,Ireland,and Japan	Chemical	• *Criminal case* • *Conviction:* SouthKorean company pled guilty to conspiring withformerDuPontemployees to stealtrade secrets withthe intentto improve the company's own para-aramid fiberproductunder18 U.S.C .§ 18 32(a)(5) • *Disposition*:Sentenced to pay an **$85 million fine**,**$275 million in restitution** and to serve a**five year term of corporate probation**[14] • *Civil Case* • Complaintalleges aSouthKorean company attempted to obtain and use DuPont's confidentialand proprietary manufacturingprocess forKevlar® technology forits own products and processes • *Disposition*:The parties agreed to settle,and the case was dismissed. Kolon agreed to make up-frontand ongoingpayments to DuPont. Additionaldetails of the settlement agreementare confidential.[15]
8	Chemicalformulas used in the manufacture of silicone-based and rubberproducts	WackerChemical Corporation,located in Michigan	Chemical	• *Criminal case* • *Conviction:* Defendantpled guilty to one countof theftof trade secrets under18 U.S.C .§ 18 32(a)(3)for transmittingand disclosingmore than 100 confidentialchemical formulas to aSouthKorean-based chemicalcompany • *Disposition*:Sentenced to **24 months** in prison and a**$7,500 fine**[16]
9	Technicaldrawings, software,and tools forpost-tensioning materials for buildings and foundations	SuncoastPost-Tension, Ltd.	Construction	• *Civil case* • Texas federaljury awarded $24.5 million to Suncoast. • $13.5 million in punitive damages $8 million in compensatory damages,and $3 million for infringingSuncoast's copyrights drawings. • FormerSuncoastemployee headed new competitor.Suncoastlearned from aclientthatcompetitorwas usingits copyrighted drawings and installation drawings.[17]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
10	Collection of confidential information regarding executives, companies,and priorsearch engagements	Kerry/Ford,located in California	Executive Recruiting	• *Criminal case* • *Conviction:* Californiafederaljury found aformerKerry/Ford employee guilty of conspiracy to misappropriate trade secrets,and unauthorized receipt,possession, and duplication of trade secrets in violation of 18 U.S.C .§ 37 1.[18] • Sentenced to **12 months and 1 day in prison**,and ordered to pay a **$60,000 fine** and **$827,983 in restitution**.[19] • Note:case is currently on appealat the NinthCircuit
11	Highfrequency tradingstrategy and infrastructure source code and the data outputpredictions aboutinvestment movements from algorithms analyzingmarket data	Citadel,LLC ,located in Illinois,and "Company A,"located in New Jersey	Financial Institution	• *Criminal case* • *Conviction:* Formeremployee pled guilty to unlawfulpossession and transmission of trade secrets belongingto his formeremployerin violation of 18 U.S.C .§ 18 32(a)(2) and (a)(3).[20] • Sentenced to **36 months in prison**, and ordered to pay **$759,649 in restitution**.[21]
12	Computerized customerlists, information,and related notes[22]	Fireworks Spectacular, Inc.,and Piedmont Display Fireworks,Inc., bothlocated in Kansas	Fireworks	• *Civil case* • *Disposition*:Defendants were acquitted of breachof non-compete agreementand breach of fiduciary duty,butwere found guilty of misappropriatingtrade secrets, specifically Plaintiff's customer information[23]
13	Information regardinggas and oilwells,including seismic data, geologicalmaps, and reserves reports	LexMac Energy LP , and Novu s Operating Co.LP ,located in NorthDakota[24]	Gas and Oil	• *Civil case* • *Disposition*:8 thCircuitupheld districtcourt's findingthat Defendants misappropriated Plaintiffs'trade secrets related to oil and gas wells.Defendants were provided the information as collateralon aloan to lease the wells,butwere inappropriately disclosed when Plaintiffs defaulted on the loan.[25]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
14	Marketresearchin the form of P owerP oint presentations on consumerbehavior in the greetingcards market.[26]	HallmarkCards Inc., located in Missouri	Greetingcards	• *Civil case* • *Disposition*:Jury found defendant corporation guilty of misappropriatingplaintiff's trade secrets.Jury awarded **$21.3 million in compensatory damages** forthe trade secretviolation based on an assessmentof whatdefendant would have paid foruse of the misappropriated trade secrets.Jury also awarded **$10 million in punitive damages**.The jury also found the individualco-defendant guilty and awarded **$125,000 in punitive damages** againsthim.[27] • 8 thCircuitupheld the award .[28]
15	Customer information stored in adatabase allowingforsorting and manipulation[29]	American Family MutualInsurance C o., located in Wisconsin[30]	Insurance	• *Civil case* • *Disposition*:parties settled priorto finaldisposition of the litigation[31]
16	Packaging materials and processes regardingatamper proof retractable non-reu sable syringe.[32]	Retractable Technologies,Inc., located in Texas	Medica l Device	• *Civil case* • *Disposition*:Jury found defendant corporation guilty of misappropriatingplaintiff's trade secrets.Ju ry award ed **$2,240,640 in compensatory damages** forthe trad e secretviolation.[33]
17	Information regardingthe design and manufacturing of adisposable pen injector.[34]	Becton,Dickinson and Company,located in New Jersey	Medica l Device	• *Criminal case* • *Conviction*:Defendantpled guilty to two counts of theftof trade secrets under18 U.S.C .§ § 18 32(a)(1),(a)(4). • *Disposition*:Courtordered the defendantto pay a**$200 fine, $32,454 in restitution** and a sentence of **18 months in prison**.[35]
18	An epoxy-based intumescent fireproofingmaterial used in paint products known as "Chartek"	InternationalPaint, located in Texas and incorporated in Kentucky[36]	PaintIndustry	• *Criminal case* • *Conviction:* Defendantpled guilty to possessingaprocess formula trade secretformulato produce and/orsellin Chinaunder§ 18 32(a)(3) • *Disposition:* Sentenced to **12 months** and 1 day in prison[37]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
19	Formulafor nutritional supplement.	NuScience Corporation, located in California	Nutritional Supplements	• *Civil case* • *Alleged Conduct*:Defendants alleged to be usingformulathat belongs to NuScience. • *Disposition:* Defaultjudgment entered and NuScience awarded $600,000,plus $15,600 in attorneys' fees and $1,7 7 7 in othercosts.[38] Defendants also take down online statements they know the ingredients and formulaforthe NuScience's "oxygen +nutrient" supplement.
20	Process for manufacturing chloride-route titanium dioxide,a paintpigment	E.I.DuPontNemours & Co.,headquartered in Delaware,butwith plants in the United States,Mexico,and Taiwan	PaintIndustry	• *Criminal case* • *Conviction*:the main defendant (Liew)was found guilty by ajury of attemptand conspiracy to commiteconomic espionage under 18 U.S.C .§ 18 31(a)and of attempt and conspiracy to committheftof trade secrets and actualpossession and conveyingof trade secrets under18 U.S.C .§ 18 32(a).Liew's co-conspirator(Maergle)was also found guilty by ajury of conspiracy to committheftof trade secrets and conveyingtrade secrets under18 U.S.C .§ 18 32(a)(2). • *Disposition:* main defendant sentenced to **180 months** in prison and **restitution of $511,487**.Other defendantsentenced to **30 months** in prison and **restitution of $367,679**[39]
21	Confidential information about"a process forapplying hard coatings to the laminate contact surfaces of caul plates."[40]	WilsonartInternational, Inc.,located in Michigan	PaintIndustry	• *Criminal case* • *Disposition*:6thCircuitaffirmed the districtcourt's denialof Defendant's motion to dismiss, findingthatthe definition of atrade secretunder18 U.S.C .§ 18 32 was notunconstitutionally vague as to Defendantsince Defendantadmits he soughtto sellinformation thathe knew was proprietary[41]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
22	Confidentialand proprietary information related to the railroad freightbu siness[42]	SierraRailroad C o., located in California	Railroad	• *Civil case* • *Disposition*:Jury found railroad company liable for misappropriatingplaintiff's trade secrets and awarded $4.28 2M in lostprofits and $18 M in loss of business value,plus $14.68 1M in unjustenrichment,fora**total damages award of $22.282M.**[43] The confidentialinformation was originally provided in furtherance of an acquisition.[44] • Note:case is currently on appealat the NinthCircuit
23	Semiconductor manufacturing methods	Taiwan Semiconductor Manufacturing(TSMC)	Semiconductor manufacturing	• *Civil case* • SemiconductorManufacturing International(SMIC),TSM C 's Chinese rival,misappropriated trade secrets—theftoccurred in China • Manufacturingtechnology used in fabricatingchips on silicon wafers • *Disposition*:Followingajury verdicton liability in favorof TSMC ,SMIC agreed to pay $200 million in cashand approximately $130 million of its company stock.[45]
24	Detailed customer information, includingcustomer productpricingand customer preferences	ATIIndustrial Automation,Inc., located in North Carolina	Technology	• *Civil case* • *Disposition*:Courtgranted ajoint motion forimpoundmentand sealingof documents and deposition testimony due to the fact thatsaid materials contained the Plaintiff's trade secrets.The parties ultimately reached an undisclosed settlementagreement.[46]
25	Designs of memory macros forcomputer chips	UniRAM Technology, Inc.,located in California	Technology	• *Civil case* • *Disposition*:Jury found defendant corporation guilty of misappropriatingthe plaintiff company's trade secrets,obtained while consultingforplaintiff as a manufacturingpartner.The district courtjudge entered judgment againstdefendant,butultimately the parties settled priorto appeal.[47]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
26	Detailed customer information and contractual information	AkamaiTechnologies, located in Massachusetts	Technology	• *Criminal case* • *Conviction*:Defendantpled guilty to one countof foreign economic espionage under18 U.S.C .§ 18 31 forstealinghis employer's customerand contractual information and transmittingitto whathe thoughtwas,an Israeli agent. • *Disposition*:Sentenced to **1 year** imprisonment(6 months in prison and 6 months in home confinement)and a**$25,000 fine**[48]
27	Design and manufacturing processes for computer microprocessors	TransmetaCorporation and Sun Microsystems, bothlocated in California	Technology	• *Criminal case* • *Conviction:* Defendants pled guilty to stealingtrade secrets withthe intention of benefitingthe P RC ,in violation of 18 U.S.C .§ § 18 31(a)(2),(3). • *Disposition:* Sentenced to **1 year and 1 day** in prison.[49]
28	Source code for proprietary trading strategies and forecasting software[50]	Quantlab Technologies Ltd.,located in Texas	Technology	• *Civil case* • *Disposition*:Courtfound defendants (aformerQ uantlab employee and an entrepreneur) liable formisappropriation of trade secrets and conspiracy to misappropriate trade secrets.[51] A jury then determined the appropriate damages award was: **$7.2M** againstthe entrepreneurand **$5M** againstthe employee.[52] • Note:Defendant's motion for Judgmentas aMatterof Law is still pending.
29	Algorithm outlining how to implementa solution to compare differentvehicles withdifferently name features; database schema describinghow the dataused in the software is arranged[53]	AutodataSolutions Company and Autodata Solutions,Inc.,located in Texas[54]	Technology	• *Civil case* • *Disposition*:Jury found that Autodataproved its counterclaim thatVersatamisappropriated its trade secrets,and awarded **$2 million in damages**.[55]

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
30	(1)technical information re. networkingproducts (e.g.source code; performance capabilities, constraints,and challenges;product developmentplans); (2)customerand marketing information (e.g. customers'unique needs,attitudes, constraints, experiences;terms of agreements; customers'key personnel); (3)employee information (e.g. skilllevels, experience, specialties,attitudes, performance attributes, compensation levels)[56]	Brocade Communications Systems,Inc.,located in California	Technology	• *Civil case* • *Disposition*:Jury found thatA 10 misappropriated Brocade's trade secrets,butawarded damages of just$1.00.The jury also found A 10 liable forpatentinfringement, copyrightinfringement,and intentionalinterference with contract.[57] The parties ultimately agreed to astipulated judgmentfor $7 5 million.[58]
31	Automated website anti-abuse technology aimed at analyzingdataand shuttingdown abusive websites[59]	Afilias PLC,located in Dublin Ireland,with subsidiaries located in the US and Canada	Technology	• *Civil case* • *Disposition*:Jury found defendant corporation guilty of misappropriatingplaintiff's trade secrets.Jury awarded **$5 million in compensatory damages** forthe trade secretviolation,foratotal award of $10 million.[60] • Note:Defendant's motion for Judgmentas aMatterof Law is still pending

No.	Trade Secret	Trade Secret Owner	Industry	Conduct and Case Disposition
32	Technology "incorporating tunneling magnetoresistance (TMR)into read heads [to] allow for improved storage capacity on hard diskdrives."[61]	Seagate Technology, LLC	Technology	• *Civil case* • *Disposition*:Arbitratorfound thata formeremployee and his new employermisappropriated plaintiff's trade secrets.A s a sanction forfabricatingevidence of public dissemination of the trade secrets,the arbitratorprecluded defendants from disputingthe validity ormisappropriation of the trade secrets.[62] Arbitratorawarded **$525 million in compensatory damages** based on the unjust enrichmentmethod,plus approximately **$109 million in pre- and post-judgment interest**.[63] • The MinnesotaSupreme Court upheld the award.[64]
33	Design forcomputer memory chips	GrailSemiconductor Inc	Technology	• *Civil case* • *Alleged Conduct*:Mitsubishi Electric & Electronics USA Inc breached an NDA withGrail.Grail entered into ND A withMitsubishi to discuss Grail's designs forsmall, efficientmemory chips in the hopes of gettingMitsubishito invest. Grailtested new chiplaunched by Mitsubishisubsidiary and found it contained secretfeatures.[65] • *Disposition:* Jury **awarded $124 million**.The courtordered anew trialon damages because the award was apparently miscalculated by the jury.The parties settled before the new trial.
34	Price lists, advertisingplans, unreleased product attributes	MGA Entertainment, Inc.,located in California	Toy (Bratz Dolls)	• *Civil case* • *Alleged Conduct*:MGA claims Mattelhad an 11-page "how to steal"manualon the trade secrets of competitors. • *Disposition:* $8 5M in compensatory and $8 5M in punitive damages—latervacated by 9thCircuitdue to lackof federaljurisdiction.Retried in Cal.State Courtseeking$1B .[66]
35	Wind turbine technology used to regulate the flow of electricity (including proprietary software forthe Low Voltage Ride Through system)	AM SC ,located in Wisconsin, Massachusetts,and Austria	Wind turbine	• *Criminal case* • *Alleged Conduct*:Charges allege a conspiracy to obtain copyrighted information and trade secrets. • *Disposition:* Case remains pending.[67]

[1] Third SupersedingIndictment,*United States v. Li Shaoming*,No.13-CR-00147 (S.D .IowaOct.28 ,2015)(ECF No.47 9).

[2] Third SupersedingIndictment,*United States v. Li Shaoming*,No.13-CR-00147 (S.D .Iowa Oct.28 ,2015)(ECF No.47 9);*see also* Press Release,U.S.D ep'tof Justice,Six Chinese Nationals Indicted ForConspiringTo Steal Trade Secrets From U.S.Seed Companies (D ec.19,2013),http://www.ju stice.gov/usao-sdia/pr/six-chinese-nationals-indicted-conspiring-steal-trade-secrets-us-seed-companies.

[3] Indictment,at1,*United States v. Huang*,No.10-CR-0102 (S.D .Ind.June 16,2010)(Doc 1).

[4] SentencingHearingTranscript,at17 ,*United States v. Kexue Huang*,No.10-CR-0102 (S.D .Ind.Dec.22,2011)() (testimony of Dow AgroSciences managingcounselsummarizinginvestigation);Judgment,*United States v. Kexue Huang*,No.10-CR-0102 (S.D .Ind.Mar.6,2012)(ECF No.107);*see also* Press Release,U.S.D ep'tof Justice, Chinese NationalSentenced to 8 7 Months in Prison forEconomic Espionage and Theftof Trade Secrets (D ec.21, 2011),http://www.ju stice.gov/opa/pr/chinese-national-sentenced-8 7 -months-prison-economic-espionage-and -theft-trade-secrets.

[5]*United States v. Lange*,312 F.3d 263 (7 thCir.2002)(affirmingbenchtrialconviction);HearingMinutes,*United States v. Matthew R. Lange*,No.2:99-CR-0017 4 (E.D .Wis.Mar.2,2000)(ECF No.34).

[6] Indictment,*United States v. Shanshan Du & Yu Qin*,No.10-CR-20454 (E.D .Mich.July 22,2010)(ECF No.3).

[7] Judgments,*United States v. Shanshan Du & Yu Qin*,No.10-CR-20454 (E.D .Mich.May 9,2013)(D ocs.214, 215);*see also* Press Release,FBI,Two Convicted in Conspiracy to StealGM Trade Secrets Sentenced to Prison (April30,2013),http://www.fbi.gov/detroit/press-releases/2013/two-convicted -in-conspiracy-to-steal-gm-trade-secrets-sentenced -to-prison.

[8] *United States v. Shanshan Du & Yu Qin*,Nos.13-1606,13-1607 ,13-17 7 8 ,13-17 8 1 (6thCir.June 26,2014) (unpublished),http://www.ca6.u scourts.gov/opinions.pdf/14a0458 n-06.pdf.

[9] P leaAgreement,*United States v. Lewis*,No.5:14-CR-00014 (E.D .Ky.Mar.3,2014)(ECF No.7).

[10] Government's SentencingMemorandum,*United States v. Lewis*,No.5:14-CR-00014 (E.D .Ky.Oct.8 ,2014) (ECF N o.19);Judgment(E.D .Ky.Oct.8 ,2014)(ECF No.21);*see also* Press Release,U.S.D ep'tof Justice, FormerWinchesterBrake P ad EngineerPleads Guilty To TheftO f Trade Secrets Charge (March5,2014),*available at* http://www.justice.gov/u sao-edky/pr/former-winchester-brake-pad-engineer-plead s-guilty-theft-trade-secrets-charge.

[11] *United States v. Williams*,526 F.3d 1312 (11thCir.2008)(affirmingconviction and sentence;concluding"the districtcourtdid noterrby considering"Coca-Cola's annualrevenues "in decidingwhetherthe $1.5 million intended loss calculated underthe guidelines underrepresented the seriousness of the offense");*see also* Judgment, *United States v. Williams*,No.06-CR-00313-03-JOF (N .D .GaMay 23,2007)(ECF No.137).

[12] Judgment,*United States v. Dimson*,No.06-CR-00313-01-JOF (N .D .Ga.May 23,2007)(ECF No.136).

[13] DocketMinute Entry,*United States v. Duhaney*,No.06-CR-00313-02-JOF (ND GA June 5,2007)(ECF No.146).

[14] OrderImposingCriminalFine,*United States v. Kolon Industries, Inc.*,No.12-CR-00137 (E.D .Va.April30, 2015)(ECF No.195);Restitution Order(E.D .Va.April30,2015)(ECF No.194);Pleaagreementat¶¶ 19-20 (E.D . Va.April30,2015)(restitution & fine)(ECF No.191);Judgment(E.D .Va.May 1,2015)(ECF No.196);*see also* Press Release,U.S.D ep'tof Justice,Kolon Industries Inc.Pleads Guilty forConspiringto StealDuPontTrade Secrets InvolvingKevlarTechnology (Apr.30,2015),http://www.ju stice.gov/opa/pr/kolon-industries-inc-plead s-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

[15] Complaint,*E. I. du Pont de Nemours and Company v. Kolon Industries Inc.*,No.09-CV-00058 (E.D .Va.Feb.3, 2009)(ECF No.1);Dismissal,(E.D .Va.May 27 ,2015)(ECF No.3056);*see also* Press Release,DuPont,DuPont and Kolon Settle Trade SecretLitigation (Apr.30,2015),*available at* http://investors.dupont.com/investor-relations/investor-news/investor-news-details/2015/DuP ont-and-Kolon-Settle-Trade-Secret-Litigation/default.aspx.

[16] P leaAgreement,atFactualBasis ¶ 1(C),*United States v. Agodoa*,No.13-CR-20525 (E.D .Mich.Sept.25,2013) (ECF N o.No.22);Judgment(E.D .Mich.Jan.17 ,2014)(ECF No.29);*see also* Press Release,U.S.D ep'tof Justice,Michigan Man Sentenced ForStealingTrade Secrets (Jan.16,2014),*available at* **Error! Hyperlink reference not valid.**http://www.justice.gov/u sao-edmi/pr/michigan-man-sentenced-stealing-trade-secrets

[17] *Suncoast Post-Tension Ltd. v. Scoppa et al.*,No.4:13-cv-03125 (S.D .Tex.2015).

[18] Amended Judgment,*United States v. Nosal*,No.08 -cr-00237 -EMC (N .D .Cal.May 30,2014)(ECF No.552); Second SupersedingIndictment,*United States v. Nosal*,No.08 -cr-00237 -EMC (N .D .Cal.Feb 28 ,2013)(ECF No. 309).

[19] Amended Judgment,*United States v. Nosal*,No.08 -cr-00237 -EMC (N .D .Cal.May 30,2014)(ECF No.552);*see* appealinformation atNo.14-10037 (9thCir.2015)and No.14-1027 5 (9thCir.2015).

[20]P leaAgreement,*United States v. Pu*,No.11-cr-00699 (N .D .Ill.Aug7 ,2014)(ECF No.17 5).

[21]Judgment,*United States v. Pu*,No.11-cr-00699 (ND IL Jan 15,2015)(ECF No.206).

[22] *Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc.*,147 F.Supp.2d 1057 (D .Kan.May 17 ,2001).

[23] *Id*.

[24] Judgment,*LexMac Enery , L.P. v. Macquarie Bank Ltd.*,No.4:08 -CV-00048 (D .N .D .Jan.7 ,2014)(ECF No. 333).

[25] *Macquarie Bank Limited v. Bradley D. Knickel et al.*,No.14-1684 (8 thC ir.July 17 ,2015).

[26] *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*,No.13-1905 (8thCir.July 15,2014).

[27] Jury VerdictForm, *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*,No.08 -cv-00 8 40 (W .D .Mich.,Nov. 19,2012)(ECF No.527);*see also* Judgment,*Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*,No.08 -cv-008 40 (W .D .Mich.,Nov.20,2012)(ECF No.526);Judgment,*Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*,No.08 -cv-008 40 (W.D .Mich.,Mar.20,2013)(ECF No.58 8)

[28] Judgment, *Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC*,No.13-1905 (8 thCir.July 15,2014).

[29] *Am. Family Mut. Ins. Co. v. Roth*,48 5 F.3d 930 (7 thCir.May 7 ,2007).

[30] Complaintat2,*Am. Family Mut. Ins. Co. v. Roth*,No.05-cv-038 39 (N.D .Ill.June 30,2005),ECF No.1.

[31] Notification of DocketEntry,*Am. Family Mut. Ins. Co. v. Roth*,No.05-cv-038 39 (N .D .Ill.Jan.31,2011),ECF No.400.

[32] Amended Complaint,*Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*,No.08 -cv-00120 (E.D . Tex.May 13,2009),ECF No.8 4;OrderDenyingDefendant's Judgmentas aMatterof Law, *Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*,08 -cv-00 120 (E.D .Tex.Aug.11,2010),ECF No.268 .

[33] Jury VerdictForm,*Retractable Techs., Inc. vs. Occupational & Med.Innovations, Ltd.*,No.08 -cv-00 120 (E.D . Tex.Dec.18 ,2009),ECF No.228 ;OrderDenyingDefendant's Judgmentas aMatterof Law,*Retractable Techs., Inc. vs. Occupational & Med. Innovations, Ltd.*,No.08 -cv-00 120 (E.D .Tex.Aug.11,2010),ECF No.268 .

[34] Complaint,*United States v. Maniar*,No.13-CR-0608 5 (D .N .J.June 4,2013),ECF No.1.

[35] PleaAgreement,*United States v. Maniar*,No.13-CR-0608 5 (D .N .J.May 28 ,2014),ECF No.22;Judgment, *United States v. Maniar*,No.13-CR-0608 5 (D .N .J.Oct.16,2014),ECF No.27 .

[36] Indictment,*United States v. Zeng*,No.08 -CR-0007 5 (S.D .Tex.Jan.22,2008),ECF No.1.

[37] P leaAgreement,*United States v. Zeng*,No.08 -CR-0007 5 (S.D .Tex.May 16,2008),ECF No.30;Judgment, *United States v. Zeng*,No.08 -CR-0007 5 (S.D .Tex.May 22,2008),ECF No.33;*see also* Press Release,U.S.D ep't of Justice,Chinese ChemistConvicted In TheftO f Trade Secrets (May 16,2008), http://www.ju stice.gov/archive/criminal/cybercrime/press-releases/2008 /zengConvict.pdf.

[38] *NuScience Corp. v. Henkel*,No.2:08 -cv-02661 (C .D .Cal.2009).

[39] Judgment,*United States v. Liew*,No.11-CR-0057 3 (N .D .Cal.Aug.28 ,2014),ECF No.921;Judgment,*United States v. Liew*,No.11-CR-0057 3 (N .D .Cal.Sep.2,2014),ECF No.924;*see also* Press Release,U.S.D ep'tof Justice,WalterLiew Sentenced to 15 Years in Prison forEconomic Espionage (July 11,2014), http://www/ju stice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage.

[40] *United States v. Krumrei*,258 F.3d 535,536 (6thC ir.2001).

[41] *Id*.at539.

[42] CounterClaim,*Patriot Rail Corp. v. Sierra R.R. Co.*,No.09-CV -00009 (E.D .Cal.Apr.2,2010),ECF No.65, *appeal docketed*,No.15-1658 7 (9thCir.Aug.7 ,2015).

[43] Jury Verdict,*Patriot Rail Corp. v. Sierra R.R. Co.*,No.09-CV-00009 (E.D .Cal.Mar.28 ,2014),ECF No.447 , *appeal docketed*,No.15-1658 7 (9thCir.Aug.7 ,2015);*see also* Entry of Judgment,*Patriot Rail Corp. v. Sierra Railroad Co.*,No.09-CV-00009 (E.D .Cal.Oct.31,2014),ECF No.532,*appeal docketed*,No.15-1658 7 (9thC ir. Aug.7 ,2015).

[44] CounterClaim,*Patriot Rail Corp. v. Sierra R.R. Co.*,No.09-CV -00009 (E.D .C al.),ECF No.65,*appeal docketed*,No.15-1658 7 (9thC ir.Aug.7 ,2015).

[45] *TSMC N. Am. et al. v. SMIC Ams. et al*.,No.RG06-28 6111 (Cal.Super.Ct.AlamedaCounty).

[46] OrderSealingDocuments at15–16,*ATI Indus. Automation, Inc. v. Applied Robotics, Inc.*,No.09-CV-0047 1 (July 12,2011),ECFNo.84.

[47] Entry of Judgment,*UniRAM Tech., Inc. v. Taiwan Semiconductor Mfg. Co.*,No.04-CV-0 1268 (N .D .Cal.Apr. 17 ,2008)(ECF No.628).

[48] PleaAgreement,*United States v. Elliot Doxer,* No.111-CR-10268 (D .Mass.July 20,2011)(ECF No.19); SentencingHearingTranscriptat5-8 ,9-10,15 (D .Mass.Dec.21,2011)(ECF No.29);*see also* Press Release,U.S. D ep'tof Justice,Employee of HighTechnology Company Charged withSeekingto Provide ConfidentialBusiness Information to aForeign Government(O ct.6,2010),*available at* http://www.ju stice.gov/archive/usao/ma/news/2010/O ctober/D oxerElliotPR.html.

[49] Judgment, *United States v. Fei Ye, et al.*,No.02-CR-20 145 (N .D .Cal.Nov.25,2008)(ECF No.268);Judgment, *United States v. Fiy Ye, et al.*,No.02-CR-20145 (N .D .Cal.Nov.25,2008)(ECF No.27 0);*see also* Press Release, U.S.Dep'tof Justice,Two Men Plead Guilty to StealingTrade Secrets from Silicon Valley Companies to Benefit China(D ec.14,2006),*available at* http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/yeP lea.htm.

[50] Complaint,*Quantlab Technologies Ltd. v. Godlevsky, et al.*,No.4:09-CV-04039 (S.D .Tex.Dec.18 ,2009)(ECF No.1);*see also* Third Amended Complaint,*Quantlab Technologies Ltd. v. Godlevsky, et al.*,No.:09-CV-04039 (S.D .Tex.July 21,2014)(ECF No.533).

[51] Order,*Quantlab Technologies Ltd. v. Godlevsky, et al.*,No.04-CV-04039 (S.D .Tex.July 21,2014)(ECF No. 7 25).

[52] JuryVerdict,*Quantlab Technologies Ltd. v. Godlevsky, et al.*,No.14-CV-04039 (S.D .Tex.May 20,2015)(ECF No.7 61);*see also* Quantlab's Motion forEntry of FinalJudgment,*Quantlab Technologies Ltd. v. Godlevsky, et al.*, No.04-CV-04039 (S.D .Tex.July 2,2015)(ECF No.7 8 6).

[53] Memorandum Opinion and Order,*Versata Software, Inc. v. Internet Brands, Inc.*,No.08 -CV-00313 (E.D .Tex. Oct.9,2012)(ECF No.37 1).

[54] Complaint,*Versata Software, Inc. v. Internet Brands, Inc.*,No.08 -CV-00313 (E.D .Tex.Aug.8 ,2008)(ECF No. 1).

[55] Memorandum Opinion and Order,*Versata Software, Inc. v. Internet Brands, Inc.*,No.08 -CV-00313 (E.D .Tex. Oct.9,2012)(ECF No.37 1).

[56] Third Amended Complaint,*Brocade Communications Systems, Inc. v. A10 Networks, Inc.*,No.10-CV-03428 (N .D .Cal.Apr.29,2011)(ECF No.8 5).

[57] Jury Verdict,*Brocade Communications Systems, Inc. v. A10 Networks, Inc.*,No.10-CV-03428 (N .D .Cal.Aug.6, 2012)(ECF No.7 7 1).

[58] Stipulated FinalJudgment,*Brocade Communications Systems, Inc. v. A10 Networks, Inc.*,No.10-CV-03428 (N .D .Cal.June 7 ,2013)(ECF No.1026).

[59] Complaint, *Afilias PLC v. Architelos, Inc.*,15-cv-00014 (E.D .Va.Jan.5,2015)(ECF No.1).

[60] JuryVerdict, *Afilias PLC v. Architelos, Inc.*,15-cv-00014 (E.D .Va.Aug.24,2015)(ECF No.240).

[61] Furtherdetails regardingthe specific trade secrets were notmade public.*Seagate Technology, LLC v. Western Digital Corp.*,8 54 N .W .2d 7 50,7 54 (Minn.2014).

[62] *Seagate Technology, LLC v. Western Digital Corp.*,8 54 N .W .2d 7 50,7 54-56 (Minn.2014).

[63] *Seagate Technology, LLC v. Western Digital Corp.*,8 34 N .W .2d 555,559 (Minn.Ct.App.2013).

[64] *Seagate Technology, LLC v. Western Digital Corp.*,8 54 N .W .2d 7 50,7 67 (Minn.2014).

[65] *Grail Semiconductor Inc. v. Mitsubishi Electric & Electronics USA Inc. et al.*,No.1-07 -CV -098 590 (C al.Sup.Ct July 24,2012).

[66] Complaint,*MGA Entertainment, Inc. v. Mattel, Inc.*,No.B C5327 08 ,(C al.Sup.Ct.Jan.13,2014)(Complaintfor Trade SecretMisappropriation).

[67] Indictment,*United States v. Sinovel Wind Group Co., Ltd., et al*,No.13-CR-8 4 (W .D .Wis.June 27 ,2013)(ECF No.25);*see also* Press Release,U.S.D ep'tof Justice,SinovelCorporation and Three Individuals Charged in Wisconsin withTheftof Amsc Trade Secrets (June 27 ,2013),http://www.ju stice.gov/opa/pr/sinovel-corporation-and-three-individuals-charged-wisconsin-theft-amsc-trade-secrets.

Appendix C

Military Application Trade Secret Examples

Based on Recent Criminal and Civil Cases

Appendix C
Military Application Trade Secret Examples
Based on Recent Criminal and Civil Cases

No.	Military Application Trade Secret	Trade Secret Owner	Conduct and Case Disposition
1	Visual simulation source code and software for military aircraft training	Quantum3D, located in California	• *Criminal case* • *Conviction:* Defendant pled guilty to foreign economic espionage under 18 U.S.C. § 1831(a)(3) for possessing a stolen trade secret with the intent to benefit a foreign government, and for violating the Arms Export Control Act under 22 U.S.C. §§ 2778(b)(2), 2778(c) for exporting a defense article without obtaining a license to do so by the Department of State • *Disposition:* Defendant sentenced to **24 months and one day in prison** and **$10,200 fine**[1]
2	Phased array antenna project for the space shuttle and two documents concerning the Delta IV Rocket, a booster rocket designed to launch manned space vehicles	Rockwell International and Boeing, located in California	• *Criminal case* • *Conviction:* Former Rockwell International and Boeing engineer convicted in a bench trial on six counts of foreign economic espionage under 18 U.S.C. §§ 1831(a)(3), as well as one count of conspiring to commit economic espionage, one count of acting as an unregistered foreign agent, and one count of making a false statement to federal agents • *Disposition*: Sentenced to serve **188 months** in prison[2]
3	Designs, mechanical parts and hardware for the manufacture and testing of detector logarithmic video amplifiers and successive detection logarithmic video amplifiers, which are microwave technology components used to enhance navigation, radar jamming, and locating enemy signals during warfare"[3]	Genesis Microwave, Inc., located in California	• *Criminal case* *Conviction:* Defendant pled guilty to stealing, downloading, and possessing trade secret under 18 U.S.C. § 1832 • *Disposition:* Defendant sentenced to **24 months** in prison and ordered to pay **$15,000 in restitution**[45]

4	A systems architecture document (a teaching instrument) for an iDEN cellular communication network, a white paper analyzing features for said network, and an interface control document to catalog messages used between network elements.[6]	Motorola, based in Illinois	• *Criminal case* • *Conviction*: Defendant was convicted in a bench trial on three trade secret counts under 18 U.S.C. § 1832 for stealing, downloading, and possessing trade secrets from her employer, but was acquitted on the three charges under 18 U.S.C. § 1831 due to reasonable doubt that she intended to benefit the PRC in any way • *Disposition*: Defendant sentenced to **48 months** in prison and ordered to pay **$20,000 fine**[7]
5	$2 billion worth of trade technical details and manuals related to the F-35 Joint Strike Fighter program and its engines and other military jet engines. U.S. Customs and Border Control officials discovered the documents in California in 11 crates bound for Iran.[8]	Multiple defense contractors, including Pratt & Whitney and Rolls Royce	• *Criminal case* • *Conviction*: Defendant pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S. in violation of the Arms Export Control Act. • *Disposition*: Defendant sentenced to **97 months** in prison and ordered to pay **$50,000 fine**[9]

[1] Redacted Plea Agreement, *United States v. Meng*, No. 04-CR-20216-JF (N.D. Cal. Aug. 1, 2007) (ECF No. 76); Judgment (N.D. Cal. June 24, 2008) (ECF No. 103); *see also* Press Release, U.S. Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html.

[2] *United States v. Chung*, 633 F. Supp. 2d 1134 (C.D. Cal. 2009) (Memorandum of Decision), *aff'd*, 659 F.3d 815 (9th Cir. 2011) (affirming conviction and sentence); Judgment, *United States v. Chung*, No. 8:08-CR-00024 (C.D. Cal. Feb. 11, 2010) (ECF No. 172); *see also* Press Release, U.S. Dep't of Justice, Former Boeing Engineer Sentenced To Nearly 16 Years In Prison For Stealing Aerospace Secrets For China (Feb. 8, 2010), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/chungSent.pdf..

[3] Plea Agreement Factual Basis for Plea, *United States v. Cotten*, No. 08-CR-00042-EJG (E.D. Cal. Feb. 29, 2008) (ECF No. 9).

[4] Plea Agreement, *United States v. Cotten*, No. 2:08-CR-00042-EJG (E.D. Cal. Feb. 29, 2008) (ECF No. 9); Judgment, *United States v. Cotten*, No. 08-CR-00042-EJG (EDCA May 21, 2008) (ECF No. 13).

[6] *United States v. Jin*, 833 F. Supp. 2d 977, 995-998 (N.D. Ill. 2012).

[7] *Id*. at 977; *United States v. Jin*, 733 F.3d 718, 718 (7th Cir. 2013).

[8] Affidavit to Complaint, *United States v. Khazaee*, No. 3:14-cr-00009 (D. Conn. 2015) (ECF No. 1).

[9] Judgment, *United States v. Khazaee*, No. 3:14-cr-00009 (D. Conn. 2015) (ECF No. 89).