Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

ECONOMIC ESPIONAGE

The author traces the kinds of prosecutions brought over the 16 years since enactment of the Economic Espionage, and he offers tips for its effective implementation in the years to come.

An Analysis of Economic Espionage Act Prosecutions: What Companies Can Learn From It and What the Government Should Be Doing About It!

By Peter J. Toren

The author is a partner with Weissbrod Matteis and Copley, Washington, D.C. Before entering private practice, as a partner with Sidley Austin, New York, Toren was a federal prosecutor with the Computer Crime & Intellectual Property Section of the Justice Department. While at Justice, he was the lead prosecutor on a number of high-profile cases involving violations of the Economic Espionage Act, Computer Fraud and Abuse Act, and criminal copyright and trademark violations. He is also the author of Intellectual Property & Computer Crimes (Law Journal Press 2003). His website, www.Petertoren-.com, contains additional information on how companies can better protect their trade secrets.

I. Introduction

The Economic Espionage Act (EEA), 18 U.S.C. §§ 1831-91, was enacted 16 years ago to great fanfare and with the stated goal of better protecting critical U.S. corporate information from theft by foreign governments and unscrupulous competitors by criminalizing the theft of trade secrets. In signing the EEA, President Bill Clinton stated, ''The act establishes a comprehensive and systematic approach to trade-secret theft and economic espionage.''[1] Since then, the federal government has brought approximately 124 prosecutions under the two separate provisions of the EEA.

The United States has now brought a sufficient number of prosecutions under the EEA to be able to draw conclusions about: (1) the location of the cases; (2) the extent of foreign government involvement; (3) defendant's gender; (4) defendant's level of education; (5) relationship of defendant to the victim; (6) nationality of the defendant/purpose of the theft; (7) type of trade secrets stolen; (8) identify of the victim; (9) adequacy of protective measures; (10) dispositions; and (11) sentences.[2]

Based on these findings and conclusions, it is also possible to make meaningful conclusions and recommendations for both government and industry. With regard to the government, the findings suggest that it

[1] Statement by President William J. Clinton upon signing H.R. 2723, reprinted in 1996 U.S.C.C.A.N. 4034.

[2] This study is based on the first compilation of EEA prosecutions under the EEA, which was conducted by the author using a variety of sources including Pacer, Westlaw, the Department of Justice website, and other public sources.

 ISSN 0148-7965

should be more aggressive in prosecuting violations of the EEA if it were truly serious about deterring thefts of trade secrets, and that the government has not been as active as claimed. Further, there is marked difference among U.S. Attorney's Offices in the number of cases the office has charged under the EEA.

The effectiveness of the EEA in protecting trade secrets is also hampered by statutory limitations of the current version of the EEA. In particular, Congress should amend the EEA so that it unambiguously covers the theft of trade secrets to the extent permitted by the Commerce Clause, and that it also should protect trade secrets in the development stage. Finally, Congress should increase the penalties for theft of trade secrets not involving a foreign entity; more than 90 percent of the prosecutions, thus far, have not involved a foreign entity, and the defendant was sentenced to probation or home confinement in almost 40 percent of the cases.

With regard to industry, the findings indicate that companies are not doing enough to protect their valuable proprietary information and that the process of protecting trade secrets is organic, in that, all businesses should constantly update their trade secret protection programs in response to ever changing conditions and threats. For example, the threat of foreign economic espionage, especially by Chinese entities, has greatly increased over the past several years.

This article first discusses the background of the EEA. Based on a review and analysis of the approximate 124 EEA prosecutions brought by the government, it then provides a discussion of 11 specific findings, and makes conclusions and recommendations on how the government and industry can take steps to better protect trade secrets.

II. Background - The Economic Espionage Act

Prior to the passage of the EEA in 1996, there was only a single, very limited federal statute that directly prohibited the misappropriation of trade secrets.[3] As noted in the EEA's legislative history, problems with prosecuting the theft of trade secrets under federal criminal law led U.S. Attorney's Offices to decline matters that involved employees of U.S. corporations attempting to sell proprietary information to foreign governments.[4] Congress realized that the only practical way to protect the trade secrets of critical U.S. corporate information was to enact a single comprehensive scheme that could bring federal resources to bear against defendants who steal proprietary information.

The EEA criminalizes two distinct, but related types of trade secret misappropriation: Section 1831 punishes the misappropriation of trade secrets when knowingly undertaken by anyone ''intending or knowing that the offense will benefit any foreign government, foreign instrumentality or foreign agent.''[5] This was originally the heart of the EEA, and was designed to cope with the problem of foreign economic espionage.[6]

In contrast, Section 1832 is a general criminal trade secrets statute. Despite its inclusion in the EEA, it does not require evidence of foreign espionage. Rather, it applies to anyone who knowingly engages in any act of misappropriation ''with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret.''[7]

Defendants convicted of violating Section 1831 can be sentenced to up to 15 years imprisonment. In contrast, defendants convicted under Section 1832 can be sentenced to up to ten years imprisonment. Further, the statute carries a range of fines of up to $15,000,000 depending upon the nature of the offense. In addition to payment of fines, EEA violators are subject to the provisions of the Mandatory Victim's Restitution Act (''MVRA'').[8] Finally, the EEA requires mandatory forfeiture to the government of property used, or intended to be used, in any manner or part to commit or facilitate the offense, as well as any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of the offenses.[9]

Pursuant to the U.S. Sentencing Guidelines, the imposition of an actual sentence under the EEA is largely based on the determination of the value of the misappropriated property and the loss caused by the theft.

III. Government Prosecutions Under the EEA

1. Number and Location of Cases

Findings:

The government has brought a total of 124 cases. As seen from the following chart and contrary to the government's claims of increased prosecution of theft of trade secrets, the number of indictments has not dramatically increased since the enactment of the EEA. Indeed, the number of indictments from 2006-2011 was relatively flat and there were only five indictments in 2012 by Sept. 1, 2012.

[3] 18 U.S.C. § 1905. It provides, inter alia for misdemeanor criminal sanctions for the unauthorized disclosure of government information, including trade secrets, by a government employee.

[4] S.Rep. No. 104-359 at 10-11 (1996).

[5] 18 U.S.C. § 1831(a).

[6] *See* 142 Cong. Rec 12208 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

[7] 18 U.S.C. § 1832(a).

[8] 18 U.S.C. §§ 1834, 2323(c).

[9] 18 U.S.C. §§ 1834, 2323.

Year	1996	97	98	99	2000	01	02	03	04	05	06	07	08	09	10	11	12	Total
§ 1831	0	0	0	0	0	1	1	0	1	0	0	1	2	0	1	2	0	9
§ 1832	1	3	8	5	6	4	8	7	3	6	11	6	10	10	11	11	5	115

  PTCJ ISSN 0148-7965

Further, the prosecutions are not evenly distributed among the 94 U.S. Attorney's Offices. The U.S. Attorney's Office for the Northern District of California is the leader in the number of EEA prosecutions with a total of 24. This is three times the number of the next closest district; the Southern District of Texas, which has prosecuted eight cases. The Southern District of New York, Central District of California and Northern District of Ohio have each prosecuted seven EEA cases.

Other districts with five or more prosecutions, (the number of total prosecutions are in parentheses), include the Northern District of Illinois (5), the District of New Jersey (6), the District of Massachusetts (5) and the Eastern District of Michigan (6). Taken together, the nine districts with at least five prosecutions have accounted for over 60 percent of the prosecutions.

Offices with relative few prosecutions given the demographics of their jurisdiction include the District of Utah (Salt Lake City) (2), the Northern District of Georgia (Atlanta) (3), the Eastern District of Virginia (Washington, D.C., suburbs) (1), the Southern District of California (San Diego) (4), and the Western District of Washington (Seattle) (1). Offices with no prosecutions include, the Eastern District of New York (Brooklyn and Long Island), and the District of Minnesota (Minneapolis and St. Paul). Less than 45 percent of all districts have prosecuted a case under the EEA.

Conclusions/Recommendations:

The relatively limited number of prosecutions in any given year strongly suggests that the EEA is not acting as a deterrent against theft of trade secrets. This is especially true because recent studies suggest that enhancing the certainty of punishment produces a stronger deterrent effect than increasing the severity of the punishment.[10] Given the languid pace of the prosecutions, it is unlikely that individuals have an understanding that they will be apprehended and prosecuted for stealing trade secrets. In addition, the number of prosecutions is not increasing, despite evidence that the problem is getting worse. It is simply not on a person's radar screen that he will be apprehended and prosecuted for misappropriating trade secrets. This is especially true because more than half of the U.S. Attorney Generals have not obtained a single EEA indictment.

If the government is truly serious about deterring the theft of trade secrets as a way to increase the protection of trade secrets, especially the trade secrets of U.S. corporations, it must increase the number of cases it investigates and prosecutes. This will not be that easy to accomplish, especially in an era of limited financial resources.

This problem is exacerbated by the nature of a trade secret prosecution. In comparison with many other types of federal crimes, EEA investigations and prosecutions are more resource intensive and complex. Often they require the ability to understand complex technologies and science that is generally not part of a federal prosecutor's job description. Given these constraints, the FBI and U.S. Attorney's Offices may be reluctant to commit scarce resources to investigate and prosecute a single matter when the same effort could result in the prosecution and conviction of multiple other federal crimes.

This reluctance to prosecute EEA cases is reinforced by U.S. Attorney's Offices' internal prosecution guidelines that often disfavor prosecuting a case in which the victim may already have a civil remedy. The victim almost always has a civil remedy in a trade secret case.

It is recommended therefore that Justice should institute a policy that the availability of civil remedies in EEA cases should not be a disqualifying factor in whether to open an investigation and to prosecute. The possibility of deterring future thefts through aggressive prosecutions, in many instances, should be enough to overcome the factors disfavoring prosecution.

The government is not completely to blame for the relatively few prosecutions. The government can only investigate and prosecute such cases if the theft is reported to the government. Businesses are understandably reluctant to report when their valuable intellectual property has been stolen because of concerns that it will lead to additional thefts and adverse publicity. The government must be sensitive to these concerns and convince companies that, in the long run, reporting and prosecution will lead to increased protection through deterrence.

The bottom line is that government should work with industry to increase the number of referrals, thereby, increasing the pool of potential cases.

2. Section 1831/Section 1832

Findings:

The government has brought nine cases under Section 1831 as compared to approximately 115 cases under Section 1832. In other words, the government has alleged that the theft was intended to benefit a foreign government instrumentality or agent in less than 10 percent of the prosecutions. In addition, the government only recently charged a foreign entity for the first time under Section 1831.

In February 2012, the Department of Justice unsealed an indictment in California that charged that the Panang Group, a Chinese company with Chinese government ties, was behind the attempted theft of trade secrets from DuPont relating to the obscure, but valuable technology to produce titanium dioxide, a white pigment used in paints and other products.[11] DuPont had allegedly been successful in keeping the information secret for over 50 years by, in part, allowing most employees to know about only individual parts of the process. According to the indictment, Walter Liew, a Malaysian born naturalized U.S. citizen, over the course of 15 years hired several employees from DuPont knowledgeable about specific pieces of the titanium process. Liew's company allegedly received more than $12 million from a subsidiary of Panang between 2009 and 20111. One of the former DuPont engineers, Tze Chao, pleaded guilty and has agreed to cooperate with the government.

Conclusions

For a number of reasons, the fact that Section 1831 prosecutions comprise less than 10 percent of the total

[10] *See e.g., Deterrence in Criminal Justice, Evaluating Certainty vs. Severity of Punishment*, Valerie Wright, Ph.D., The Sentencing Project, November 2010.

[11] *United States v. Walter Lian-Heen Liew*, No. 11-CR-0573 (N.D. Cal.).

prosecutions under the EEA should not be the basis to conclude that the actual amount of foreign economic espionage is also less than 10 percent. For a number of reasons, the number of prosecutions under Section 1831 is likely to substantially understate the actual amount of foreign economic espionage.

First, it is more difficult for the government to establish foreign government involvement under Section 1831 than it is to establish a violation of Section 1832. As a practical matter, foreign government operatives are likely to be more skilled in stealing trade secrets and, thus, are less likely to be caught.

Second, Section 1831 punishes the misappropriation of trade secrets when knowingly undertaken by anyone ''intending or knowing that he offense will benefit any foreign government, foreign instrumentality or foreign agent.''[12] Foreign companies or individuals do not fall within the ambit of Section 1831 unless they are ''substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government.''[13] The intent of Section 1831 is to target foreign government action, not any act of espionage undertaken by a foreign corporation.[14] The government cannot, accordingly, prosecute a foreign business unless there is ''evidence of foreign government sponsorship'' or ''coordinated intelligence activity.''[15] The pertinent inquiry is whether the activity of the company is, from a practical and substantive standpoint, foreign government directed.''[16] This means that the United States may have some evidence of foreign government involvement, but not sufficient evidence to establish that the theft was directed by the foreign government, leaving the United States with no choice but to prosecute under Section 1832, if it is to go forward with the case.

Third, in cases even where there is evidence that foreign government's involvement was substantial, prosecutors may be discouraged from charging a violation under Section 1831 because, in addition to the higher burden of proof, the current sentencing guidelines for a violation of Section 1831 are not so different from Section 1832 as to encourage a prosecution under the former. In other words, prosecutors can get just as much bang from the buck by charging a violation of Section 1832 instead of Section 1831.

Fourth, the bureaucratic system discourages charging a violation of Section 1831. The responsibility for investigating and charging violations of Sections 1831 and 1832 lie within different sections of the Department of Justice. Section 1831 cases are the purview of counterintelligence agents and prosecutors in the Internal Security Section, whereas Section 1832 cases are investigated and prosecuted by fraud and IP agents, AUSAs, and trial attorneys in the Computer Crime & Intellectual Property Section.

When the U.S. opens a theft of trade secret investigation, it may not even suspect foreign government involvement. The identity of the individual who committed the theft may usually be known, but foreign involvement is generally not discovered until later. Once evidence of foreign involvement is uncovered, the agents and prosecutors working have a vested self-interest in not pursuing foreign government involvement or at least not charging it.

If foreign government involvement is acknowledged, the agent and prosecutors may be removed and management responsibilities shifted to counterintelligence personnel. Because the number of ongoing prosecutions is an important metric in determining future funding and for other reasons, agent and prosecutors are often reluctant to be removed from a case.

Recommendations:

It is recommended that the government take steps to consolidate its investigations and prosecutions under Sections 1831 and 1832 in order to more accurately reflect whether the theft is sponsored by a foreign entity.

3. Defendant's Gender

Findings:

The defendant was male in more than 93 percent of the prosecutions. Indeed, with few exceptions, even in those cases in which a woman was charged, the primary defendant was male and the woman's involvement was generally in a supporting role, for example, assisting her husband in stealing the trade secrets.

In one of the few cases involving a female lead defendant, after a three-week bench trial in the Northern District of Illinois, the court found Hanjuan Jin guilty of three counts of stealing trade secrets from Motorola in violation of Section 1832.[17] She was acquitted of violating Section 1831.[18] Jin was an engineer with Motorola. On Aug. 29, Jin was sentenced to four years imprisonment. While on medical leave from the company, Jin pursued employment with a company in China. On the day she returned to Motorola from her medical leave she copied and downloaded thousands of Motorola confidential documents. As she attempted to depart Chicago for China, authorities stopped her at the airport and seized the materials that included a description of communication features that Motorola incorporates into its telecommunications products sold around the world.

In one of the few other serious cases involving a female defendant, Yuan Li, a Chinese national, pleaded guilty to stealing trade secrets from Sanofi Aventis.[19] While working for Sanofi, Li downloaded information about a number of Sanofi's proprietary and secret compounds and sought to sell them through the U.S. branch of a Chinese chemical company. She was sentenced to 18 months imprisonment.

4. Defendant's Level of Education

Findings:

Theft of trade secrets is truly a white-collar crime. The defendant is most often well educated and by virtue of his senior position had access to the company's valuable proprietary information. Indeed, in a number of cases, the defendant had a doctorate and was highly regarded in his field. In perhaps the most egregious ex-

[12] 18 U.S.C. § 1831(a).
[13] 18 U.S.C. § 1839(1).
[14] *See* 142 Cong. Rec. H12137-01 (daily ed. Sept. 28, 1996) (statement of Rep. McCollum).
[15] 142 Cong. Rec. S12212 (daily ed. Oct. 2, 1996).
[16] *Id.*
[17] *United States v. Jin*, 833 F. Supp. 2d 977 (N.D. Ill. 2012).
[18] *Id.*
[19] *United States v. Li*, No. 2:2001-CR-00034 (D.N.J. 2011).

  PTCJ ISSN 0148-7965

ample, Hong Meng, pleaded guilty to stealing trade secrets from DuPont relating to Organic LEDs.[20] Meng not only had a PhD, but also was co-nominated in 1991 for the Nobel Prize in chemistry.

Conclusions/Recommendations:

Companies should view all employees as equally capable of stealing valuable trade secrets and make sure that their trade secret protection programs reflect this understanding.

5. Relationship of the Defendant to the Victim

Findings:

In more than 90 percent of the EEA prosecutions, the defendant was an ''insider,'' and had access to the trade secret because he was an employee of the victim, or worked for a vendor or contractor of the victim. Another commonality is that in many of the cases the defendant committed the theft shortly before leaving the victim company. For example, in September 2011, Chunlai Yang was indicted in the Northern District of Illinois for theft of trade secrets from his employer, CME Group.[21] According to the indictment, beginning approximately six months before he gave notice, Yang downloaded and removed computer source code and other proprietary information relating to an electronic trading program with the intention of using the information to increase the trading volume at a chemical electronic exchange in China.[22]

In another example, an Intel Corp. engineer pleaded guilty on April 5 to stealing very valuable trade secrets just before he left the company to begin work at rival Advanced Micro Devices.[23] According to the indictment, the trade secrets included details on the development of Intel's newest generation of microprocessors. The defendant intended to use the information to further his career at AMD.

Conclusions/Recommendations:

Since the immediate period leading up to an employee giving notice presents the greatest danger to a company, the company, as part of its trade secret protection plan, should carefully review its procedures when an employee gives notice, especially for an employee who had access to confidential information. At a minimum, the company should not only immediately revoke the employee's ability to access all proprietary information, but also should conduct an exit interview and require him to attest that he is not taking any confidential information or proprietary information to a new employer.

Further, in the event, for example, that the departing employee had routinely been given access to valuable trade secrets, a company should seriously consider whether to launch an investigation into the employee's computer records and travel activity over the previous few months to see whether there is any suspicious activity. Where there is evidence of suspicious activity, e.g., unexplained foreign travel, the company should consider opening a full investigation including a forensic analysis of the employee's computer records.

6. Nationality of the Defendant/Purpose of the Theft

Findings:

While more than a majority of the individual defendants are U.S. citizens, there is a ''China connection'' in a high percentage of the prosecutions. In particular, more than 30 percent of all of the prosecutions involved Chinese citizens or naturalized U.S. citizens originally from China. In addition, the defendant, in slightly less than 30 percent of the total EEA prosecutions, misappropriated the trade secrets to benefit the Chinese government, an existing Chinese company or to start a company there.

The trend of a China connection is also increasing. Since 2008, the government has indicted 50 cases under both sections of the EEA, and approximately 40 percent have a China connection. In 2010, six out of the seven cases that were adjudicated under the EEA involved a link to China. Further, seven of the nine prosecutions that the government has brought under Section 1831 involve an allegation of Chinese government involvement.

This does not mean that an entity of the Chinese government was charged in each case, but that the defendant(s) acted to benefit an entity associated with the Chinese government. Indeed, as described above, in February, the government unsealed an indictment charging, for the first time, a company controlled by the Chinese government, the Panang Group, and a number of individuals violated Section 1831 by stealing and attempting to steal trade secrets from DuPont.[24].

In the most serious EEA case ever, as judged by the length of the prison sentence, following a three-week bench trial, in July 2009, the court convicted Dongfan Greg Chung of stealing trade secrets from his employer Boeing and from Rockwell Helicopter with the intent to benefit the People's Republic of China.[25] The trade secrets related to the space shuttle, Delta IV Rocket, F-15 Fighter, B-52 Bomber and Chinook helicopter. Apart from the length of the sentence, this case is noteworthy in a number of other respects. First, the sheer amount of secret information possessed by Chung was staggering. During a search of his house, the FBI discovered more than 300,000 pages of Boeing and Rockwell documents with approximately 250,000 pages kept in binders in an unfinished storage area under Chung's house.

The length of time of defendant's illegal activities was also stunning. The defendant, who was born in China in 1936, became a naturalized U.S. citizen in 1972, and began working at Boeing in 1964. The evidence at trial established that defendant first offered his services to the Harbin Institute of Technology in China in 1979 expressing his wish to contribute ''to China's Four Modernizations.''

Other notable Section 1831 and 1832 cases with a link to China include:

[20] *United States v. Meng*, No. 4:10-CR-00013 (D. Del. 2010).
[21] *United States v. Yang,* No. 1:11-CR-00458 (N.D. Ill. 2011).
[22] *Id.*
[23] *United States v. Pani,* No. 4:08-CR-40034 (D. Mass. 2008).
[24] *United States v. Liew*, No. 11-CR-0573 (N.D. Cal. 2011).
[25] *United States v. Chung*, No. 8:08-CR-00024 (N.D. Cal. 2008).

■ Kexue Huang, a Chinese national pleaded guilty to violating Section 1831 by stealing trade secrets relating to insecticides from Dow Chemical, where he was employed as a research scientist and from Cargill relating to a new food product. Defendant intended to benefit Beijing University.[26]

■ In April 2011, Xiang Dong Yu was sentenced to 70 months imprisonment for stealing trade secrets from the Ford Motor Company. Yu worked for Ford from 1997 to 2007 and had access to many Ford trade secrets including design documents. Before telling Ford he had accepted a job in China, Yu downloaded 4,000 Ford documents onto an external hard drive. When Yu returned to the United States in October of 2009, he was arrested. The FBI discovered 41 Ford system design specification documents had been downloaded onto his laptop computer belong to his new employer, Beijing Automotive Company. The FBI also discovered that each of those design documents had been accessed by Yu during his employment at Beijing Automotive Company, which is a direct competitor of Ford.[27]

■ In January 2011, Yuan Li pleaded guilty to stealing trade secrets from Sanofi-Aventis, where she worked as a research chemist and offering to sell them through the U.S. branch of a Chinese chemical company.[28]

■ In June 2010, Hong Meng pleaded guilty to stealing trade secrets from DuPont relating to organic LEDs. While still employed by DuPont, Meng accepted a position with Beijing University and through an intermediary sent 109 chemical samples to himself at the university.[29]

This emerging trend confirms an understanding that, as part of development process, China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to U.S. corporations to steal trade secrets using a variety of methods.[30] Other anecdotal evidence supports this conclusion as well. The high percentage of the recent cases with a China connection also suggests that the pace of Chinese economic espionage is increasing.

Other than China, defendants also intended to benefit foreign companies in India (2),[31] Dominican Republic (1),[32] Korea (2),[33] and South Africa (1),[34] under Section 1832 and Israel[35] and Japan[36] under § 1831.

Finally, in approximately 70 percent of the cases in which the purpose of the theft was discoverable, the defendant committed the theft in order to help start a new company or for personal use at a new employer without knowledge of the new employer. In virtually all of the remainder of the cases the defendant provided the trade secret to a competitor of the victim or offered to sell it to a competitor.

7. Type of Trade Secrets

Findings:

The type of trade secrets at issue in the EEA prosecutions varies greatly. Most of the stolen trade secrets were high-tech, such as the formula used in the manufacture of solar cells.[37] Other types of high-tech trade secrets included drug formulae (4), design of parts for cars (5), and semiconductor equipment (3). By far, the largest general type of trade secrets stolen was source code (17). The code related to a variety of products including financial products,[38] system for processing health care benefit forms,[39] location-based services and applications for mobile phones,[40] medical programs,[41] website design and operations,[42] and Microsoft Windows N.T. 4.0 and Windows 2000.[43] The next most sought-after trade secrets related to pricing/profitability, customer lists and marketing plans[44](12). However, stolen trade secrets also included information related to less hi-tech subjects such as ''starter'' tobacco,[45] which is used to make various tobacco products, and advance copies of a Nike catalogue.[46]

Conclusions/Recommendations:

While high-tech information is the most sought after type of information, no species of information that meets the definition of a trade secret should be considered immune from theft. Accordingly, companies should enact security measures to protect confidential information that are commensurate with the economic value of the information.

8. Victim

Findings:

In the vast majority of cases, the victim was a large U.S. corporation, often with international offices. In-

[26] *United States v. Huang*, No. 4:01MJ01704 (D. Ind. 2010).
[27] *United States v. Yu*, No. 09-CR-20304 (E.D. Mich. 2009).
[28] *United States v. Li*, No. 2:2001-CR-00034 (D.N.J. 2011).
[29] *United States v. Meng*, No. 4:10CR00013 (D. Del. 2010).
[30] 2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement, at 30 (March 2012), available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf
[31] *United States v. Mohopatra*, No. 2:11CR02123 (D. Utah 2011); *United States v. Jhaveri*, 5:2010-CR-00523 (N.D.N.Y. 2010).
[32] *United States v. Mulhollen*, No. 4:10-CR-00013 (W.D. Ky. 2010).
[33] *United States v. Mitchell*, No. 09-CR-00425 (E.D. Va. 2009); *United States v. Shin*, No. 1:08-CR-00458 (N.D. Ohio 2008).
[34] *United States v. Buffin*, No. 1:06-CR-00031 (N.D. Ohio 2006).
[35] *United States v. Doxer*, No. 1:11-CR-10268 (D. Mass. 2010).
[36] *United States v Okamoto*, No. 1:01-CR-00210 (N.D. Ohio 2010).
[37] *United States v. Pham*, No. 2:11-CR-00722 (E.D. Pa. 2011).
[38] *See e.g., United States v. Yang*, No. 1:11-CR-00458 (N.D. Ill. 2011).
[39] *United States v. Cullen*, No. 3:011-CR-0002 (W.D. Ky. 2011).
[40] *United States v. Zhang*, No. 5:10-CR-00827 (N.D. Cal. 2010).
[41] *United States v. He,* No. 2:09-CR-00424 (E.D. Pa. 2009).
[42] *United States v Hummel*, No. 2:09-CR-20566 (E.D. Mich. 2009).
[43] *United States v Genovese*, No. 1:05-CR-00004 (S.D.N.Y. 2005).
[44] *See e.g., United States v Martinez,* No. 1:09-CR-00486 (N.D. Ga. 2009).
[45] *United States v Mulhollen*, No. 4:10-CR-00013 (W.D. Ky. 2010).
[46] *United States v. Chapin*, No. 3:07-CR-00439 (D. Ore. 2007).

   ISSN 0148-7965

deed, DuPont,[47] Dow Chemical,[48] Corning,[49] Lockheed[50] and Boeing[51] were victims more than once. Smaller companies, however, were also the victims of thefts. For example, the executive search Korn-Ferry was a two-time victim of theft of trade secrets.[52]

Conclusions/Recommendations:

The bottom line is that no company is too small to be the victim. The only requirement is that possess secret and economically valuable information. In short, in the information age, virtually every company is at risk and should act accordingly.

There are a number of plausible explanations for five corporations comprising 8 percent of the prosecutions. The simplest explanation is that these corporations, because of their size and the value of their trade secrets, are likely to be most often targeted by thieves. However, this does not fully explain why they were victimized multiple times.

After all, there are a great many other corporations in the United States of similar size and with very valuable trade secrets that have not been the victim in even a single EEA case. Accordingly there must be more to it than simply the size of the corporation. The likely explanation stems from a combination of a trade secret protection program that successfully leads to the discovery of thefts and a corporate policy to report thefts to the federal government for possible prosecution.

Businesses should learn from these companies.

9. Trade Secret Protection Programs

Findings:

A number of cases suggest that regardless of the steps undertaken by a company to protect trade secrets, the protection is only as strong as the weakest link. For example, Motorola had extensive security measures in place, yet Hanjuan Jin was apparently easily able to circumvent them and was only caught through happenstance as she was leaving this country on her way to China with Motorola's trade secrets.

The security measures included: (1) physical security measures that carefully controlled access to the company's facilities, security cameras at the entrances to the buildings and a large security force;[53] (2) network and computer security that included passwords and firewalls to prevent identification by hackers and other outside threats and internal measures that restricted access within the computer network depending on the user's authorization and classification status of a document or file; and (3) a specific trade secret protection program containing detailed policies regarding the classification and marking of proprietary documents and access to documents and their physical handling and providing for the training of new hires and current employees, as well as audits to promote compliance with the program's policies.

Finally, Motorola also required its employees to sign an employment agreement, a code of conduct containing a confidentiality provision and a policy on the appropriate use of computer resources.

Despite this multi-pronged and comprehensive approach, Jin, was able to download thousands of company documents onto her personal laptop and a thumb drive, and only a limited number of the documents related to her work. She was also able to leave the premises on a number of occasions carrying documents in her arms, even late at night. She accomplished all of this on her first day back at work after a more than one-year absence for medical reasons.

Conclusions/Recommendations:

Jin probably would have succeeded had she not been stopped at a Chicago airport as she attempted to board a flight to Beijing. She was only detained and searched after she had given misleading and evasive answers to how much cash she was carrying. If this had not occurred, the company may never have learned about the thefts or, at the very least, the defendant would have been able to return to China with all the company's documents.

The outcome of Jin suggests that companies must continuously reevaluate their intellectual property programs to ensure that they reflect the evolving nature of threats and must learn from their mistakes. For example, employees who return to work after a long absence should not be immediately given access to a broad range of confidential information, especially to confidential information that is not within their area of expertise.

In addition, employees' travel, especially for those who have access to extremely valuable and confidential information should be monitored. There is no evidence in the record that Motorola reviewed such travel records. Had it done so, the company would have learned that Jin had spent a great deal of time in China, which, at the very least, should have raised questions about what she was doing while there.

10. Dispositions

Findings:

In almost 85 percent of the EEA prosecutions that are no longer pending, the defendant pleaded guilty to violating the EEA or to another federal statute. In approximately 6 percent of the prosecutions, the charges were dismissed with prejudice after the defendant had completed pretrial diversion, a similar program or for other reasons. In 4 percent of the cases the charges were dismissed without prejudice. At least five defendants fled and are still being sought by the United States. According to the government, three of the defendants are in

[47] *United States v. Meng,* No. 4:10-CR-00013 (D. Del. 2010); *United States v. Mitchell,* No. 09-CR-00425 (E.D. Va. 2009).

[48] *United States v. Huang,* No. 4:10-MJ-01704 (D. Ind. 2010); *United States v. Liou*, 2:06-MJ-00436 (S.D. La. 2006).

[49] *United States v. Sanders,* No. 06-CR-6005 (W.D.N.Y. 2006); *United States v. Wu*, 6:05-CR-06027 (W.D. Wis. 2006).

[50] *United States v. Satchell*, No. 04-mj-01067 (C.D. Cal. 2004); *United States v. Branch*, No. 2:03-CR-00715 (C.D. Cal. 2003).

[51] *United States v. Branch*, No. 2:03-CR-00715 (C.D. Cal. 2003); *United States v. Chung,* No. 8:08-CR-00024 (C.D. Cal 2008).

[52] *United States v. Nosal*, No. 08-CR-0237 (N.D. Ca. 2008); *United States v. Jacobson*, No. 3:07CR00568 (N.D. Cal. 2007).

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

China,[54] one is in Taiwan[55] and the remaining defendant is in Japan.[56]

Only 12 cases went to trial,[57] with the defendant being acquitted of all charges in just two of these.[58] In a bench trial in 2008, the court acquitted the defendant of stealing trade secrets from his then current employer, Broadcom.[59] At trial, the defendant claimed that the trade secrets were part of his ''toolkit.'' The judge agreed and found that the defendant lacked the requisite intent to convert Broadcom's trade secrets. The court also noted that the defendant did not disclose the trade secrets to his new employer and did not directly use them himself.

In *United States v. Aleynikov*,[60] the Second Circuit reversed defendant's conviction for stealing proprietary source code from Goldman Sachs' high-frequency trading program under the EEA and the Interstate Transportation of Stolen Property Act. With regard to the EEA, the court held that the government must prove that the trade secret itself is ''intended to, actually move in interstate or foreign commerce.''

The court found it insufficient for the product merely to relate to interstate or foreign commerce and, instead, must be related to products ''produced for'' or ''placed in'' interstate or foreign commerce must be read as a term of limitation. The court, thus, agreed with the defendant that:

Goldman's HFT system was neither 'produced for' nor 'placed in' interstate or foreign commerce. Goldman had no intention of selling its HFT system or licensing it to anyone . . . It went to great lengths to maintain the secrecy of its system. The enormous profits the system yielded for Goldman depended on one else having it. Because the HFT system was not designed to enter or pass in commerce, or to make something that does, Aleynikov's theft of source code relating to that system was not an offense under the EEA.[61]

The court also found support for its conclusion from its understanding that the two terms, ''produced for'' or ''placed in'' interstate commerce, identify two separate but related categories. The latter refers to trade secrets related to products that are presently being sold in interstate commerce. The former refers to trade secrets that relate to products that are being developed but are not yet actually ''placed in,'' commerce.

The court stated that the EEA ''would fall short of critical protections if it applied only to products that had already been 'placed in' the marketplace; left vulnerable would be the class of trade secrets inhering in products that have not yet been placed on the market; Congress thus plugged a gap by extending the statute's coverage to include products 'produced for' commerce as well as those already in the marketplace.''[62]

In 25 percent of the cases that went to trial, the defendant waived the right to a jury trial.[63] This is a much higher percentage than in other white-collar cases. Since all of the defendants who waived their right to a jury trial were of Chinese ancestry or were Chinese nationals, the defendants may have been concerned about racial bias and believed that they would have a better chance for acquittal with a judge than a jury. A court convicted two of the three defendants.

Conclusions/Recommendations:

First, Congress should amend the EEA so as to remove any doubt that trade secrets that are related to products or processes and that are used internally are protected to the extent permitted by the Commerce Clause. There is simply no reason to limit the EEA any further beyond that required by the Commerce Clause.

Second, the amendment should also clarify that trade secrets relating to a product in the development stage are also protected. Finally, while not addressed by the *Aleynikov* court, the present language of the EEA may also exclude from protection trade secrets related to services. No explicit reason for this limitation is offered in the text or legislative history of the EEA, and it seems at odds with the spirit of the expansive definition of trade secrets offered in Section 1839, but it exists nevertheless. Accordingly, an amendment should include language that services are covered.

11. Sentencing

Findings

As seen from the following chart, 33 percent of the 81 defendants, who have been sentenced so far for violating the EEA, were sentenced to probation or supervised released. If home confinement is included, 38 percent of the defendants sentenced for violating the EEA served no time in prison.

---

[54] *United States v. Zhang*, No. 5:10-CR-00827 (N.D. Cal. 2010) (Yanmin Li, Xiadong Li); *United States v. Wu*, No. 6:05-CR-06027 (W.D.Wis. 2005) (Xingkun Wu);

[55] *United States v. Hsu*, No. 2:97-CR-00323 (E.D. Pa. 1997) (Jessica Chou).

[56] *United States v. Okamoto*, No. 1:01-CR-00210 (N.D. Ohio) (Takashi Okamoto).

[57] (1) *United States v. Agrawal*, No. 1:10-CR-00417 (S.D.N.Y. 2010); (2) *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012); (3) *United States v. Zhu*, No. 3:09-CR-00722 (D. N.J. 2009); (4) *United States v. Roberts*, No. 3:08-CR-0017 (E.D. Tenn. 2008); (5) *United States v. Williams*, 526 F.3d 1313 (11th Cir. 2008); (6) *United States v. Shiah*, No. 8:06-CR-00092 (C.D. Cal. 2006); (7) *United States v. Zhang*, No. 5:05-CR-00812 (N.D. Ill. 2005); (8) *United States v. Four Pillars.*, 281 F.3d 534 (6th Cir.), *cert. denied*, 537 U.S. 1170 (2003); (9) *United States v. Lange*, 312 F.3d 263 (7th Cir. 2002); (10) *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000); (11) *United States v. Jin*, 833 F. Supp.2d 977 (N.D. Ill. 2012); (12) *United States v. Chung*, 659 F.3d 815 (9th Cir. 2011).

[58] In *United States v. Jin*, 833 F. Supp. 2d 977 (N.D. Ill. 2012), the court after a bench trial acquitted the defendant of violation of Section 1831, but convicted her under Section 1832. With regard to Section 1831, the court found that the evidence at trial was insufficient to support a finding that the defendant intended to steal the trade secrets for the benefit of the Chinese government, as required under that section.

In particular, there was no evidence that although defendant took a job with a Chinese telecommunications company, after leaving her U.S. employer, that developed technology for the Chinese military, the technology sought by the Chinese military was superior to, and incompatible with the technology of her former employer in the United States.

[59] *United States v. Shiah*, No. 8:06-CR-00092 (C.D. Cal. 2008).

[60] 676 F.3d 71 (2d Cir. 2012).

[61] *Id.* at 82.

[62] *Id.* at 80.

[63] *United States v. Shiah*, No. 8:06-CR-00092 (C.D. Cal. 2008) (acquitted); *United States v. Jin*, 833 F. Supp. 2d 977 (N.D. Ill. 2012) (convicted under § 1832); *United States v. Chung*, 659 F.3d 815 (9th Cir. 2011).

  PTCJ ISSN 0148-7965

Sentence	§ 1831	§ 1832
Probation/Supervised Release	0	27
Home Confinement	0	4
0-6 months	1	7
6-18 months	0	13
19-36 months	1	17
37-54 months	0	4
55-95 months	1	5
>96 months	1 (Chung – 188 months)	1 (Williams – 96 months)

In comparison the longest sentence for violating either of the sections of the EEA was imposed on Dongfan Chung, who was sentenced to 188 months for violating Section 1831. As described above, Chung stole trade secrets from Boeing relating to the Space Shuttle and the Delta IV Rocket. The length of this sentence may be considered an outlier, however, since it was primarily based on Chung having also been convicted of failing to register as a foreign agent.

Joya Williams received a sentence of 96 months, which is the longest sentence for violating Section 1832. She was convicted of offering to sell confidential Coca-Cola marketing documents and a product sample. On appeal, the Eleventh Circuit found that the sentence was not unreasonable, even though it was above the sentencing guidelines range, based on the seriousness of the offense.[64] Kexue Huang, a Chinese national, received the next longest sentence for violating Section 1832.[65] In December 2011, he was sentenced to 87 months imprisonment for misappropriating trade secrets from Dow AgroSciences LLC and from Cargill Inc. with the intent to benefit Beijing University. According to the plea agreement, the aggregated loss from Huang's conduct was between $7 and $20 million.

Conclusions/Recommendations:

Both houses of Congress are currently considering a bill that would increase criminal penalties for theft of trade secret for the benefit of a foreign government or other foreign entity. For offenses committed by individuals, the bills would increase the maximum period of imprisonment from 15 years to 20 years, and the maximum fine from $500,000 to $5,000,000. Under current law, the maximum penalty for such an offense by an organization is a fine of $10,000,000.

The House version of the bill would add an alternative maximum penalty of three times the value of the stolen trade secret if that amount exceeds $10,000,000. The bills would also direct the U.S. Sentencing Commission to set guidelines to reflect the intent of Congress that penalties for such offenses should reflect the seriousness of these offenses, account for the harm they cause, and provide adequate deterrence.

While there is certainly no downside in amending the EEA as proposed, it is unlikely that such an amendment would actually deter foreign economic espionage as intended. As noted above, since the enactment of the EEA, the government has brought fewer than 10 cases for foreign economic espionage. Since as described above, recent studies suggest that increases in the certainty of punishment, as opposed to the severity of punishment, are more likely to produce deterrent benefits.

While increasing the severity of the punishment under Section 1831 may promote and serve other important social and public policy goals of punishment and retribution, it is unlikely to lead to greater deterrence. Given the odds of being prosecuted and convicted, and the value of intellectual property information, the benefits to some of illegally acquiring valuable trade secrets to may continue to far outweigh the risks of being caught and prosecuted.

Accordingly, it is recommended that the penalties for violating Section 1832 also be increased. For example, defendants who are convicted of violating Section 1832 with the intent to benefit a foreign company should receive a lengthier sentence. This would address the wide spread situation described above, in which defendants misappropriate that the trade secrets benefit a foreign corporation that directly competes with their United States-based employer but are sentenced without consideration of this circumstance.

More importantly, as described above, an increase in the punishment for violating the EEA must be accompanied by substantially increasing the number of investigations and prosecutions.

IV. Conclusion

A review and analysis of the more than 120 EEA prosecutions suggests that neither government, nor industry is doing enough to protect against the theft of trade secrets by foreign entities and unscrupulous competitors. The Department of Justice must substantially increase the number of EEA prosecutions if the EEA is to truly serve as a deterrent against thefts. While there is no mechanical formula to determine the minimum number of prosecutions that would be needed to act as a deterrent, the current level is unlikely to reach that level, especially since a majority of the U.S. Attorney's Offices in the United States have not prosecuted even a single case.

In addition, the results of the study suggest that Congress' emphasis on amending the EEA to simply increase the penalties for conviction under Section 1831 does not address more important shortcomings in the statutory language. Where there is no doubt that foreign government economic espionage is a serious concern and represents a genuine threat to the intellectual property of U.S. corporations, the relatively limited number of prosecutions under Section 1831, as com-

[64] *United States v. Williams*, 526 F.3d 1312 (11th Cir. 2012).
[65] *United States v. Huang*, No. 4:10-CR-01704 (D. Ind. 2010).

pared to Section 1832, suggests that the EEA would serve as a more effective deterrent against thefts of trade secrets if the penalties were also increased under Section 1832. This is especially true since a majority of the recent prosecutions under Section 1832 have a foreign connection.

Courts should also amend the EEA so that the statute unambiguously covers the theft of trade secrets to the extent permitted by the Commerce Clause, and that it protects trade secrets in the development stage.

Finally, the findings indicate that companies are also not doing enough to protect their valuable confidential information. As a first step, companies should routinely report thefts to the government for review and prosecution. It is also essential that all companies, regardless of size and purpose, institute a trade secret protection program that is continuously being updated to reflect ever-changing market conditions and threats.

The report establishes that thieves are interested in almost any type of trade secret, regardless of the technology involved so long as the trade secret has economic value.

  PTCJ ISSN 0148-7965