

The Theft of Trade Secrets: Evidence from the Economic Espionage Act of 1996

Abstract

This paper reports on an analysis of 130 cases arising from prosecutions under the U.S. Economic Espionage Act (EEA) of 1996. It considers use of trade secrets by firms, characteristics of offenders and firms, the value of stolen property and the effects of criminalization. It finds that most theft is by insiders, and not by non-nationals. Further, only 40% of the Intellectual Property subject to theft was potentially patentable, suggesting that trade secrecy is particularly vulnerable to the threat of theft.

JEL Codes: K14, O34

Keywords: Economic Espionage Act, Trade Secrets, Intellectual Property, White Collar Crime

Date of Draft: September 10, 2008

Provisional only: not to be quoted without author's consent.

Nicola Searle, ncs5@st-andrews.ac.uk

Research Associate

Center for Research in Industry, Enterprise, Finance and the Firm (CRIEFF)

School of Economics & Finance, University of St Andrews, Scotland

St. Salvator's College, KY16 9AL

Working paper presented at the ONE RIGHT SYSTEM FOR IP – VISION IMPOSSIBLE?
Conference by the IPR University Center, 1 – 3 October 2008, Helsinki

1. Introduction

This paper analyzes evidence gathered on prosecutions under then U.S Economic Espionage Act (EEA). It does so under the four headings of: economic espionage (as theft of trade secrets); prosecution data (as derived from the Department of Justice and Public Access to Court Electronic Record Sources); value estimation (methods and effects of values) and, finally, criminalization and detection (with reference to the act of trade secret theft itself, prosecution methods, and compensatory choices.) It aims to bring fresh insights to: the modal defendant and the positive incentives of criminal, as opposed to the civil, prosecution of those who steal trade secrets.

One of the most famous trade secrets in the world, the secret Coca-Cola formula, has long been a subject of fascination.¹ Tales of the century-long, highly maintained secret have become part of the company's folklore.² However, Coca-cola's secrecy was recently tested when Joya Williams and her two partners attempted to sell Coke secrets to its main rival, Pepsi, for \$1.5 million.³ Pepsi turned the thieving trio over to the authorities and Williams was subsequently sentenced to 8 years in prison.⁴

The law that put Williams behind bars is the EEA. Amid concerns over the vulnerability of American trade secrets, the United States enacted the EEA in 1996. Prior to the EEA, the theft of trade secrets was, by itself, not a crime. This paper reports on research developing a database of EEA prosecutions; this new database, which provides extension information on the 131 defendants charged with EEA violations in 93 cases, provides insight into the stolen trade secrets.

The EEA was created to reinforce protection of American trade secret by elevating the theft of trade secrets to a felony and broadening the definition of trade secrets. In order to address the concerns of economic espionage by foreign entities, the act also includes provisions which extend its jurisdiction to have extraterritorial applications. The paper examines the impact of this new law and the insights its application provides; these criminal prosecutions offer a heretofore unexplored data source for evidence on trade secrets.

For the purposes of the research detailed in this paper, the EEA prosecution data have been collected using online court records, media reports and academic papers. The aggregate of this data provides a rich source of evidence on the value of trade secrets, and the way in

which firms use trade secrets. While the process of data collection raises some non-trivial challenges, particularly of adverse selection (arising from the process of selecting cases for prosecution), once obtained, the data represent a unique source of trade secret information which, by its nature, is typically undisclosed. Contrary to the operating assumptions of the EEA, the data demonstrate that the majority of defendants are classified as insiders and are U.S. citizens. Further, it is shown that the majority of these trade secrets would not qualify for patent protection, which indicates that the use of trade secrets is particularly important for these intellectual assets.

Another fruitful aspect of the database is the value of the stolen trade secrets. Four main methods are used to obtain estimates of these values: unjust enrichment, lost profits, replacement costs and reasonable royalty. These methods result in highly heterogeneous estimates and the resulting values range from \$5,000 to \$600m in EEA cases.

The escalation of the theft of trade secrets to the status of a felony affects the incentives for firms and potential thieves alike. In comparison to civil cases, the criminal enforcement of trade secret theft introduces incarceration as a form of punishment. When confronted with a theft of trade secrets, a firm must decide whether to seek legal recourse and if that recourse should be criminal and/or civil. However, the financial damages assessed in EEA criminal cases are compared to civil cases and found to be lower. In favor of the EEA route, it is found that choosing to punish thieves via a criminal action has some positive incentives, in terms of future deterrence, moral punishment and the shifting of legal costs from the victim company to the State.

The paper begins in Section 2 with a discussion on trade secrets followed by Section 3 which goes into the economic and political beginnings of the EEA. Section 3 introduces the data gathered to create the EEA database and Sections 5 and 6 analyse the descriptive statistics with respect to the composition of defendants, victims and trade secrets. Section 7 details the various methods of valuing the trade secrets and the evidence in the EEA cases of their use. Finally, Section 8 examines the effects of criminalization and the detection of trade secret theft in EEA cases and is followed by Section 9 which contains concluding remarks.

2. Trade Secrets

Trade secrets present an analytical and empirical challenge to economists. Amongst intangible assets, trade secrets represent the illusive, difficult to quantify extreme. Unlike their counterparts, patents, copyright and trade marks, trade secrets are not subject to a formal registration process or any obligatory disclosure. It is these characteristics which make trade secrets a challenging yet important subject of research, given their widespread use to protect intellectual property in modern enterprises.

Cohen, Nelson and Walsh (2000) caught the attention of economists with their survey which indicated that patenting is considered an inferior strategy by firms when compared to trade secrets, lead time and marketing. This new research has caused a change in thought to the traditional, patent-focused lines of research, and has generated an interest in alternative means of Intellectual Property (IP) protection such as trade secrets.

To qualify as a trade secret, the intangible property must meet three requirements: it must be secret; it must derive economic value from being secret; and it must be subject to reasonable protection measures to maintain its secrecy. The interpretation of these requirements varies by jurisdiction and, in some jurisdictions, trade secrets are not recognised as intellectual property. However, these three requirements reflect the standards of most countries and are reflected in the World Trade Organization's agreement on Trade Related Aspects of Intellectual Property (TRIPS) which dictates the minimum standards required of TRIPS signatories.⁵

While the law literature examines trade secrets regularly, this is less so in the economic literature. In contrast to the patent literature, which is well established, the economics literature addressing trade secrets is relatively small. Economic models of trade secrets, e.g. incorporating trade secrets into the decision of firm's choice of intellectual property protection (see Anton and Yao (2003), Bessen (2004), Erkal (2005), Encaoua and Lefoulli (2006)) and licensing (see Cugno and Ottoz (2006) Bhattacharya and Guriev (2006)), are fairly well developed and their maturation has mimicked the development of the patent literature. To name but a few, these patent models address cumulative innovation (Chang (1995) and Scotchmer (1991, 2005)), patent design (Klemperer (1990), Gilbert and Shapiro (1990), Gallini (1992), Denicolo (1996), and Scotchmer (2005)) and harmonization (Kotabe (1992), and Park & Ginarte, (1997)).

The empirical literature on patents benefits greatly from the vast data resources available to researchers. The same cannot be said of the current state of the empirical basis of the trade secret literature. The data are limited, and the literature extends to just a few papers including surveys (including some evidence from litigation) (see (Lerner (2006), Cohen, Nelson and Walsh (2000), and Arundel (2001)). This scarcity of material makes the new evidence from the EEA, the subject of this paper, particularly valuable for research into trade secrecy, its causes, consequences, incentive and allocation properties, and policy implications.

3. The Economic Espionage Act (EEA) of 1996

Amid reports of the theft⁶ of American trade secrets by foreigners, the United States enacted the EEA in 1996. The act marked a significant change in the legal approach to trade secrets by elevating the theft of trade secrets to a felony, broadening the definition of trade secrets and including extraterritorial jurisdiction. While most American states had enacted the Uniform Trade Secrets Act (UTSA)⁷, the EEA harmonised trade secret law across the country. This harmonization makes it possible to thoroughly examine trade secrets in a consistent manner among all states. <

Figure 1 near here>

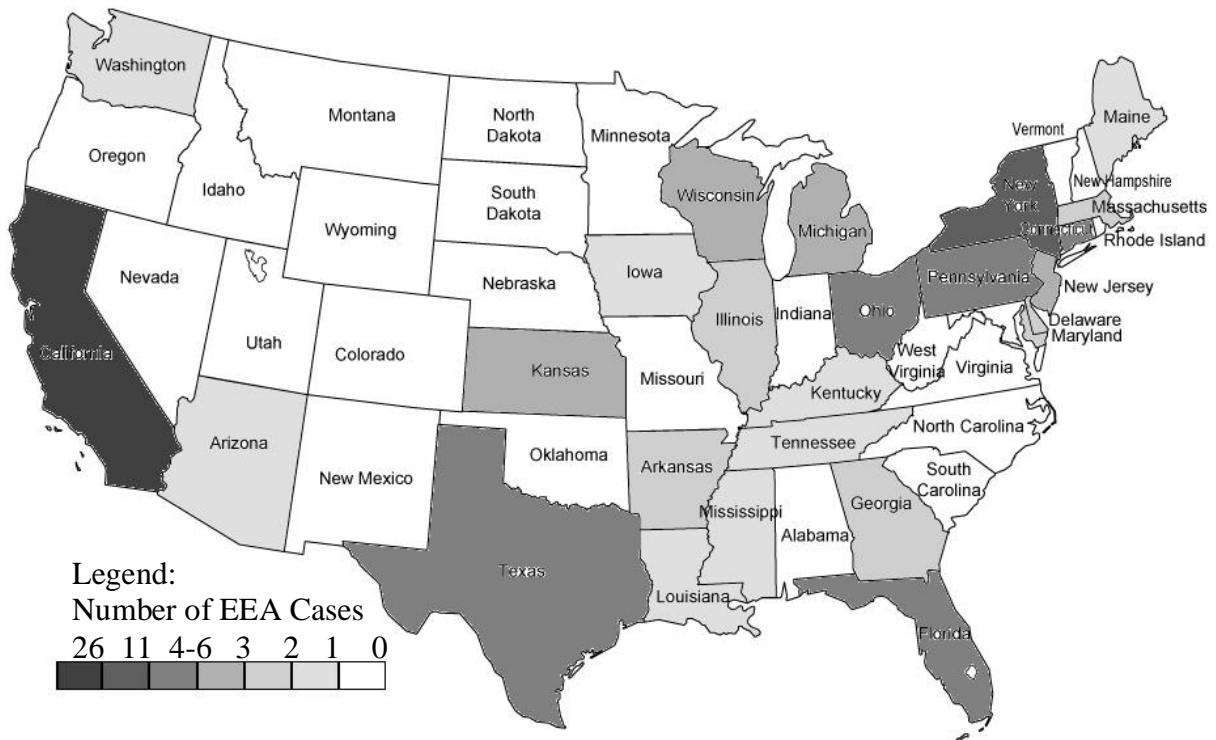
Figure 1 shows the distribution of EEA cases from 1996-2008 through the United States. This map roughly coincides with the economic distribution (by gross domestic product) of the United States.

<

Figure 1 near here>

Figure 1

Number of EEA Cases, by state, from 1996-2008



Source: Data from the EEA database created as part of this research covered in this paper.
See appendix.

The EEA was enacted under the presidency of Bill Clinton and coincided with a time of economic prosperity in the U.S. It was, however, drafted in a post-Cold War era during which the U.S. enjoyed a relatively militarily peaceful time.⁸ Given these circumstances, many authors⁹ argue that the closing down of the market for political and military spies meant these spies adapted their trade to industrial espionage. While this research project into EEA cases has uncovered no evidence to either refute or support this argument, the plausible idea that former spies were now engaging in economic espionage was of great interest to U.S. politicians and businesses.¹⁰ A series of incidents involving French businessmen and spy allegations in the early 1990s caught the attention of the U.S. intelligence agencies.¹¹ Acquisitions of American assets by Chinese and Japanese entities alarmed American businesses.¹² At the same time, the economy was in the process of shifting to an ever more information based, digital platform which both increased the bulk of potentially valuable information and, at the same time, exposed that the information to the inherent insecurity (e.g. its easily replicable nature) of the digital world.¹³ These political and economic shifts drew to public attention the potential threat of economic espionage and trade secret theft.

Prior to the EEA, the theft of trade secrets was dealt with primarily via civil actions and related criminal charges (e.g. transporting stolen property and wire fraud.) In two main provisions, sections 1831 and 1832, the EEA elevated economic espionage and the theft of trade secrets to a felony. Section 1831, Economic Espionage, makes the theft of trade secrets to benefit a foreign agent a criminal act punishable by up to 15 years imprisonment and \$500,000 for individuals and up to \$10 million fine for corporations. Section 1832, Theft of Trade Secrets, makes theft of, attempted theft of or conspiracy to steal trade secrets a crime. In this case, the individual can be fined up to \$250,000 and imprisoned up to 10 years while corporations are subject to fines up to \$5 million. The longer prison terms and higher fines of Economic Espionage indicate that the drafters of the act intended it to be a harsher sentence than the Theft of Trade Secrets.

Two elements of the act have been controversial: the extension of the definition of trade secrets and the potential extraterritorial application of the act.

“To the UTSA’s “formula, pattern, compilation, program, device, method, technique, or process,” the EEA adds “plans, . . . program devices, . . . designs, prototypes, . . . techniques, . . . procedures, . . . or codes” and expressly protects “financial, business, scientific, technical, economic, or engineering information.”¹⁴

This extension to named types of information broadens the overall definition of trade secrets. In addition, the concept of “public” is somewhat obfuscated in the EEA by merely stating “from not being generally known to ... the public”¹⁵ which leaves large room for interpretation of who the public entails.

In addition, the act has extraterritorial applications specifically included in Section 1837, Applicability to conduct outside the United States which extends the prosecution of economic espionage and the theft of trade secrets

“to conduct occurring outside the United States if
(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or
(2) An act in furtherance of the offense was committed in the United States.”¹⁶

This extraterritorial reach may force companies with U.S. links to enact protection schemes for the trade secrets or alter their behavior in ways they would have done prior to the EEA. While this provision does not appear to have provoked public outrage, at least one case has involved conduct outside the U.S. In the *U.S. v. Cartwright et al*¹⁷, two of the individual defendants were U.S. citizens living abroad in Prague and receiving stolen information to benefit two foreign corporations (owned by the defendants) from their U.S.-based counterpart in Maryland. However, in cases involving acts committed by foreign nationals, a difficulty arises where other countries may not be willing to extradite suspects. This was the case of *U.S. v. Okamoto*¹⁸ in which Japan refused the U.S. extradition request.¹⁹ These two cases are the only two, of EEA prosecutions, that appear to involve the extraterritorial application and the question of extradition. The challenges to extraditing suspects will limit the extraterritorial applications of the EEA, nonetheless may force firms to adhere to the law’s provisions.

To temper some of this controversy, the Attorney General (Jane Reno at the time of the signing of the EEA) required that the first five years of prosecutions be subject to express approval of the office of the attorney general.²⁰ As a result, 23 cases were filed in the first five years of the EEA but 38 were filed in the following five years. This may, however, reflect growing awareness of the EEA in general.

4. Database Construction

At the time of writing, there have been 130 defendants in 93 cases involving the EEA. These cases have been identified using two sources: the Department of Justice (DOJ) Compute Crime and Intellectual Property website²¹ and the Public Access to Court Electronic Records (PACER) system. From the DOJ, two sources were used: a table of EEA prosecutions²² from 1999 to 2005 and the DOJ press releases.²³ This method identifies high profile cases and, in three cases, identifies cases in which the defendants were not ultimately charged with EEA violations. The second method, using PACER, requires a time intensive searching of each court by prosecution code. This method was performed to identify all 1832 (theft of trade secret) cases as the process is time consuming. The PACER search method uncovered roughly 40 cases which were not issued DOJ press releases or included in the EEA prosecution table. 1831 (economic espionage) cases, given their political importance, are identified via DOJ. The 1831 cases may be subjected to the PACER method in the future.

Once identified, each case was then investigated via docket reports, court documents and online media coverage. An abbreviated sample of the data collected can be found in the appendix. The docket reports were the most consistent source of quantitative information and provided filing and termination dates, sentences, fines and conviction codes. Linked to some docket reports were court documents (e.g. plea agreements and the original criminal complaint) which contained qualitative information about the defendant, the alleged crime, and the victim.

Media reports often provided details on the victim's relationship to the defendant, alleged value of the stolen trade secrets and parallel civil actions. Further information was gathered from academic papers related to the EEA.²⁴ Depending on the court, official documents are only available from more recent cases; in some courts, the documents are only available for cases since 2004. For a minority of cases, little to no information on the victim company and stolen information was available.

For example, as seen in the appendix, the case of *US v. Petrolino*, filed on November 29, 2001 in the Southern District of Florida, shows that the defendant was not a foreigner, an outsider in relation to the victim company (First Union Securities, a bank) and stole

“securities broker customer and account information.” This stolen trade secret was not patentable or protected under copyright and the defendant sought to sell the confidential information for \$3,800. The defendant was convicted of Theft of Trade Secrets and sentenced to 24 months of probation and no financial punishment. The other 129 data points have similar information.

The information gathered in this prosecution data represents a unique look into the use of trade secrets, their theft and the policy choices available to governments.

4.1 Data bias

The use of prosecution data in economics faces a number of challenges and the EEA data is no exception. The primary obstacle is that of adverse selection. Prosecutors select cases based on the severity of the crime and the likelihood of successful prosecution. Thus, the sample set is unlikely to include minor thefts and more likely to include major thefts leading to a negative skew in the distribution of the prosecuted thefts in comparison to actual thefts. There are exceptions, however, when a prosecutor chooses to prosecute a specific defendant in the hopes of deterring other criminals. This was likely the case in *U.S. v. Genovese*²⁵ where the defendant was convicted based on the sale of Microsoft source code for \$20.

Prosecutors are also more likely to seek prosecution in cases where the evidence is strong and a conviction is likely. The EEA data has a conviction rate of 69% on at least one count (includes plea bargains), 11% not convicted and the remaining 20% still pending at the time of writing. This compares to an estimated 90% conviction rate in federal court²⁶ of all federal cases that go to trial. The majority of prosecutors is elected and therefore has an incentive to keep their conviction rates high to appeal to voters.²⁷ In order to maintain these high rates, weaker cases are turned away. According to Transaction Records Access Clearinghouse (TRAC), from 2000 to 2002, U.S. attorneys declined to prosecute 32% of cases referred to them by investigative agencies.²⁸ The referred cases have already been filtered as the agencies only refer cases deemed worthy of potential prosecution.

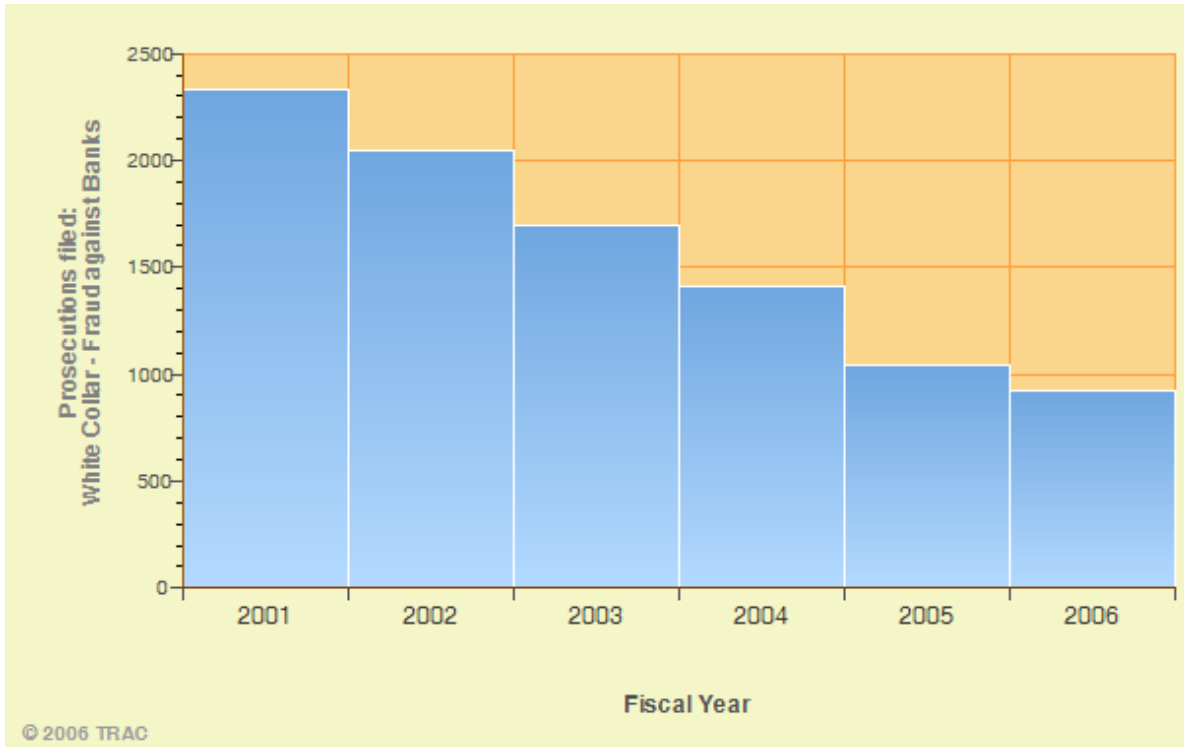
There is also concern that the shift in priorities towards combating terrorism has led to a decrease in the FBI's attention to white collar crime. FBI Assistant Director Chip Burrus “likened the FBI's current fraud-enforcement policies – in which losses below \$150,000 have

little chance of being addressed – to “triage.” Even cases with losses approaching \$500,000 are much less likely to be accepted for investigation than before 9/11.”²⁹ The shifting to cases with higher losses means that the EEA data will contain a distorted sample with an overrepresentation of high loss cases. Enforcement of White Collar Crime, as measured by prosecutions of fraud against banks has also been falling as seen in Figure 2. The decrease in the priority of white collar crime can further distort the data by including only strong cases.

<Figure 2 near here>

FBI Enforcement: White Collar Crime FY 2001-2006

Figure 2



From TRAC, accessed September 09, 2008 from <http://trac.syr.edu/cgi-bin/tracslides2.pl?id=fbi2005&slide=7>

A general argument based on the colloquial expression in the US that “only the stupid ones get caught,” could further distort the sample. If the intelligence of criminals and the level of sophistication of the crime are negatively correlated with detection and conviction, then the sample data will be biased towards less intelligent criminals committing simpler crimes. Unfortunately, intelligence measurements are not readily available in the EEA cases so this argument remains untested.

A final point further obfuscating the use of the prosecution data is the actual reporting of the theft of trade secrets. In order to seek prosecution, victims must first report the alleged crime to the FBI via an official document reporting the offense.³⁰ The decision to report is influenced by a number of factors including initial detection, fear of negative publicity and reputation costs, fear of having the trade secret made public during the process of prosecution and the burden of proving that the trade secret existed in the first place. These influences are further discussed later in the Section 8.

The cumulative effect of these challenges to the use of prosecution data is that conclusions arising from the data are tempered by the inherent sample bias. Despite this, it is important to remember that, given the nature of trade secrets, very little empirical data is available on their use. While the EEA data has its weaknesses, it gives us a unique insight into the use and theft of trade secrets. Economists have long used evidence from litigation³¹ to investigate the use of patents and their economic importance.³² The EEA offers a glimpse into the unseen world of trade secrets.

5. Composition of Defendants

To date, 130 defendants have been charged under the EEA. These defendants are alleged to have taken a trade secret from its legitimate owner. Given the economic espionage concerns that surrounded the birth of the EEA, the composition of the defendants themselves provides insight into the relevance of these concerns.

5.1 Relationship to the Victim

In order to commit the act of trade secret theft, the defendant had to be aware of and gain access to the trade secret. The data indicates that the threat is not external but internal. As shown in the last row of Table 1, the reality is that 75% of the defendants are insiders, 17% are outsiders and 8% have an unknown relationship. An “insider” is defined as a current or

former employee who includes permanent and temporary employees, consultants or workers performing contracted-out work (for a third party company.) These insiders had legitimate reasons to have knowledge of and at least partial access to the trade secret. In contrast, only 22 defendants were classified as outsiders which include competitors, non employees or other roles which do not provide legitimate access.

While the fact that insiders are disproportionately responsible for theft in EEA cases should come as no surprise, it highlights the vulnerability that trade secrets face when much of their protection is based on nondisclosure agreements and the implicit trust required to support them. It also indicates that some of the presumptions leading up to the signing of the EEA were misguidedly concentrated on outside threats when the focus should have been more on the internal threat to the security of trade secrets.

Table 1

Characteristics of Defendants								
	Total		Relationship to the Victim					
Nationality	Count	%	Outsider	%	Insider	%	Unknown	%
Foreign	29	22%	7	5%	22	17%		
National*	101	78%	15	12%	75	58%	11	8%
Total	130		22	17%	97	75%	11	8%

Source: EEA database as seen in Appendix 1.

*if nationality unknown, defendant assumed to be US national

5.2 Nationality

The nationality of the defendants presents another test to the original presumptions of the EEA. As seen in the second column of Table 1, only 22% of the defendants were foreign nationals with the remaining 78% either US nationals or nationality unknown. Of the 29 foreigners charged with EEA violations, only one was convicted under 1831 (Economic Espionage.)³³ Given the concern with economic espionage at the drafting of the EEA, these numbers indicate that either economic espionage is less prevalent than trade secret theft or its detection is more difficult. In the fourth column of Table 1, only 5% of defendants were both foreign and classified as an outsider. The remaining 17% of foreign defendants were classified as insiders which indicates that they had some form of formal employment relationship with the victim. However, given the relatively small sample size of only 22

foreigners, it is difficult to extend these estimates to make robust conclusions. Despite this, patriotism, nationalism and existing relationships make foreigners in the US prime recruitment targets for economic espionage. A 2008 review of 60 years of American spies revealed that foreign influences and loyalties play an increasing role in espionage.³⁴ While the role of monetary payoffs is likely an important motivation in economic espionage, nationalism can be a contributing factor.

6. Composition of Victims and Stolen Trade Secrets

In all EEA cases, the trade secrets and their legitimate owners have been the targets of trade secret theft. The composition of these targets can further explain the use of trade secrets.

6.1 Industrial Sectors of Victims

The EEA data also provides a look into the industries using trade secrets. The trade secret theft victim companies were identified and a Standard Industrial Classification (SIC) code assigned. For listed companies, this was done in a straightforward manner via the United States Securities and Exchange Commission (SEC) filing system Edgar³⁵. Where Edgar did not provide a code, a description of the company was obtained via Goliath Company Profiles³⁶ and then the SIC code cross referenced using the US Department of Labor's SIC Search System.³⁷ For 12 cases, the victim company was not identified.

Table 2 shows the results, grouped by the SIC divisions and, where larger than 5%, the SIC major group. Note that, in the majority (58%) of cases (based on cases, not number of defendants), the victim company operated in the manufacturing sectors. Of those in manufacturing, the largest groups include those in semiconductor manufacturing and manufacturers with software applications. The second largest sector is the service industry (17% of cases) and the remaining cases are scattered throughout other sectors.

The 1997 US Census³⁸ indicates that only 6% of establishments were classified as manufacturing. The largest sector is Service Industries which comprises 32% of all establishments and 20% of the EEA cases. Interestingly, the census lists Retail Trade as the second largest sector which accounts for 24% of all establishments but no EEA cases. The relative positions change slightly when the sectors are ranked by gross receipts (instead of number of establishments) where Manufacturing represents 22% of total gross receipts, Service Industries 10% and Retail Trade 14%.

The large discrepancy between the 58% of EEA cases and only 6% of establishments being in manufacturing suggests that trade secret theft is particularly important to the sector. Manufacturing is a fairly IP aware sector which has long had patents available as a robust form of protection. This long history with IP makes the industry aware of IP and their use of IP and its enforcement more likely. It is also possible that the relative concentrations of manufacturing make detection more likely. For example, the aerospace industry is dominated by two firms: Lockheed Martin and Boeing. Movement of employees between these two firms is easy to track and therefore trade secrets can be closely watched.³⁹

That the manufacturing sector, a sector which has long had patent and copyright protection available, should be so active in trade secrets, emphasizes the importance of trade secrecy protection. In the absence of this protection, the sector would have to alter its behavior to either shift towards greater reliance on patents and copyrights or enact potentially costly protection schemes to preserve the confidentiality of trade secrets.

<

Table 2 near here>

Table 2

Industries of Victims by SIC code: EEA Cases from 1996-2008		
Industry	Count	%
Agriculture, Forestry and Fishing	0	0%
Mining	0	0%
Construction	2	2%
Manufacturing	54	58%
<i>Electronic And Other Electrical Equipment And Components, Except Computer Equipment (Includes Semiconductors)</i>	14	15%
<i>Chemicals And Allied Products</i>	11	12%
<i>Industrial And Commercial Machinery And Computer Equipment</i>	9	10%
<i>Other</i>	20	22%
Transportation, Communications, Electric, Gas and Sanitary Services	3	3%
Wholesale Trade	2	2%
Retail Trade	0	0%
Finance, Insurance and Real Estate	4	4%
Services	16	17%
<i>Business Services</i>	11	12%
<i>Other</i>	5	5%
Public Administration	0	0%
Unknown	12	13%
Total	93	

Source: EEA database as seen in Appendix 1.

6.2 Subject Matter of Stolen Trade Secrets

Trade secrecy protection encompasses a large scope of confidential information including source code for software, test data, strategic business information and potentially patentable subject matters. In the EEA cases, as seen in Table 3 column 2, only 41% of the stolen trade secrets are deemed potentially patentable (meaning that their subject matter is not excluded from patents; inventive step was not judged.) 10% of stolen trade secrets had no descriptive information. Of the remaining 49%, which is comprised of diagrams, pricing information, test data, marketing plans, software code etc, 20% of the stolen trade secrets have the potential to receive either trademark or copyright protection. This 20% is predominately source code for computer software programs. The other 29% had only trade secrecy as a form of IP protection which means that this confidential is particularly vulnerable and its theft particularly damaging. Table 3 shows the summary statistics of the characteristics of these stolen trade secrets.

Table 3

Characteristics of Stolen Trade Secrets: EEA Cases from 1996-2008		
Type	Count	%
Potentially patentable	38	41%
Not patentable	46	49%
<i>Protected by other IP</i>	<i>19</i>	<i>20%</i>
<i>Not protected</i>	<i>27</i>	<i>29%</i>
Unidentified	9	10%
Total	93	

Source: EEA database as seen in Appendix 1.

It is important to emphasize that these classifications are based on limited information regarding the nature of the stolen trade secrets. Given the requirements for patent protection, Table 3 probably represents an overestimation of the number of stolen trade secrets that are potentially patentable. Additionally, copyright can be insufficient protection for software source code; reverse engineering is relatively easy and the information contained in source code allows competitors to develop add-on programs which may compete with the source code owner's other products. Thus, this table likely overstates the number of trade secrets

that could rely on other IP protection. The fact that these trade secret owners chose not to use those alternate protections is further evidence of the importance of trade secret protection.

7. Value Estimation

The value of the stolen trade secrets is of great interest to economics as it gives insight into the relative importance of trade secrecy protection for firms. In EEA cases, sentencing guidelines link the alleged value of the stolen property to recommended fines and imprisonment. What actually constitutes the value varies depending on the estimation method. Often, the estimation is based not on the fair market value of the trade secret (the value a willing buyer and a willing seller would agree on) but the losses suffered by the victim.⁴⁰ As the fair market value of the trade secret in EEA cases cannot be measured directly (due to information asymmetries, lack of a willing seller and a willing buyer etc.), loss estimation often provides a close substitute. In this section, the estimation methods used in EEA cases is described and their highly heterogeneous results analyzed.

As in patent disputes, the determinants of the valuation of IP fall under two main categories: lost profits and reasonable royalty.⁴¹ In cases of trade secret theft, the theft element adds additional methods: unjust enrichment, replacement costs, research and development costs, direct costs arising from the theft (detection, prosecution, damage control etc.) and the value which the accused believed the stolen trade secret to be worth.⁴² Following Zwillinger and Genetski (2000), these methods are lumped into four categories: unjust enrichment, lost profits, reasonable royalty and replacement costs or research and development costs. In the EEA cases reported here, the valuations have been obtained from a combination of court documents, media reports and academic papers.

Due to the highly heterogeneous nature of the valuations, a high and low value (as in Carr and Gorman (2001)) of the trade secrets was collected for the EEA cases. These values are reflected in

Table 4. Unfortunately, due to the lack of a consistent official source for these estimates, estimates are only available for one third of the EEA cases.

Table 4

Value Estimates for Stolen Trade Secrets in EEA Cases 1996-2008		
	Low Estimate	High Estimate
Average	\$6,738,970	\$57,009,956
Median	\$500,000	\$2,000,000
Minimum	\$5,000	\$9,045
Maximum	\$100,000,000	\$600,000,000

Source: EEA database as seen in Appendix 1.

7.1 Unjust Enrichment

Under the doctrine of unjust enrichment, the value or loss estimation is determined by the profits gained by the defendant from the use of the stolen trade secret. The goal is to determine the thieves’s financial gain from the theft. According to Zwillinger and Genetski (2000) this is typically used when the victim suffered no actual loss or the loss does not fairly represent the value of the trade secret.⁴³ The difficult is determining the amount directly related to the trade secret as the trade secret is unlikely to be used independently of other inputs (e.g. marketing, other intellectual property, raw materials etc.) Courts can either determine all profits related to the trade secret as tainted or attempt to estimate what portion of the profits were directly related to the trade secret.

In the EEA case of U.S. v. Keppel⁴⁴, the value of the goods was determined to be between \$500,000 and \$800,000 where \$800,000 was the “amount of the defendant’s gain from committing the offense.”⁴⁵ A press release by the Department of Justice reported that Keppel had two bank accounts, one with deposits totaling \$756,633 which resulted from sales of Microsoft Certified Systems Engineer and Microsoft Certified Solution Developer tests and another, with an unspecified amount, from sales of “proprietary information belonging to Microsoft Corporation, Cisco and other business.”⁴⁶ In this case, the court applied the unjust enrichment doctrine and allocated all of the sales from the first account and an unknown portion of the second account for the upper bound of the loss estimate. However, the plea

agreement also states that “The parties agree that the actual loss amount is extremely difficult to ascertain.”⁴⁷

Related to unjust enrichment is the value which the thief sold or attempted to sell the stolen trade secrets. Given the criminal theft of the IP in question, this differs from the typical IP infringement case because the thief may not have intended to exploit the trade secret but simply profit from its black market value. The black market value is typically less than the full market value given that the thief may not have an accurate estimate of the value the market is willing to bear nor the value to the legitimate owner. An example is the *Genovese* case where the thief sold the stolen Windows source code for \$20 which hardly begins to approach the value to Microsoft of the Windows programs which are considered the “crown jewels”⁴⁸ of the corporation. The potential financial harm and loss of strategic advantage to Microsoft is not reflected in the black market \$20 price tag. Compare this to the case of *U.S. v. Trujillo-Cohen*⁴⁹ in which the defendant attempted to sell her employer’s proprietary software to a competitor for a reported \$7 million.⁵⁰ The amount the thief attempt to profit from, the accuracy of their estimation and whether or not they actually managed to sell can greatly affect the valuation.

7.2 Lost Profits

Calculating the victim’s lost profits is another standard valuation method. Under the lost profits doctrine, the damages (losses) are calculated as the financial disadvantage (measured in profits) the trade secret owner suffered as a result of the theft. Restoration of these profits makes the owner whole but for the theft. This estimation requires predicting the counterfactual (profits without the theft) and comparing this to the factual (profits with the theft.) The difficulty is that the counterfactual cannot be directly observed and must be estimated taking into account market conditions, the portion of profits directly related to the trade secrets and other factors such as each firm’s market capitalization. For example, if a company with a small market has its trade secrets stolen and used by company with a large market, then the lost profits of the company with the smaller market may be relatively small compared to the unjust enrichment of the other company.

Another difficulty is accounting for the portion lost as a result of the theft. In the *U.S. v. Branch and Erskine* case, stolen strategic business information aided Boeing in winning 19 out of 28 contracts worth a total of \$2 billion. The victim company, Lockheed Martin, was awarded the remaining nine. Would it be appropriate to value the stolen trade secret as the total value of the 19 contracts? A series of criminal and civil actions resulted in Boeing losing some of the contracts and being fined \$625 million.⁵¹ The lost profits doctrine suffers when the contribution to profits of the trade secrets is unclear and when the actual lost profits do not accurately reflect the value of the trade secret.

Related to loss profits is the out-of-pocket expenses incurred as a direct result of theft. An example is the \$68,000 incurred by DirecTV⁵² in tracking down the source of a trade secret disclosure and mitigating damages in *U.S. v. Serebryany*.⁵³ The trade secrets disclosed related to bypassing restrictions in conditional access cards for subscription television. The potential for lost profits and the \$25 million DirecTV spent on developing the access cards are not reflected in the \$68,000 incurred as a direct result of the theft. Furthermore, these out-of-pocket expenses could be interpreted as the cost of doing business and the general costs associated with obtaining the “reasonable” protection required to achieve trade secret status. In this case, however, the defendant sought no financial gain from the trade secrets and was ordered to pay \$146,085 in restitution.

7.3 Reasonable Royalty

A popular method of determining values and damages in IP cases is the principle of reasonable royalty. This method estimates the damages by calculating the amount for which the trade secrets would have been licensed. The royalty is “based on the amount that a willing buyer would have paid a willing seller to license the stolen trade secret.”⁵⁴ However, as pointed out in Shankerman and Scotchmer (2001), there is some circularity in the fact that damages are determined by reasonable royalty while, at the same time, royalties are affected by the damages assessed. If a royalty exceeds expected damages sufficiently, a potential licensor may find it more profitable to steal, rather than license, the trade secret. As Zwillinger and Genetski (2001) note, reasonable royalty is a useful tool in EEA cases as the defendants are often unable to exploit the trade secrets before being caught. However, it remains difficult for courts to estimate the amount considered reasonable as it requires

conjecturing what the parties would have agreed to in normal license negotiations. Despite the assertion that reasonable royalty is particularly useful, this research has uncovered no evidence of its use to date in EEA cases.

7.4 Research & Development and Replacement Costs

A final, but problematic, method of valuation is that of replacement or Research & Development costs. According to Research & Development costs, the value is the amount invested by the trade secret owner to develop the trade secret. The replacement cost is the amount the defendant would have spent to independently develop the trade secret. These two techniques can vary as the defendant had the option of reverse engineering the trade secret and therefore saving on research costs whereas the legitimate owner may have started from a blank canvas and may have invested in other costly but failed projects before the successful project. Additionally, development costs may not accurately reflect the value of the trade secrets. A brilliant flash of insight may cost a trade secret owner very little while an arduous process of developing a new formula, for example, may incur years of salaries and inputs. As Zwillinger and Grenetski (2000) note,

“Research and development overstates the loss because when someone steals a trade secret, the theft rarely deprives the owner of the trade secret from the full value of the stolen technology... Conversely, research and development costs understate the fair market value of stolen trade secrets because rational actors will not invest \$5 million to develop information that will be worth only \$5 million. Instead, a company invests \$5 million only with the expectation of producing a significant return on the investment.”⁵⁵

Thus, neither of these costs may reflect the added value to the trade secret owner.

Some examples of the discrepancies created using the replacement costs and other methods can be found in the EEA cases. In the DirecTV case mentioned earlier, the technology cost the company \$25 million to develop, \$68,000 to detect the leak of its trade secrets and then the cards in question were replaced within two years due to compatibility problems.⁵⁶ The stolen Microsoft tests cost the company \$200,000 to develop⁵⁷ but were valued at \$500,000 to \$800,000 in court documents. In *U.S. v. Krumrei*,⁵⁸ the defendant stole trade secrets related to a laminate that cost the company \$31.4 million to develop,⁵⁹ which the defendant attempted to sell for \$350,000⁶⁰ and was ultimately required to pay \$10,000 in restitution.

These heterogeneous values demonstrate the highly variable estimates stemming from the various methods of loss and value estimation of trade secrets.

8. Criminalization and Detection

In order to have a true picture of the evidence found in the EEA prosecutions, it is important to examine the external effects created by the advent of criminal prosecutions of trade secrecy theft. The EEA offers firms a means of seeking criminal, in addition to the existing civil, actions against trade secret thefts. It also affects the behavior of employees and increases the potential punishment associated with theft.

8.1 Comparison to Civil Actions

Lerner (2006) investigates trade secret litigation for insights into trade secrets and compares this data to similar data on patent litigation. He notes that “In those cases where the damages were determined, they averaged \$1.5 million in 2004 dollars. This is less than one-third the mean level of damages in the patent cases examined by Moore [2000].”⁶¹ In the EEA cases, which do not exclude the possibility of parallel civil cases, defendants are subject to fines, forfeitures and restitution. The victim can benefit from restitution but does not necessarily receive the benefits of fines and forfeitures. The median restitution was \$193,043 which is just over one tenth of the damages in Lerner’s cases. The average restitution of \$1.6 million more closely resembles Lerner’s average but has an upward bias due to a number of high awards.

Table 5 contains the medians, minima and maxima for the fines, forfeitures and restitutions levied against EEA defendants.

<Table 5 near here>

Table 5

EEA Fines, Forfeitures and Restitutions, 1996-2008			
	Fine	Forfeiture	Restitution
# of defendants (%)	34 (26%)	1 (1%)	30 (23%)
60 (46%) defendants were subject to fine, forfeiture and/or restitution			
Average	\$76,482	\$60,000	\$1,565,455
Median	\$5,000	\$60,000	\$193,043
Minimum	\$500	\$60,000	\$500
Maximum	\$2,000,000	\$60,000	\$7,655,155

Source: EEA database as seen in Appendix 1.

An obvious difference from civil cases is the incarceration penalties associated with criminal cases. In EEA cases, as noted in Table 6, 65% of all defendants were sentenced to some form of incarceration, house arrest, probation or supervised release. 64% of defendants were sentenced to probation which averaged 33 months. Only 38% of defendants were incarcerated for an average of 22 months. However, as the conviction rate of EEA cases is 69%, this data indicates that 94% of those convicted in EEA cases receive some form of incarceration. 5 corporations are included in that conviction rate and are not subject to incarceration; therefore, virtually all individuals convicted in EEA cases receive incarceration and/or probation sentences.

Table 6

EEA Incarceration and Probation, 1996-2008		
	Incarceration	Probation
# of defendants (%)	50 (38%)	84 (64%)
85 (65%) defendants were subject to incarceration (including house arrest) and/or probation (including supervised release)		
Average (in months)	22	33
Median	13	36
Minimum	2	12
Maximum	96	60

Source: EEA database as seen in Appendix 1.

Further work remains to be done on the comparison of the EEA criminal cases to trade secret civil cases. This work should provide insights into the policy differences between criminal and civil cases, the effects of the escalation of trade secrets to a felony and the influence on firms' behavior.

8.2 Detection and Reporting by Victims

In EEA cases, all of the victims have been corporations, not individuals. The decision of these firms to detect, investigate, report and proceed with criminal prosecution involves a complex weighing of costs and benefits as opposed to civil cases.

8.2.1 Benefits

From a resource perspective, a decision to seek a criminal prosecution involves a number of benefits to the victim firm. Due to the defendant's right to a speedy trial, criminal cases cannot drag on as long as civil cases. As a result, the victim firm will save itself time and money by not being involved in a lengthy, distracting, resource-absorbing court case. In addition, in criminal cases, the cost of prosecution (lawyer's fees, court fees etc.) is borne by the government and not the victim. This is not the case with a civil case in which the plaintiff must pay their own lawyer's fees and may face expensive countersuits.

The moral benefits of choosing criminal prosecution of a trade secrets theft include the ability to prosecute judgment-proof defendants, stronger sense of retribution and a potentially stronger enforcement message. As trade secrecy theft can be committed by defendants with no financial resources, a civil suit resulting in damages can be a moot point as the defendant is unable to pay (i.e. judgment proof.) The criminal system avoids this problem by including the option of incarceration as a form of punishment. Incarceration may have a stronger sense of retribution for trade secret victims as trade secret thieves are removed from the workplace and society at large. This incarceration also sends a strong enforcement message and decreases the expected benefits of theft.

8.2.2 Costs

The primary resource cost associated with criminal prosecutions in EEA cases is lower financial damages, as noted in Section 8.1. If a victim's primary goal is to seek financial damages, then a criminal prosecution alone will not satisfy that goal. However, a criminal action against the defendant does not preclude a parallel civil action. Victims can choose to seek both a criminal and a civil action and thereby not suffer the lower damages. Trade secret cases also run the risk of exposing the secret to the public, however the EEA includes confidentiality requirements.⁶²

From a moral perspective, the costs of choosing a criminal prosecution include reputational and control costs. As with civil cases, the revelation that a company has been the victim of a trade secrets theft can damage its reputation. The market may view the theft as evidence of lax security standards or future potential liability.⁶³ However, criminal charges are likely to have particularly adverse effects on a firm's relationship and reputation with its employees. As the EEA data demonstrates, the majority of defendants are insiders and employees may object to the criminal prosecution of one of their colleagues. Increased distrust can change company culture and lower social capital within a firm.

In addition, criminal prosecution requires that the firm relinquish control over the action to the government. The FBI will be in charge of the investigation and federal prosecutors will make important decisions related to the case. This loss of control presents a risk not associated with civil cases where the plaintiff has significant control over the course of the case.

The victim firm faces a number of options when confronted with a theft of trade secrets: do nothing, discharge the offending employee or seek legal recourse in the form of criminal and/or civil actions.⁶⁴ As noted, the decision to seek criminal action involves a number of financial and moral costs not associated with civil actions. At the same time, the moral and financial benefits may make a criminal action worthwhile. The firms in the EEA cases, by definition, weighed these costs and benefits ex-ante and proceeded with reporting the crime.

From both an empirical and theoretical perspective, the comparison between the civil and criminal actions in trade secrecy cases and firms's decisions present a potentially fruitful research area. One possibility will be identifying the companion civil cases to the criminal EEA cases. Further work will need to be done in investigating the EEA data for evidence of these important issues.

9. Conclusion

The EEA marked a change in the US approach to trade secret theft and the threat of economic espionage. It also offered researchers an unprecedented opportunity to gain insight into the

use of trade secrets by US firms and their theft. While the data suffers from some biases, it nonetheless provides a heretofore unavailable look into the world of trade secrets.

The 130 defendants in 93 cases of the EEA since its inception in 1996 until the time of writing in 2008 demonstrate that some of the original concerns of the drafters of the act were misguided. Insiders to firms present the largest threat to trade secrets and are responsible for the vast majority of thefts. Foreigners, the initially suspect group of economic spies, have turned out to be less of a concern, or at least a less detected problem than originally anticipated. The industry reporting the most thefts is the manufacturing sector which suggests that trade secrets are of particular importance to these firms and their enforcement a priority. Finally, the nature of the trade secrets in EEA cases reveals that a mere 41% of them could be patented. Even with this liberal estimate, the choice of trade secrecy by firms indicates that the firms view trade secrets as an important IP tool and that these secrets are particularly vulnerable.

The value of the stolen trade secrets remains somewhat of a mystery, given the various methods of valuation. Considering that the estimated value is a factor in both deciding which cases to prosecute and determining fines and incarceration sentences, these value estimates have important implications within the legal system. The economic implications of these estimates provide insight into the use of trade secrets and their relative value to US firms. These values also play a role in the decision making process of firms, when confronted with a trade secret theft.

This paper suggests how EEA data create a promising first step towards developing more thorough empirical analyses of trade secrets and their use. The data are suggestive of further areas of potential research. These include a more detailed comparison of criminal versus civil cases, theoretical modeling (including game theoretic analysis), and econometric modeling (e.g. of the relations between the value of trade secret theft and severity of punishment of theft.)

Bibliography

- Anton, James J. and Dennis A. Yao (2004), "Little Patents and Big Secrets," *RAND Journal of Economics*, 35:1, 1.
- Arundel, Anthony (2001), "The relative effectiveness of patents and secrecy for appropriation," *Research Policy*, 30, 611-624.
- Bessen, James E. (2004), "Patents and the Diffusion of Technical Information," Available at SSRN: <http://ssrn.com/abstract=517024> 9.
- Bhattacharya, Sudipto and Sergei Guriev (2006, "Patents vs. Trade Secrets: Knowledge Licensing and Spillover," *Journal of the European Economic Association*, 4:6, 1112-1147.
- Denicolo, Vincenzo (1996), "Patent Races and Optimal Patent Breadth and Length," *The Journal of Industrial Economics*, 44:3, 249-265.
- Carr, Chris and Larry Gorman (2001), "The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act," *The Business Lawyer*, 57:1, 25-53.
- Carr, Chris, Morton, Jack and Jerry Furniss (2000), "The Economic Espionage Act: Bear Trap or Mouse Trap?" *Texas Intellectual Property Law Journal*, 8:2, 159-209.
- Chang, Howard (1995), "Patent Scope, Antitrust Policy and Cumulative Innovation," *The RAND Journal of Economics*, 26:1, 34-57
- Cohen, Wesley M., Richard R. Nelson and John P. Walsh (2000), "Protecting their Intellectual Assets: Appropriability Condition and Why U.S. Manufacturing Firms Patent (or Not)," *National Bureau of Economic Research*, 7552.
- Cugno, Franco and Ottoz, Elisabetta (2006) "Trade Secret vs. Broad Patent: The Role of Licensing," *Review of Law & Economics: Vol. 2 : Iss. 2, Article 3*. Available at: <http://www.bepress.com/rle/vol2/iss2/art3>
- Effron, Robin (2003), "Secrets and Spies: Extraterritorial Applications of the Economic Espionage Act and the TRIPS Agreement," *New York University Law Review*, 78:1475.
- Encaoua and Lefouli (2006), "Choosing Intellectual Protection: Imitation, Patent Strength and Licensing," *CESIFO working paper 1715*.
- Erkal, Nisvan (2005), "The Decision to Patent, Cumulative Innovation and Optimal Policy," *International Journal of Industrial Economics*, 25, 535-562.
- Fialka, John J. (1997), War by Other Means: Economic Espionage in America, W.W. Norton & Company, New York.
- Gallini, Nancy (1992), "Patent Policy and Costly Imitation," *The RAND Journal of Economics*, 23:1, 52-63.

- Gilbert, Richard and Carl Shapiro (1990), "Optimal Patent Length and Breadth," *The RAND Journal of Economics*, 21:1, 106-112.
- Herbig, Katherine (2008), "Changes in Espionage by Americas: 1947-2007," *Department of Defense*, Technical Report 08-05.
- Hodkinson, Keith and Martin Wasik (1986), Industrial Espionage Protection and Remedies, Longman, London.
- Klemperer, Paul (1990) "How Broad Should the Scope of Patent Protection Be?," *The RAND Journal of Economics*, 21:1, 113-130.
- Kotabe, Masaaki (1992), "A Comparative Study of U.S. and Japanese Patent Systems," *Journal of International Business Studies*, 147-168.
- Lanjouw, Jean and Mark Shankerman (2004), "Protecting Intellectual Property Rights: Are Small Firms Handicapped?," *Journal of Law and Economics*, XLVII, 45-75.
- Lanjouw, Jean and Mark Shankerman (1997), "Stylized Facts of Patent Litigation: Value, Scope and Ownership," *National Bureau of Economics Research*, Working Paper 6297.
- Lerner, Josh, Using Litigation to Understand Trade Secrets: A Preliminary Exploration(August 2006). Available at SSRN: <http://ssrn.com/abstract=922520>
- Lerner, Josh and Adam B. Jaffe (2004), Innovation and Its Discontents: How Our Broken Patent System is Endangering Innovation and Progress, And What to Do About It, Princeton Paperbacks, Princeton, New Jersey.
- Nasheri, Hedeih (2005), Economic Espionage and Industrial Spying, Cambridge University Press, Cambridge, Massachusetts.
- Park, Juan C. and Walter G. Park (1997), "Determinants of Patent Rights: A Cross-National Study," *Research Policy*, 283-301.
- Scotchmer, Suzanne (2005), Innovation and Incentives, Massachusetts Institute of Technology, Cambridge, Massachusetts.
- Shankerman, Mark and Suzanne Scotchmer (2001), "Damages and Injunctions in Protecting Intellectual Property," *RAND Journal of Economics*, 32:1, 199-220.
- Slottje, Daniel, ed. (2006), Economic Damages in Intellectual Property, John Wiley & Sons, New Jersey.
- Uhrich, Craig (2001), "Economic Espionage Act, Reverse Engineering and Intellectual Property Public Policy," *Michigan Telecommunications Technology Law Review*, 147.
- Zwillinger, Marc and Christian Genetski (2000), "Calculating Loss Under the Economic Espionage Act of 1996," *George Mason Law Review*, 9:2, 323-356.

Appendix 1: EEA Database Example

Category of Information	Case Information			Characteristics of Defendant		Characteristics of Trade Secret						Characteristics of Victim		Conviction and Punishment						
Source	Docket Reports from PACER			Docket Reports, Media Reports, Academic Papers		Docket Reports, Media Reports, Academic Papers						Docket Reports, Media Reports, Academic		Docket Reports						
Variables	Colloquial Case Name (District)	Filing Date	District	Dummy Nationality (1=foreign)	Insider/Ex vs. Outsider Dummy (1=outsider)	Type of Information Stolen	Potentially Patentable Dummy, 1=yes	Potentially TM or Copyrightable Dummy, 1=yes	Alleged worth of stolen items (low)	Alleged worth of stolen items (high)	Proposed or Actual Sale Price	Victim Company	Victim SIC	Conviction Code	Incarceration	Probation	Total financial punishment	Fine	Forfeiture	Restitution
Definition of Variable	US v. Last Name of Defendant	Date case filed in district court	District and State of court case (S.D. = Southern District, C.D. = Central District, etc.)	Nationality dummy, 1 = foreign or dual nationality, 0 = unknown or US national	Relationship to the victim, 1 = outsider, 0 = insider, N/A = not available	Brief description of the stolen trade secret.	Determines whether stolen trade secret was potentially patentable, 1 = yes, 0 = no, N/A = not available	Stolen trade secret was potentially protected under copyright or trademark, 1 = yes, 0 = no, N/A = not available	Low estimate of stolen trade secrets in dollars	High estimate of stolen trade secrets in dollars	Dollar amount the defendants were seeking to gain from the sale of the information to others	The legitimate owner of the stolen trade secret	SIC code of victim	Convicted offenses by US Criminal Code, 0 = no conviction, 1832 = Theft of Trade Secrets	Sentence in months of incarceration and home confinement	Sentence, in months, of probation and supervised release	Total amount of Fines, Forfeiture and Restitution	Dollar amount of all fines levied against defendant	Dollar amount of forfeiture assessed against defendant	Dollar amount the defendant is required to compensate the victim
Sample Cases	US v. Campbell (Susan)	February 25, 1998	N.D. CA	0	0	Confidential and proprietary information	0	0	150,000	800,000	150,000	Cray Comm.	4833	0	0	0	0	0	0	0
	U.S. v. Petrolino	November 29, 2001	S.D. FL	0	1	securities broker customer and account information	0	0	N/A	N/A	3,800	First Union Securities	6189	1832	0	24	0	0	0	0
	US v. Tejas Procurement Services	December 9, 1999	N.D. TX	0	0	Plan for oil field and pipeline machinery	1	0	7,650,000	200,000,000	100,000	Caterpillar	3531	1832	0	60	7,655,155	0	0	7,655,155
	US v. Krumrei	October 28, 1996	E.D. MI	0	0	Floor coating machine	1	0	31,400,000	31,400,000	350,000	Wilsonart (owned by Illinois Tool Works: ITW)	3083	1832	24	24	10,000	0	0	10,000
	U.S. v. Serebryany	January 16, 2003	C.D. CA	1	0	access card control information	0	1	68,000	25,000,000	N/A	DirecTV	4841	1832	0	60	145,900	0	0	145,900

The above table represents an abbreviated sample of the information contained in the EEA database created as part of this research. In the interest of space, a number of variables (e.g. dropped charges, number of co-defendants and descriptive information) have been omitted.

End notes

¹ In addition to press coverage, there have been at least three books written on Coca-Cola and the formula in the last 18 years - *Secret Formula: How Brilliant Marketing and Relentless Salesmanship Made Coca-Cola the Best-Known Product in the World* by Frederick L. Allen (1995), *For God, Country, and Coca-Cola: The Definitive History of the Great American Soft Drink and the Company That Makes It* by Mark Pendergrast (2000), *The Real Thing: Truth and Power at the Coca-Cola Company* by Constance L. Hays (2004)

² For a discussion on the Coke folklore, see <http://www.snopes.com/cokelore/formula.asp> by Barbara Mikkelsen

³ CNN online, May 7th, 2006, “3 arrested in Coca-Cola trade secret scheme”, Accessed 12/09/2008 from http://money.cnn.com/2006/07/05/news/companies/coke_pepsi/

⁴ *U.S. v. Williams et al*, Criminal Case 1:06-cr-00313-JOF-GGB (Northern District of Georgia, filed July 11, 2006.)

⁵ For further information, see the WTO’s website on TRIPS http://www.wto.org/english/tratop_e/TRIPS_e/TRIPS_e.htm

⁶ See Fialka (1997)

⁷ Effron (2003) p. 1485

⁸ As noted in Carr and Gorman (2001), p 30

⁹ Carr, Moron and Furniss (2000), Carr and Gorman (2001), Nasheri (2005)

¹⁰ As noted in Effron (2003) and Fialka (1997)

¹¹ Fialka, John, *War by Other Means: Economic Espionage in America*, 1997, Chapter 8, pp 87-112.

¹² Fialka (1997), Chapters 4, 5, pp 41-65.

¹³ Carr and Gorman (2001), p 31

¹⁴ Effron (2003), p. 1487.

¹⁵ 18 U.S.C. §1839, Definitions.

¹⁶ 18 U.S.C. §1837

¹⁷ *U.S. v. Cartwright et al*, Criminal case 1:07-cr-00570-WMN (District of Maryland, filed January 7, 2008)

¹⁸ *U.S. v. Okamoto*, Criminal case 1:01-cr-00210-DDD-1 (North District of Ohio, filed May 8, 2001)

¹⁹ Pearson, Natalie Obiko, March 29, 2004, “Tokyo Rejects Extradition of Alleged Spy”, *Associated Press*, Accessed September 08, 2008, from http://www.economicespionage.com/tokyo_rejects_extradition_of_all.htm

²⁰ Urich (2001), p. 179

²¹ Press releases available from <http://www.usdoj.gov/criminal/cybercrime/index.html>

²² Available from <http://www.usdoj.gov/criminal/cybercrime/eeapub.htm>

²³ Available from <http://www.usdoj.gov/criminal/cybercrime/ipnews.html>

²⁴ Particularly Effron (2003), Carr, Morton and Furniss (2000), Carr and Gorman (2001), Zwillinger and Genetski (2000) and Nasheri (2005).

²⁵ *U.S. v. Genovese*, Criminal case 1:05-cr-00004-WHP (Southern District of New York, filed January 4, 2005)

²⁶ From <http://www.masscriminal-lawyers.com/pages/types/whitecollarcrimes.html>

²⁷ From http://www.lovefraud.com/06_legalSystemFailures/scant_prosecution.html

²⁸ From http://www.lovefraud.com/06_legalSystemFailures/scant_prosecution.html The TRAC website is <http://trac.syr.edu/tracfbi/>

²⁹ Shukovsky, Pual, Johnson, Tracy and Daniel Lathrop, April 11, 2007, “The FBI’s terrorism trade-off,” *The Seattle Post-Intelligencer*, accessed September 09, 2008 from http://seattlepi.nwsourc.com/printer2/index.asp?ploc=t&refer=http://seattlepi.nwsourc.com/national/311046_fbiterror11.html

³⁰ Via their local FBI office, reporting form is “Checklist for Reporting Theft of Trade Secret Offense”, available from <http://www.usdoj.gov/criminal/cybercrime/reportingchecklist-ts.pdf>

³¹ Patent litigation has many parallels with trade secret prosecution in that it requires detection of the infringement, the decision to prosecute and a selection bias from the fact that only a minority of patents are litigated and, of those, a further share are settled in out of court decisions.

³² For example, Lanjouw and Shankerman (1997, 1999, 2001, and 2004), Shankerman and Scotchmer (2001), Jaffe and Lerner (2004)

³³ Source: Excerpt from EEA database as seen in Appendix 1.

³⁴ Herbig (2008)

³⁵ <http://www.sec.gov/edgar.shtml>

³⁶ http://goliath.ecnext.com/coms2/page_subscribe_compint

³⁷ <http://www.osha.gov/pls/imis/sicsearch.html>

³⁸ The 1997 Economic Census: Comparative Statistics for United States available from <http://www.census.gov/epcd/ec97sic/E97SUS.HTM>

³⁹ *US v. Branch and Erskine*, Criminal case 2:03-cr-00715-RSWL-1 (Central District of California, filed July 17, 2003).

-
- ⁴⁰ Zwillinger and Genetski (2000) p 324
- ⁴¹ Slottje (2006) lists four: lost profits, price erosion, entire market value and reasonable royalty. Here, I lump the first three into lost profits. Price erosion is the lowering of the price due to patent infringement and entire market value allows for damages to be calculated based on the entire value of the infringing good when the infringed patent is the basis for demand. As Slottje notes, both of these are included in lost profits (pp 8-9.)
- ⁴² Slottje (2006) p 267 identifies five main categories of damages calculations in trade secret theft: value of the trade secret to the plaintiff, lost profits, price erosion, unjust enrichment and reasonable royalty. Here, I identify all the methods used in my data collection.
- ⁴³ Zwillinger and Genetski (2000), p. 331
- ⁴⁴ U.S. v. Keppel, Criminal case 3:02-cr-05719-RBL, (Western District of Washington, filed August 8, 2002)
- ⁴⁵ See case US v. Keppel, Document 10, Plea Agreement, p. 3
- ⁴⁶ U.S. DOJ Western District of Washington (August 23, 2002), "Former Vancouver, Washington, Resident Pleads Guilty to Theft of Trade Secrets from Microsoft Corporation," Accessed July 07, 2008 from <http://www.usdoj.gov/criminal/cybercrime/keppelPlea.htm>
- ⁴⁷ See case US v. Keppel, Document 10, Plea Agreement, p. 3
- ⁴⁸ Department of Justice, Southern District of New York (August 29, 2005), "Connecticut Man Pleads Guilty in US Court to Selling Stolen Microsoft Windows Source Code," Access June 15, 2008 from <http://www.usdoj.gov/criminal/cybercrime/genovesePlea.htm>
- ⁴⁹ U.S. v. Trujillo-Cohen, Criminal case 4:97-cr-00251-1, (Southern District of Texas, filed on November 14, 1997)
- ⁵⁰ Wiggin and Dana, White Collar Defense (1998), "Investigations and Corporate Compliance Advisory, Theft of Trade Secrets," 2:2 available from http://www.wiggin.com/pubs/advisories_template.asp?GroupName=White-Collar+Defense%2C+Investigations+%26+Corporate+Compliance&ID=143715822000
- ⁵¹ Statement of Deputy Attorney General Paul J. McNulty before the Senate Committee on Armed Services, August 1, 2006, available from <http://www.usdoj.gov/archive/dag/testimony/2006/080106dagmcnultystatementsenate.htm>
- ⁵² Poulsen, Kevin, April 24, 2003 "DirecTV Mole to Plead Guilty", Security Focus, accessed August 04, 2008 from www.securityfocus.com/print/news/4173
- ⁵³ U.S. v. Serebryany, Criminal case 2:03-cr-00042-LGB (Central District of California, filed on January 16, 2003)
- ⁵⁴ Zwillinger and Genetski (2000), p. 332
- ⁵⁵ Zwillinger and Grenetski (2000), pp 344-345
- ⁵⁶ "DirecTV - Access Card History, D1 replaces P4," accessed September 07, 2008 from http://www.experiencefestival.com/a/DirecTV_-_Access_Card_History/id/4986861
- ⁵⁷ Two tests at \$100,000 each from DOJ press release, "Former Vancouver ..."
- ⁵⁸ U.S. v. Krumrei, Criminal case 2:98-cr-80943-DPH-1 (Eastern District of Michigan, filed on October 28, 1998)
- ⁵⁹ Honolulu Star Bulletin, News Briefs May 15, 1998, "Attorney accused of industrial espionage", accessed May 20, 2008 from <http://starbulletin.com/98/05/15/briefs.html>
- ⁶⁰ See U.S. v. Krumrei, Court document 47 related to appeal case #99-2500, 2001 Fed App. 0241P (6th Cir.)
- ⁶¹ Lerner (2006) p. 13 referring to Moore, Kimberly, 2000, "Judges, Juries, And Patent Cases — An Empirical Peek Inside the Black Box," *Michigan Law Review*, 99, 365-409.
- ⁶² 18 U.S.C. §1835, "Orders to preserve confidentiality"
- ⁶³ As noted in Carr and Gorman (2001)
- ⁶⁴ Hodskin and Wasik (1986)