May 31, 2011

The Economic Espionage Act: Is the Law All Bark and No Bite

Nathaniel J Minott, Harvard Law School

Available at: https://works.bepress.com/nathaniel_minott/1/
Synopsis

The Economic Espionage Act suffers from an insurmountable enforcement problem and is thus unlikely to ever be effective in stemming the tide of economic espionage besieging U.S. corporations. Passed in 1996, the EEA has never enjoyed the sort of government backing that foreign espionage agencies targeting the U.S. have received from their governments. That is because from day one, the individual lawyers who would actually use the EEA have been reluctant to do so in the face of excessive political pressure, heavy evidentiary burdens, and feeble institutional support. This paper seeks to isolate and explain the manifold issues presented by the EEA and hopes to demonstrate the fact that economic espionage as a general matter can not be addressed by a the EEA, or any domestic statute for that matter.

Table of Contents

I. Introduction..............................................................................................................................................
II. Background
   a. The Background and Necessity of the Economic Espionage Act..........................
   b. Economic espionage and the Economic Espionage Act.........................................
III. The EEA’s Enforcement Problem .................................................................................................9
   a. Barriers to Effective Enforcement of the .................................................................9
      i. The EEA statute is too hard to satisfy .................................................................9
      ii. The U.S. government under enforces the EEA ...........................................10
      iii. The EEA does not allow for civil enforcement ...........................................10
      iv. Foreign enforcement is weak ............................................................................11
      v. The guilty parties are rarely held accountable ..............................................12
      vi. Jurisdiction makes it hard to catch violators ................................................14
      vii. Victimized companies don’t help .................................................................15
          1. Companies deliberately prefer to not pursue these cases ..........15
          2. Companies may be unhelpful just because it is hard to catch violations when nothing is amiss ..........16
   b. Reasons for the Barriers .................................................................................................17
      i. Problems with legal design .............................................................................17
          1. The EEA’s built-in jurisdictional limitations are inappropriate to policing digital crime ..........17
          2. Domestic law is inherently of limited effectiveness .........................17
          3. Spies are judgment proof .................................................................18
      ii. U.S. government has bad incentives .........................................................19
          1. Agency problems within the federal government .........19
          2. The government is more attuned to politics than legal ..........................19
Punishment ........................................................................................................... 21
3. Political interference hinders effective enforcement .................. 22
   iii. In the post-Cold War world, Economic Espionage is not only fair, but prized .......................................................... 24
       1. Foreign government’s don’t share the United States’ position that they shouldn’t be involved .................. 24
       2. Foreign governments engage in such activities because the costs are minimal ................................................................. 25
   iv. The reasons not to report espionage attacks are legitimate .......... 27
IV. Conclusion ........................................................................................................ 27
The Economic Espionage Act: Is the Law All Bark and No Bite

I. Introduction

In 1982, the FBI executed a sting operation against Hitachi, one of the largest and well-known tech companies in the world.¹ The two companies had been accused of paying over $600,000 in bribes to undercover FBI and IBM officials in an attempt to steal design and software information for IBM’s new mainframe computer technology, codenamed “Adirondack.” The FBI had secured reams of information implicating Hitachi in the theft and attempted export of IBM’s intellectual property. When the FBI finally executed the sting, though, the most serious charge that could be leveled against Hitachi was conspiring to transport stolen property to Japan.² Hitachi pleaded guilty and was fined $10,000, the maximum penalty allowed by law at the time.³ Given IBM’s dominance in the multi-billion dollar computer and server industry in the 1980s, the Adirondack workbooks Hitachi was trying to procure could easily have been valued in the millions. Even including the money paid out in bribes, it was clear that Hitachi gained enormously as a result of this scheme. The FBI was outraged at the anemic outcome and, moreover, was fully aware that this sort of activity was going to continue if left unchecked. Charles Harwood, the then-president of Signetics—at the time a major player in Silicon Valley—described Japan’s “win at all costs” desire for dominance in the computer industry as similar to the competitiveness between the U.S. and the Soviets in the 1950s and 1960s. The problem, in other words, was not going to simply disappear.⁴

The Economic Espionage Act was passed in 1996 to much fanfare and bipartisan support. It was hailed as a success for Corporate America, which, along with the intelligence community, had lobbied strongly for the law in hopes that they could ward off the continuing and growing threat economic espionage had presented for several years since the end of the Cold War.⁵ But the legislative victory and significant trumpeting of the heretofore vague and silent threat of economic espionage did not lead to the successful deterrence and diminution of the activity. Since 1996, virtually all reports and expert opinions given on the subject have concluded that industrial espionage⁶ in general, and international economic espionage in particular, have both continued to increase, with no end in sight.⁷ Because the United States is the primary global

---

¹ Christopher Joyce et al., The Night They Raided Silicon Valley, NEW SCIENTIST, July 1, 1982, at 8-9.
² FRED W. RUSTMANN, JR., CIA, INC. 108-09 (2002).
³ Id.
⁴ Joyce, supra note 1, at 9.
⁶ See Phillip C. Wright & Geraldine Roy, Industrial Espionage and Competitive Intelligence: One You Do; One You Do Not, 11 J. OF WORKPLACE LEARNING 53 (1999) (explaining “industrial espionage” as including “economic espionage” and also being variously termed “corporate espionage,” “industrial intelligence” and, “competitive intelligence”). For purposes of this paper, “intelligence” will be considered legal and ethical, whereas “espionage” will be considered the legally and ethically problematic activity.
⁷ E.g., Herbert Snyder & Anthony Crescenzi, Intellectual Capital and Economic Espionage: New Crimes and New Protections, 16 J. FIN. CRIME 245, 252 (2009) (“The frequency and virulence of economic espionage attacks has increased markedly over the last ten years and will almost certainly continue to grow as the importance of IC (intellectual capital) grows and as criminals (both private and state-sponsored) increase in number and sophistication.”)
target, economic espionage presents issues of both national security and national prosperity that are uniquely salient to the United States. Fast-forward to 2001, the year § 1831 became active. Finally free to bring § 1831 cases to court, the DOJ’s track record has been one failure after another. Iconic companies like GM continue to be victimized. Friendly nations like Israel continue to thumb their noses at our laws. Clearly, the problem is not, and probably never was, a legal one.\(^8\)

It is without a doubt the case that the EEA has been a major failure, to the detriment of U.S. economic interests. The reasons are manifold, to be sure, but it is this paper’s argument that the EEA itself suffers from an unworkable and insurmountable enforcement problem. Namely, international espionage, of the form Section 1831 seeks to prohibit, is not something that domestic law can control. It may be that espionage and the law are incompatible, or that espionage is “beyond” law, or something else entirely. But the problem remains: the EEA is ill equipped to do what it was designed and hoped to do: deter and punish state-sponsored, international economic espionage. As a criminal statute, § 1831 of the EEA fails to deter spies, companies, and foreign nations from engaging in economic espionage. Since it is a domestic law and there has been almost no international cooperation, enforcement falls entirely on the U.S. law enforcement agencies. It insufficiently balances the costs of engaging in the illicit activity against the benefits, which for other nations and corporations are tangible and significant. Stealing. The EEA is dated and poorly structured, and those design problems lead directly into many of the enforcement shortcomings as well. Like other criminal statutes, the EEA includes a mens rea requirement, which impedes enforcement. The penalties, while stiff, are not so accurately directed as to most effectively deter economic espionage.

The layout of this paper is as follows. Section II will provide the pertinent background information to give a clearer understanding of what “economic espionage” is and which particular kinds of conduct the separate sections of the Act sanction. Section II will also include some of the pertinent legislative history and various studies that helped color the debate and motivate passage of the Act. Section III, the bulk of the analysis, will delve into the various issues and holes that comprise the larger enforcement problem besetting § 1831. This will include issues of domestic reporting, extraterritorial enforcement, and politics and diplomacy matters, among others. Finally, Section IV will provide the conclusion and a short discussion of a possible treaty-based solution.

II. Background

The U.S. may not be able to compete internationally in terms of cheap labor or natural resources, but it remains the gold standard in inventiveness and high technology. Arguably no other company better epitomizes this then Intel, the chipmaker. Former Intel VP and current NVIDIA executive David Shannon stated in his congressional testimony that Intel “is a world class, sophisticated company with world class security . . . even though we have world class security and are very deeply involved in the computer industry . . . we recently were the victim of economic espionage where the value to the receiver of that information could range as high as $300 million.”\(^9\) General Motors, too, is no stranger to the economic espionage problem. José Ignacio López de Arriortúa had been an up and coming General Motors executive in the early

\(^8\) See A. Coskun Samli & Laurence Jacobs, Counteracting Global Industrial Espionage: A Damage Control Strategy, 108 BUS. & SOC’Y REV. 95, 96-97 (2003). (some “believe that the world’s legal posture is so variable from one country to another, that it is almost impossible to stop international industrial espionage by legal means.”)

\(^9\) Id.
1990s, first establishing a name for himself as an effective cost-cutter and production innovator in Europe for GM’s Adam Opel brand and later, in the 1990s, in Detroit. This caught the attention of Volkswagen’s Chairman Ferdinand Piech, who, not unlike professional intelligence agents, started a months’ long development and recruitment of López. Over the course of several months and clandestine meetings, Piech secured Lopez’ move to VW at a cost of $1.6 million, over five times Lopez’ previous salary and an atypically large figure for German executives. Moreover, Piech succeeded in having Lopez stay in his previous position long enough to recruit a number of his top associates to move with him to VW, as well as to surreptitiously procure thousands of documents concerning GM’s various global facilities to take with them as well. The move sent shockwaves throughout the automotive industry and, when discovered, led to industrial espionage investigations commencing in both Germany and the United States against VW. Feeling pressure on all sides, and being caught with at least four boxes of GM documents by the German police that had not yet been shredded, VW accepted the resignation of Lopez and settled with GM. The final cost was $1.1 billion for the intrigue. VW’s reputation suffered a substantial hit as well, but Piech managed to avoid making the public apology GM was pursuing. Lopez, though only initially barred from all relations with VW for three years, was never able to revive his career. But, as is common in these cases, Lopez managed to avoid extradition and jail. Despite a 1999 grand jury indictment in Detroit for charges stemming from this incident, Lopez remains free. Most recently in 2001, the Spanish High Court refused to extradite him in 2001 to face the charges.

A. The Background and Necessity of the Economic Espionage Act

The Economic Espionage Act came to be on the heels of the end of the Cold War. The close of the U.S.-Soviet hostilities brought about several significant changes to the international landscape. Steven Fink described the new, post-Cold War world:

“Lets face it, the paradigms have shifted dramatically. Once, we catalogued the world by such contrasts as friends versus enemies, democracies versus dictatorships, free market systems versus Communism, the United States versus the former Soviet Union, and North America versus Europe and Asia. Since the fall of the Berlin Wall, the new paradigm makes us all simply competitors. Where we are located no longer matters. All that matters is, can we play the game? Can we compete? What do we have to do (or steal) to remain competitive?”

As numerous experts have noted, in addition to the resulting shift in national rivalries, the end of the Cold War took a huge wave of former intelligence professionals out of government work, and one place many of them ended up was in the commercial sector, either as private independent contractors, or as new members of in-house corporate intelligence units. Military competition took a backseat to economic rivalry; in the post-Cold War world, “the nation’s

---

11 Rustmann, supra note 2, at 40.
14 Emma Daly, Spain Court Refuses to Extradite Man G.M. Says Took Its Secrets, NY TIMES, June 20, 2001 at W1.
security is increasingly linked to its economic strength,“\(^{17}\) and not its nuclear arsenal or the size of its armed forces. The shift in rivalries also affected the “who’s who” of post-Cold War espionage. Before the 1990s, the global political system was bipolar with centers of activity and influence in the United States and the U.S.S.R. In the new era, the picture became much more complicated, with dozens of active competitors, and manifold competitive rivalries. The United States, it is frequently mentioned, is besieged on all sides by foreign nations’ economic espionage efforts; most sources put the number at roughly two dozen countries actively engaged in espionage efforts against U.S. corporations.\(^{18}\) But it is also equally likely that many of those same nations will be actively engaged in economic espionage against each other and against even some other, unrelated nations. An active participant may be engaged in these efforts against the United States, Japan, and a host of other countries in between.

The end of the Cold War allowed the U.S. government to shift more of its focus to domestic concerns and provided U.S. corporations with a more receptive congressional audience. For years, U.S. corporations had to treat economic espionage and trade secret theft as simply a cost of doing business abroad because they were left with no effective defense against it.\(^{19}\) In the 1990s, U.S. corporations were able to convince Congress of the import of economic espionage with information that commonly fell on deaf ears before. Even today, the statistics are harrowing. Experts have found that 75% of US companies’ market valuation is based on their IP and corporate know-how; even more telling, 86% of worldwide investment in Research and Development (R&D) is based in the United States;\(^{20}\) almost inconceivably, the United States spends ten times more than any other country on R&D.\(^{21}\) U.S. companies lost an estimated $300 billion from trade secret theft annually at the turn of the last century.\(^{22}\) And 37% of Fortune 500 companies reported a security breach over the last year.\(^{23}\) Given the statistics, Congress was compelled to act. The national security threat, though, was the most important consideration, “since the transfers directly and indirectly provide the latest technology to countries that are off-limits to U.S. vendors because they are considered potentially hostile,” not to mention damaging the to the United States’ global position.\(^{24}\)

The United States Congress made the theft of trade secrets a federal crime in 1996.\(^{25}\) Former FBI director Louis Freeh concluded that existing statutes were not strong enough to deter what was a rising tide of trade secret theft. The 1982 FBI investigation of Hitachi’s protracted theft operation of IBM’s classified Adirondack project, and the subsequent slap on the wrist Hitachi was fined with——$10,000——was the final straw.\(^{26}\) Louis Freeh testified in Congress to the severity of the issue, stating that foreign espionage against U.S businesses was a real and

\(^{17}\) Effron, \textit{supra} note 5, at 2.

\(^{18}\) See, e.g., HEDIEH NASHERI, \textit{ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING} 8 (2009).


\(^{21}\) Fink, \textit{supra} note 15, at 13.


\(^{23}\) Samli & Jacobs, \textit{supra} note 8, at 97.


\(^{25}\) Nasheri, \textit{supra} note 18, at 26.

\(^{26}\) RUSTMANN, \textit{supra} note 2, at 108-09.
growing threat. The Act passed with bipartisan support in both chambers and was signed by President William Clinton on 11 October 1996, who proclaimed at the signing that “economic espionage and trade secret theft threaten our Nation’s national security and economic well-being...This Act will protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secret theft.” The passage of the law, and the seeming zest within law enforcement circles to curtail this type of activity, did not lead to a successful combatting of the problem.

B. Economic Espionage and the Economic Espionage Act

The two branches of the EEA attempt to police industrial espionage activity in general. The drafters of the EEA were deliberate in choosing to punish foreign-state sponsored economic espionage more heavily. Traditionally, economic espionage was considered “low politics,” not worth the full force of the victimized state’s defenses. By comparison, military and political intelligence, matters of so-called “high politics,” were more heavily valued and protected. As the world entered a new decade post the Cold War hostilities, the aforementioned “low politics” took on a more central role in the intelligence spheres.

Addressing the two branches separately, economic espionage “consists of covert actions intended to eliminate market advantages.” It can be between corporate competitors, separate nations, or a combination of both. It is distinguished from the legitimate activity of “competitive intelligence” and is sanctioned by 18 U.S.C. §§ 1831 and 1832. A different and, for this project, more apt definition is given by the Canadian Security Intelligence Service (“CSIS”): economic espionage is “illegal, clandestine, coercive or deceptive activity engaged in or facilitated by a foreign government designed to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage.” Competitive intelligence includes the research and examination of publicly available information, such as court records, annual and market reports, trade fairs, company presentations

27 Id. at 109. 
29 Danielson, supra note 20, at 537. 
In general- Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

[...] shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both. 18 U.S.C. 1831 (2006)

and demonstrations, and speeches by corporate executives. This activity is not sanctioned in the United States, and in a recent survey it was found that more than 80% of U.S. corporations with annual revenues greater than $10 billion have an organized intelligence unit within their structure. Economic espionage of the kind § 1831 is focused is different from competitive intelligence in that it expressly contemplates “misappropriating trade secrets belonging to citizens of one country in order to benefit another country” and “to include that unlawful taking…of proprietary information by anyone not lawfully entitled to it.”

The EEA covers the entire gamut of “economic espionage,” but reserves its harsher punishment for the state-sponsored, international variety. Section 1832 polices the more common kind of economic espionage, the pilfering proprietary information and trade secrets from market competitors for purely corporate gain. This activity, judging by the frequency of prosecution and anecdotal evidence, is undoubtedly the more common form of economic espionage. Conversely, Section 1832 may enjoy more DOJ support because it is less fraught with political risks and, typically, deals with wholly domestic matters where jurisdiction is not an issue, though there are some exceptions that do broach into international competition.

International intelligence, as the old idiom describes it, “is the world’s second-oldest profession.” It is the more commonly known, typically more publicized and valorized version of espionage activities. This is the stuff of James Bond features and tales abound of wartime spies pilfering enemy secrets and turning the tides of global conflicts—like the Allies’ use of spies during World War II to defeat the Axis powers. More recently, though, international intelligence activities have changed focus. International intelligence agencies had primarily been focused on political intelligence. Further, intelligence was valued primarily for its potential military or strategic use against enemies—either active wartime combatants, or more recently, Cold War rivals over the course of continuing tension. Since the end of the Cold War, though, strategic international intelligence has taken a back seat to economic intelligence, much the same

34 Samli & Jacobs, supra note 8, at 96-97.  
36 Snyder and Crescenzi, supra note 7, at 246.  
37 Theft of Trade Secrets, 18 U.S.C. § 1832 (2006): Whoever, 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, knowingly—[…] shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.  
38 Westlaw search conducted March 25, 2011 produced more than sixty cases citing 18 U.S.C. § 1832. By comparison, a similar search for 18 U.S.C. § 1831 returned only twenty-two such matches.  
40 See, e.g., Avery Dennison Corp. v. Four Pillars Enterprise Co., 45 Fed.Appx 479 (6th Cir. 2002).  
42 Sepura, supra note 35, at 129.
way military posturing and activities have taken a back seat to economic rivalries in this modern political climate.\textsuperscript{43}

Even with these fundamental changes to the field of international intelligence gathering, the prior central issues remain. It has always been utilized by rivals, for whatever purpose was the most pressing at the time, and has always existed in a sort of legal “lacuna,”\textsuperscript{44} being neither legal nor illegal by international standards. Its practitioners are alternately vilified and valorized, depending on which side of the border they are found.\textsuperscript{45} Virtually every industrialized country—including the United States,\textsuperscript{46} and continuing through the 1996 passage of the EEA—continues to partake. And no country—again, including the United States\textsuperscript{47}—has established laws proscribing its own continued employment of international intelligence or outlawing intelligence activities directed outside its borders. The international accords concerning espionage, such as the Geneva Conventions and The Hague Convention on Diplomatic Relations, are essentially silent on the issue of economic espionage.\textsuperscript{48} Customary international law also has very little to say on the issue.\textsuperscript{49} It is safe to assume that international intelligence is in no danger of losing its relevance in the global political system.

III: The EEA’s Enforcement Problem

The Economic Espionage Act is a feeble, legislative solution to a problem that is only marginally centered on domestic crime. Because the EEA is a domestic criminal statute, almost by definition it is most effective in policing domestic parties’ conduct that violate the strictures of the law. Sadly, while that story may hold true for other white-collar offenses like identity theft or insider trading, it very much is not the story with economic espionage in the 21\textsuperscript{st} century.

A. Barriers to Effective Enforcement of the EEA

1. The EEA statute is too hard to satisfy

The \textit{mens rea} requirement in § 1831 is unnecessarily difficult. The EEA, as presently applied, only polices unlawful conduct that the government can show was indeed intended to “benefit a foreign government.” This interpretation is needlessly onerous and, in many respects, is unusual compared to other criminal statutes.

For the government to successfully convict a spy for violation of § 1831, they will have to prove two separate specific intents. They must demonstrate specific intent to misappropriate proprietary information, and the additional specific intent for the theft to be “to benefit a foreign government.”\textsuperscript{50} This has been a significant hurdle to enforcement even in those rare cases when § 1831 cases are indeed brought to trial. In the \textit{Lee and Ge} case, the court found the evidence

\begin{itemize}
  \item \textsuperscript{44} Id.
  \item \textsuperscript{46} Danielson, \textit{supra} note 20, at 511.
  \item \textsuperscript{47} Id. at 514
  \item \textsuperscript{48} See Radsan, \textit{supra} note 45, at 598.
  \item \textsuperscript{49} Id. at 597.
  \item \textsuperscript{50} 18 U.S.C. § 1831(a) provides that “[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent…”; \textit{see also} United States v. Lee and Ge, No. 5:06-CR-0424 (N.D.Cal May 21, 2010) (holding government must demonstrate defendant’s specific intent to benefit a foreign government).
\end{itemize}
lacking for a § 1831 charge because of this requirement. The prosecution was therefore forced to try the defendant under the less onerous § 1832. The chief hurdle is convincing the court that the entity or individual for whom the defendant was working for was sufficiently controlled by a foreign government. This has proven difficult in years past, and, naturally, given that foreign governments are loath to assist the prosecution in unearthing this evidence, it remains a halting burden on § 1831 prosecutions.

Often, criminal law does not require the prosecutor to demonstrate the specific, separate dual intents when the law has two branches. Usually, it is sufficient only to demonstrate that the defendant had the requisite intent to set the cause in motion. Looking at § 1831 cases, the statute would be more easily applied if it were sufficient to show only that the defendant did intend to misappropriate the other party’s proprietary information. Burdening the prosecution with showing how involved a foreign government was in the operation, or delving into the entire structure of the criminal enterprise, seems unnecessary and serves no purpose other than to make these cases that much harder to pursue to a judgment.

2. The U.S. government under enforces the EEA

Despite the apparent intensity of interest of Congress to make a law specifically to police international economic espionage, the executive agencies assigned to use the EEA have been loath to do so. This has been both explicit, as in the case of the Department of Justice (“DOJ”), and implicit, as seen in the pattern and practice of the intelligence agencies since the EEA’s passage in 1996.

Shortly after the EEA’s signing into law by President Clinton, then-Attorney General Janet Reno significantly shackled the DOJ’s ability to pursue those cases. She stated that for the first five years after passage of the EEA, no cases would be brought unless expressly approved by at least one of the top three deputies of the DOJ, including herself. This ensured that, at the very least, only the most winnable cases would even be brought to the indictment stage, never mind trial.

This practice somewhat mirrors the pattern of the intelligence agencies. They have consistently been interested in these cases—indeed, it was at the behest of the FBI head that the EEA was even created—but it would be wrong to assume that the intelligence agencies were sufficiently invested. Being involved in hundreds of investigations may be good for informational or statistical purposes, but it is hardly useful for the victims if investigations are not pursued to the end, and arrests made.

3. The EEA does not allow for civil enforcement

Trade secrecy is unique in the IP legal regime because unlike patent and copyright infringement, trade secret misappropriation can subject the violator to criminal penalties in the United States. The EEA is lacking in that it only provides for criminal penalties, completely ignoring civil enforcement. As a direct result, the U.S. government is tasked with the sole

52 MPC 5.01(1)(b)
53 See Fink, supra note 15, at 42 (discussing the intensity of the lobbying efforts in the lead up to the EEA)
55 Desmet, supra note 19, at 97.
responsibility of enforcement. This is counter-productive because, unless the interests of the
victimized corporations and the U.S. government are perfectly aligned, there are necessarily
going to be instances where the company would choose to pursue an action and the government
would not, and vice versa.

The exclusive government enforcement structure presents basic problems of motivation,
not only at the institutional level—the DOJ, the intelligence agencies, and the State Department,
as will be discussed later—but at the human level. Since the EEA does not provide for any civil
actions, there is no other legal recourse under the EEA for victims of economic espionage when
the government chooses not to pursue the action. There is no safety mechanism of enforcement
for when the government drops the ball, as it has been doing fairly consistently. Losing all ability
to control the litigation probably has a chilling effect on reporting. Victimized corporations may
be reluctant to give over all of their information and control of the case, if it could mean risking
further loss of proprietary information, either by accident or as part of the litigation process.

This problem does not center only on the less-convincing cases, where the company may
have been significantly harmed but the evidence is less than compelling to necessitate a suit.
Corporations and their legal counsel have one major duty: to work for the benefit of the firm and
its shareholders. Corporations would presumably go after every trade secrets case that
objectively presented a net gain of value, all other factors considered. There would also be
signaling value: corporations may want to show that they vigorously protect their rights to the
fullest extent of the law, and are not apt to sit idly by in the face of criminals and spies raiding
the company’s wealth. The government, unlike the corporations themselves, has to be at least
partially concerned with politics. Money would not be the only consideration. Indeed, it is not
hard to imagine scenarios where the victimized company and the U.S. government were
completely at odds as to how to proceed in the face of a misappropriation of a company trade
secret by a foreign-sponsored agent. In that situation, the government itself would be another
potential barrier to enforcement of the EEA.

4. Foreign enforcement is weak

Foreign governments have been virtually useless in assisting the U.S. government in
enforcing the EEA. Since the EEA was enacted, there has been no diminution in economic
espionage activity\(^\text{56}\) and by many accounts, it will loom an even larger problem in the coming
years.\(^\text{57}\) Most of this espionage activity is targeted towards the U.S. but maintains its operations
centers abroad. Foreign governments could be helpful allies, or even just idle bystanders, but
they are neither. They are all too often active participants in these illicit activities.

Even on the rare occasions when the U.S. does pursue and apprehend violators, the
common response from foreign governments is to freeze the case in its tracks. The Cleveland
Clinic Foundation (“CCF”) case, concerning the U.S. and Japan, is illustrative of this malaise.

In the aforementioned Cleveland Clinic Foundation, the accused Japanese researcher,
Takashi Okamoto, succeeded in returning to Japan before the authorities could arrest him under a
§ 1831 indictment. U.S. authorities had shortly before apprehended and arrested his accomplice,
Hiroaki Serizawa, charging him with two counts of conspiring to violate the EEA, one count of

\(^{56}\) Christopher G. Blood, Holding Foreign Nations Civilly Accountable for Their Economic Espionage

\(^{57}\) See e.g., Christopher A. Ruhl, Corporate and Economic Espionage: A Model Penal Approach For
Legal Deterrence to Theft of Corporate Trade Secrets and Proprietary Business Information, 33 VAL. U.
information represents the greatest single problem facing U.S. corporations in the next century.”)
transporting stolen property across interstate lines, and making false statements to the
government. Serizawa plead guilty to the lesser charges in exchange for agreeing to testify
against Okamoto and having the EEA charges dropped. Okamoto and Serizawa, both Japanese
nationals holding permanent residency in the U.S., were both medical researchers in the U.S.
Okamoto accepted a position with the Japanese Institute of Physical and Chemical Research, a
quasi-public Japanese corporation known as Riken, while still employed by the CCF. In
preparation of the move, it was alleged that Okamoto stole several DNA and cell line reagents
and constructs from his lab at the CCF and sent them first to Serizawa in Kansas, and then to
Riken in Japan. He also allegedly destroyed the remaining cell lines and reagents he left at the
CCF lab, and instructed Serizawa to refill the vials with plain tap water in preparation for the
authorities locating Serizawa and demanding the return of CCF’s property. Despite evidence
strong enough to garner a grand jury indictment—the first of its kind for a § 1831 case—an
accomplice ready to testify as to the certainty of the indictment, along with the United States and
Japan having an extradition treaty in force for almost two decades and being consistently strong
allies for several decades up to this point, the U.S. DOJ was unable to secure Okamoto’s
extradition for violation of the EEA. Somehow, the Japanese court found the indictment lacking
in evidentiary support, and also that the conduct the defendant was accused of partaking in to not
be illegal in Japan nor explicitly covered by the U.S.-Japan extradition treaty. The treaty that
they consulted was originally put into effect in 1980, years before the EEA was passed.
Furthermore, it was the Japanese High Court that heard the arguments and ruled against the
United States in the matter, the case was effectively closed. This case supports Brenner and
Crescenzi’s assertion that “in pursuing foreign nationals who misappropriate U.S. trade secrets
[p]erhaps the most difficult issue is extradition.”

5. The guilty parties are rarely held accountable

Section 1831 of the EEA fails to stem the rising tide of espionage because it fails to
properly apply punishment to the respective parties. The penalties provided for in the Act appear
severe in regards to the money and prison time contemplated, but are actually misguided and
therefore severely lacking in deterrence value.

Director Freeh and the FBI viewed foreign nations, both rivals and allies, as the more
serious threat in regards to economic espionage, and his statements to Congress described them
as such in the mid-1990s. But the EEA does nothing to target foreign nations for punishment in
any of its several sections. Nor how could it. The EEA, as noted, is a domestic law. Its
application to foreign governments themselves, through the federal court system, is impossible.

58 Nasheri, supra note 18, at 142.
59 Tetsuya Morimoto, First Japanese Denial of U.S. Extradition Request: Economic Espionage Case, 20
60 Nasheri, supra note 18, at 143.
61 Fink, supra note 15, at 181-82.
892.
63 Morimoto, supra note 59, at 289-90
64 Id.
66 Fink, supra note 15, at 74.
67 Danielson, supra note 20, at 518.
Congress enacted a law that was supposed to target a certain class of violator, but left the “head” of the beast unscathed.

Foreign corporations are similarly, but not quite as wholly, secure in their espionage activities. The financial penalties applied to corporate defendants can now reach the millions. But as the story surrounding the invention and growth of MRI technology shows, large-scale economic espionage operations can yield benefits for foreign corporations in the hundreds of millions, even billions, of dollars.\(^{68}\) Dr. Damadian was the proprietor of Fonar Corporation, owner of the first patent for MRI imaging, and the inventor of MRI technology. From the outset, Dr. Damadian’s company was targeted by some of the worlds most well-known and well-regarded companies, such as Toshiba and Siemens, seeking to get their hands on the unique technology and enter the burgeoning market.\(^{69}\) These companies openly used unsavory—if not unlawful—tactics to misappropriate Fonar’s proprietary information, such as deliberately employing Fonar’s engineers despite two-year non-compete contracts or plying Fonar technicians with copious amounts of alcohol in a gambit to secure proprietary information.\(^{70}\) They were largely successful. MRI technology has now grown into a multi-billion industry, but because of the lack of adequate IP protection, Fonar is now the smallest of the handful of companies that dominate the market.\(^{71}\) It is also the only U.S. firm still in the market.\(^{72}\) Ten million dollars in fines and criminal sanctions may harm the corporation’s reputation, but it can hardly be expected to severely harm its bottom-line, especially when thinking of a company like Toshiba. Granted, the EEA does include a section concerning forfeiture and restitution for the misappropriated proprietary information,\(^{73}\) but as is the case with much of trade secrets law, once the information has been exposed, its value, even if returned to the owner, is severely if not entirely destroyed.

The EEA, incongruously, reserves its harshest punishment for the lowest actors on the international espionage ladder, the actual individuals who misappropriate IP from U.S. companies. These people—disgruntled former employees, dishonest mid-to upper-level executives changing firms, or professional intelligence operatives—are the most numerous and fungible of the lot. Moreover, aside from long prison sentences—which have not been indicative of the pattern of enforcement the last fifteen years—these people are most likely judgment-proof. Few apprehended criminals can pay the fines associated with conviction, and they certainly cannot provide restitution to the victimized companies should associated criminal and civil charges be brought.

Additionally, customary international law insulates some violators from punishment. Foreign agents caught in the United States are often protected by diplomatic immunity.\(^{74}\) Ambassadors, diplomats and the like—even when using such positions purely as covers for their real intentions—enjoy the protections that customary international law provides them. This is the case both for traditional allies, like Israel and Japan, and the less favorably regarded others, like China. In many cases, even if foreign operatives are in fact caught violating the EEA, they will not be exposed to legal punishment by nature of their legally privileged position. The worst

\(^{68}\) Clark, supra note 30, at 9.

\(^{69}\) Id.

\(^{70}\) Id. at 9-10

\(^{71}\) Id. at 10

\(^{72}\) Id.


\(^{74}\) Rustmann, supra note 2, at 111.
official punishment they will likely be subject to is being designated persona non grata and expelled. But as with all things espionage-related, the more likely result will be the very quiet removal of the guilty party with hushed diplomatic negotiations surrounding the incident between the nations to come up with a satisfactory resolution.

The result of these factors is that effective enforcement of the EEA almost impossible. There is no shortage of intelligence professionals and disgruntled employees to keep the business of economic espionage moving. Thus even when spies are apprehended with overwhelming evidence of culpability, the entities that contracted their services—the foreign corporations and states seeking a leg-up—will be undeterred because the lost asset would be easily replaceable. The cost to foreign nations and states of being caught complicit in the crime is minimal in most instances, and certainly worth continuing.

6. Jurisdiction makes it hard to catch violators

The EEA is lacking in regards to providing jurisdiction for U.S. authorities to pursue violators. This makes even the most brazen cases of international economic espionage difficult if not impossible to pursue.

As noted earlier, the intelligence and law enforcement professionals who sounded the alarms as to the growing concern economic espionage presented voiced the greatest concern in regards to international espionage. There had been laws on the books for years protecting trade secrecy and policing corporate behavior, but the greatest concern was the lack of protection afforded U.S. corporations from international IP infringement and unlawful competition. This was also the concern that most resonated with the federal government; as Senator Herbert Kohl stated,

“Since the end of the Cold War, our old enemies and our traditional allies have been shifting the focus of their spy apparatus. Alarmingly, the new target of foreign espionage is our industrial base. But for too many years, we were complacent and did not heed these warnings. And we left ourselves vulnerable to the ruthless plundering of our country’s vital information. We did not address this new form of espionage—a version of spying as dangerous to our well-being as any form of classic espionage. Today, that complacency ends.”

Even the Act itself lists international economic espionage first, and reserves the harsher punishment for that, signaling that Congress found international espionage more important than the more pedestrian variety covered by § 1832.

Despite all of this, the Act limits itself—excepting instances when the violation is done and caught within U.S. borders—to international espionage done by Americans, defined as citizens or permanent residents, or when an act done in furtherance of the violation was committed on U.S. soil. In this “digital age,” entire hosts of operations by U.S. companies may

75 Chesterman, supra note 41, at 1088-89.
76 Smith, supra note 24, at 79-80 (“It is also well documented that few of the thousands of privately reported suspected espionage incidents ever generated DOJ criminal complaints or indictments.”)
77 See Fink, supra note15, at 73.
79 18 U.S.C. § 1837 (2006). Applicability to Conduct Occurring Outside the United States: This chapter also applies 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
be done over seas, remotely, and attacked remotely. Huge swaths of violations, by the real targets of the Act, are left completely out of the purview of the EEA. This hole in jurisdiction—insisting the some portion of the violation touch the U.S. or a citizen thereof—is extremely problematic and illustrative of how dated the EEA. Indeed, its illustrative of a problem seen over and over again, which is technology surging ahead and the law struggling to keep up.

7. Victimized companies don’t help
   i. Companies deliberately prefer to not pursue these cases

   Typically, the victim of a crime would be one of the most bullish in seeking punishment of the transgressor and restitution for itself. Economic espionage is different because the successful execution of the crime leaves the victim unknowledgeable of the harm it has suffered. But even in cases, successful or not, where the victim become aware of the loss, corporations regularly decide to leave the culprit alone.80

   Companies think twice about calling in the feds. “When a spy has stolen a company’s trade secret and the company ponders whether or not to call in the FBI, the question often asked is whether it is better to have one individual or one company have the trade secret, or call in the Feds and run the risk that carelessness or lack of trade secret protection or improper handling might expose the trade secret to the whole world.”81 Yes, all corporations would enjoy seeing economic espionage diminish or cease altogether. But their greater concern is the “blame the victim” effects that notifying outside actors of the breach will prompt, like the bad press and possible termination of certain employees or executives.82 When it comes to corporate executives protecting themselves or their firm’s valuable IP, they self-servingly choose to protect themselves. This is true even despite the fiduciary duties imposed upon corporate executives and directors by corporate law.

   That is not to say that the decision not to report security breaches and espionage events is necessarily bad for the corporation. Corporations themselves are harmed by the process: stock prices falter, reputation is damaged, and publicizing the event may lead to further risks to the trade secret.

   The adverse results of this practice are that culpable actors are more likely to engage in these espionage activities when targeting, for instance, publicly traded corporations. Corporations that are not as susceptible to ruination by bad press—especially bad American press—are likely to continue their espionage activities. This is because the largest financial deterrent for almost any for-profit company is the loss of U.S. business. For example, Deutsche Telekom, a German company whose fiscal health is intimately tied to its operations in the U.S. through its ownership of T-Mobile, may think twice before violating the EEA and risk being publically maligned. On the other hand, Digicel, a Central-American peer, would decide differently since it has no significant operations within the U.S. The same effect could be seen with respect to foreign nations.83

   (2) an act in furtherance of the offense was committed in the United States.

80 See Sepura, supra note 35, at 137.
81 Fink, supra note 15, at 75.
82 See id.
83 See Danielson, supra note 20, at 543:
   “Less-Developed States (“LDSs”) have little incentive to participate given that economic espionage is profitable to participants and saves the time and financial resources required to develop technologies independently. A movement for change will not come from states desperate to catch their more successful neighbors. LDSs may ignore reputational concerns to engage in
Companies may be unhelpful just because it is hard to catch violations when nothing is amiss

The successful execution of an EEA violation should leave the victim completely unaware of their loss. The victim’s particular loss is not the culprit’s direct gain. Often times, the spy simply copies or downloads the proprietary information; they do not physically take the trade secret in the form of a prototype. For this reason, unwitting victims are in certain ways the worst victims of all. Not only do they not report the crime in a timely fashion, but whatever information they do finally report may be replete with holes due to time lapse, the sophistication of the violators and their adeptness at covering their tracks, and the fact that the intellectual property taken, while valuable, may not yet be at a stage where it can accurately particularized and monetized. Unsurprisingly, some commentators and professionals attribute, at least partially, the rising tide of economic espionage on the fact that the trade secret owners, the U.S. corporations, do not do enough themselves to protect their own valuable IP. That may ring of “blaming the victim,” but their point is simple: effective prevention before the breach is better than efficient detection after.

Economic espionage is not of the James Bond variety. No doubt, there are some sophisticated, state-sponsored, high-risk operations from time to time targeting U.S. corporations. The more typical story though is much more pedestrian, both in organizational structure and the individuals involved. A mid- or upper-level professional with access to protected information or trade secrets seeks to make something extra. She downloads the particulars of a new technology or product design onto some sort of removable storage, like a flash drive or CD. With a partner located off-shore who already set up a shell company, she could chose to remit that information abroad for it to be implemented in the manufacturing process, or she could seek to sell it to an established competitor of her employer. She may already have an ownership stake, or be offered shares of the foreign company, as well as payment, for the misappropriated IP. This would have all been done surreptitiously, with the only notice to the employer being her two-weeks notice informing the corporation that she would be leaving. And that notice would hardly be cause to sift through the heretofore honest and satisfactory employee’s data records.

While the statute contemplates the trade secret being stolen or “carried away,” the most likely result is not for the violator to take the prototype. The background data to actually replicate the technology is both more valuable, and easily duplicated. The owners of the technology will not be put on notice that it was taken immediately, but when the competitor brings to market—or the public—the technology that had theretofore been a secret. Thus, even with security protocols in place, corporations have to be vigilant not just against infiltration from without—like the case of a Japanese film crew entering a pharmaceutical company’s lab economic espionage and free-ride off the gains made publicly available….This would b rational for a LDS already suffering from a poor reputation for corruption or integrity.”

---

84 See Snyder & Crescenzi, supra note 7, at 252 (“One proposed solution…is to allow the federal government to bring suit against those firms which lose information as they do in similar actions such as antitrust suits. Another possibility for enforcement is criminal liability for data breaches. The option may seem draconian in that it appears to punish the victim….The firm, however, is not the only party suffering damages in the event of IC theft.”)
86 18 U.S.C. 1831(a).
pretending to be taping a documentary on the biotech industry but instead focusing their recordings on the manufacturing process—but from within.

B. Reasons for the Barriers

1. Problems with legal design

Many of the problems presented are not a result of politics or people actively working against an effective EEA regime, but are an inherent a result of how the EEA was created. The statute attempts to police an activity that is widespread and endemic to international relations. Congress, in its foolhardy haste to solve the problem chose to draft a law, and did not wait to garner the necessary support from the different sides playing a role in international economic espionage. One could say that Congress attempted to tackle a problem outside of its purview and yet nevertheless decided to do all that it could do address it: pass a law. The old adage, “if all you have is a hammer, everything looks like a nail” is very much applicable.

i. The EEA’s built-in jurisdictional limitations are inappropriate to policing digital crime

A large proportion of international economic espionage is done in the digital domain. Indeed much of the most valuable proprietary information constantly being sought by the United States’ rivals is high-tech innovations that rarely exist in tangible form. One of the reasons for creating the EEA in 1996 was because the laws extant in the 1980s conceived of tangible property being misappropriated. That is not the case in the 2000s.

The shortcoming of the EEA is its statutory limitation as to conduct that happens in, or at least touches within, U.S. borders. This jurisdictional hook may have made sense in 1996 since the Internet was not nearly as ubiquitous, nor the technology as capable as it would be at the turn of the century. It should also be noted that the major espionage operations of the late 1980s and early 1990s—the very ones that motivated the creation of the EEA—were traditional, face-to-face intelligence operations. That is type of activity Congress was targeting in the EEA.

By 2001 though, when Attorney-General Reno’s regulation concerning pursuing §1831 cases was set to expire, the Internet was a very different creature. The law, which was meant to have an extraterritorial effect as described in § 1837, was hindered as a result of the Internet and digital crime taking off at the turn of the twenty-first century and the statute becoming dated before it even became effective and operational. This limitation has the potential to totally excise from the breadth of the EEA a very broad subset of putatively criminal conduct. Essentially all conduct that is done from a remote location—as digital crime is likely to be—and targets only foreign subsidiary operations of U.S. firms or foreign firms while being careful not to route any data transfers through proxy servers housed within the United States would be explicitly outside the jurisdictional scope of the Act. Given the increasing globalization of U.S. firms, which has seen U.S. corporations store and run more and more of even their domestic operations on servers housed abroad, this shortcoming has the potential to leave a myriad of U.S. firms’ operations unprotected. Granted, it is quite difficult to deliberately route information only through servers and network channels located without, but assuming the increasing sophistication of perpetrators, this presumably small hole in jurisdiction could develop into a gaping rift requiring amendment of the law itself.

ii. Domestic law is inherently of limited effectiveness

---

87 Fink, supra note 15, at 49.
88 18 U.S.C. § 1837; cf. Nasheri, supra note 18, at 139 (asserting that the statute “has a very broad territorial reach”).
The EEA is a domestic, criminal statute. By nature, such constructions are most useful for policing domestic activity by actors through which U.S. federal courts can exercise jurisdiction. The problem, then, is not in how the law was conceived or drafted by Congress, but in how it can be properly enforced. The EEA’s efficacy will be strongest when the perpetrators are easily identified, domestic agents and are apprehended within U.S. borders. That is far from the typical scenario when dealing with § 1831 cases. The law has less reach in dealing with the foreign agents involved in § 1831 violations.

Snyder and Crescenzi describe how economic espionage, especially in cyberspace, simply does not fit within the normative conditions of criminal investigation and prosecution as a general matter. They explain that there are four basic conditions of crime: reactive responses to crime by the police; the police, the criminal, and the locus of the crime share physical proximity; criminal activity by the individual perpetrator is of limited frequency, and almost certainly not simultaneous and numerous; and that criminal activity is viewed as a threat by all jurisdictions which the specific crime or criminal touches.\(^{89}\) All four of these conditions are routinely defied in § 1831 cases, thereby showing the inappropriateness of criminal law in policing international economic espionage.

This problem is not unique to the EEA. It is rarer than not for a domestic law to provide for extraterritorial enforcement. Particular to the EEA, though, is that the jurisdiction within which the crime is committed is just as likely to be within the borders of the United States as without. Domestic laws, with rare exceptions,\(^{90}\) are intended primarily to police conduct within the jurisdiction that the law is effective. It is not in the realm of domestic law to police purely international activity; indeed, such overstepping by national law-making bodies is both largely ineffectual and, usually, bad politics. But Congress clearly intended the EEA to have just such an international effect. There is much discussion that despite the pattern of enforcement of the EEA since 1996, both Corporate America’s and the U.S. intelligence community’s main concern with respect to economic espionage was the international theft of trade secrets, not the more pedestrian—and more easily policed and punished—economic espionage between corporate competitors.\(^{91}\) But the United States’ law enforcement agencies do not have the wherewithal to effectively police the whole range of this type of criminal conduct alone, especially as it continues to increase in scope.

### Spies are judgment proof

The EEA fails to properly deter the respective actors in international economic espionage cases. This was a result of Congress failing to accurately match significance, ability to withstand pressure, and numerosity with level of punishment. This was a needless mistake that could have been avoided had Congress better designed the law to address the respective parties in economic espionage operations better.

The law reserves its harshest punishment for *individuals* engaged in economic espionage. They can be fined up to $500,000 or imprisoned up to fifteen years.\(^{92}\) This is clearly a mistake; Congress undoubtedly missed the goal here. Simply put, very few individuals have the capacity to pay that sort of money, and compromising or incapacitating an intelligence professional, as trying and convicting one will necessarily do, will lead to nothing else besides her employer

---

89 Snyder & Crescenzi, supra note 7, at 251.
91 See Effron, supra note 5, at 1477.
replacing her with another agent. Organizations are limited, statutorily, to fines of up to $10,000,000. The deterrent effect of a multi-million dollar fine when the IP being sought could be worth hundreds of millions is negligible. The law also includes no provisions for punishing governments, though it presumably could. Ignoring the imprudence of drafting a domestic criminal statute to combat foreign governments’ activities that touch on or within U.S. borders, if Congress was determined to follow this route it should have included some sanctions that would have affected foreign governments. For example, it would have been at least possible for Congress to close off U.S. markets that foreign governments would like to engage. A rule prohibiting foreign nations indicted on § 1831 offenses from selling sovereign debt on U.S. bond markets, and prohibiting U.S. citizens, both individual and corporate, from dealing with such instruments, would be something that at least the developing countries that engage in this conduct would consider when weighing the dangers of being caught. Another would be barring the importation of raw materials extracted and exported by the state-run enterprises of foreign nations that are indicted on § 1831 charges. This hole in the penalties scheme can be attributed to Congress and is another reason the EEA lacks the requisite “bite” of an effective criminal statute.

2. U.S. government has bad incentives

If the EEA truly is ineffectual, it is because the U.S. government itself has chosen against effective enforcement. Despite the impressive statistics claiming that the FBI is actively engaged in hundreds of EEA investigations concerning roughly two dozen countries, the EEA is still seldom used in matters of international concern. A quick look at the statistics bears this out. The activity of the DOJ is squarely focused on § 1832, which, judging by the frequency of prosecution and anecdotal evidence, is undoubtedly the more common form of economic espionage. Conversely, § 1832 may enjoy more DOJ support because it is less fraught with political risks and, typically, deals with wholly domestic matters where jurisdiction is not an issue, though there are some exceptions that do broach into international competition. Whatever the reason, the U.S. has not upheld its side of the bargain in enforcement. Moreover, the drafters of the bill failed to include a separate civil enforcement measure so as to allow the victims to pursue EEA cases if law enforcement, for whatever reason, does not.

i. Agency problems within the federal government

Agency problems exist both at the top and the bottom. Despite passing with what appeared at the time as broad support, the agencies charged with enforcing the EEA have been far from vigorous in pursuing these investigations.

At the top, there was reluctance. Most notably, there was Attorney-General Janet Reno’s declaration that for the first five years of the EEA’s lifetime the DOJ would append heavy bureaucratic hurdles to the process of bringing an EEA suit. A pre-indictment approval procedure that required the signature of the U.S. Attorney General, Deputy Attorney General, or the Assistant Attorney General of the Criminal Division prior to bringing suit was imposed. This coincided with the DOJ policy of only bringing the most convincing, sure-fire cases to

93 Westlaw search conducted March 25, 2011 produced more than sixty cases citing 18 U.S.C. § 1832. By comparison, a similar search for 18 U.S.C. § 1831 returned only twenty-two such matches.


95 See, e.g., Avery Dennison Corp. v. Four Pillars Enterprise Co., 45 Fed.Appx 479 (6th Cir. 2002).

96 Letter, supra note 54.

97 Fink, supra note 15, at 42.
court. Although Attorney General Ashcroft allowed the three-signature approval policy to lapse in the DOJ in 2001, the DOJ has continued to sparingly bring § 1831 cases and, despite the FBI’s pursuit of hundreds of EEA investigations, only rarely has the DOJ gone so far as to take a § 1831 case to the grand jury.

The proffered reason for the Attorney-General’s bureaucratic rule was to ensure that the government lawyers and intelligence agencies had time to get familiar with the new law and learn which kind of potential cases were supposed to be brought. Attorney-General Reno sought to ensure that execution of the law matched congressional intent. Yet it is a matter of course to assume that the language Congress chooses to use in drafting a law is deliberately chosen; therefore, it is logical to assume that the EEA was deliberately written with broad strokes, covering an extremely wide swath of information that could qualify under the Act as proprietary information, so as to not put burdensome or confusing limitations on the executive branch. The way the EEA defined “trade secrets” was extremely broad, especially when compared to other, purely domestic definitions, such as the ones found in the Uniform Trade Secrets Act or the Restatement (First) of Torts. Even if Reno was correct and such an agency regulation was

98 Danielson, supra note 20, at 517 [5] I remember
99 Desmet, supra note 27, at 97.
100 Letter, supra note 54.
102 Compare the EEA definition, 18 U.S.C. § 1839 (3):

(3) the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--
(a) the owner thereof has taken reasonable measures to keep such information secret; and
(b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public;

with the UTSA definition, §1 (4):

“trade secret” means information, including a formula, pattern, compilation, program device, method, technique, or process, that:
(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

103 Restatement (First) of Torts § 757 cmt. b (1939).

"Definition of trade secret.” A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. It differs from other secret information in a business (see § 759 of the Restatement of Torts which is not included in this Appendix) in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for
indeed needed, certainly five years would have been sufficient time for regulations and institutional procedures to be implemented by the respective executive agencies to ensure a responsible application of the EEA. That was not the case. In 2002, then-Attorney General John Ashcroft renewed the approval process for § 1831 cases for another five years.\textsuperscript{104} Thus, for the first ten of eleven years of its existence, DOJ attorneys were shackled with a peculiarly restrictive and long-term policy with regards to their pursuit of § 1831 cases. Even though those restrictions have since loosened, “[i]t remains for the Bureau and the Justice Department to explain why they lobbied so hard for the passage of a bill that would allow the United States to prosecute a foreign company that is owned or majority controlled by a foreign government, if they’re not going to use it and use it effectively.”\textsuperscript{105}

The individuals tasked with investigating and enforcing the EEA were less than enthused about doing so anyway. Simply put, U.S. intelligence agents—the “foot soldiers” in this economic war—may be prepared to risk life and limb “for [their] country, but not for General Motors.”\textsuperscript{106} This lack of motivation presents problems because very often the secrets pilfered from the “GMs” of this country are the same secrets that provide the United States with its strategic advantages in technology and national defense. Government agents’ disinclination towards pursuing these investigations whole-heartedly—whether widespread or not—presents a two-fold problem. First, given the increasing sophistication and the clandestine nature of these crimes, without constant vigilance the U.S. intelligence agencies may start to lag behind their counterparts in the economic espionage battlefield. Second, since the EEA does not provide for civil enforcement, there is no backstop to the government’s laziness, leaving corporations without options should they come under siege.

\textit{ii. The government is more attuned to politics than legal punishment}

Section 1831 of the EEA does not make concessions for the fact that it is attempting to deal with a very politically sensitive issue. Former Special Assistant to the Director of the CIA—and current Deputy Secretary of the Treasury—Neal Wolin explained that bringing a § 1831 case against a foreign power would require the U.S. government to explain “what it knows and how it knows it,” in addition to maneuvering issues of diplomatic relations with the accused country, broader foreign policy if the country is a major player, and possibly even national security concerns.\textsuperscript{107} That is a significant amount more tangle to deal with than a typical § 1832 case.

Section 1831 of the EEA is intentionally targeted at international economic espionage. The drafters of the legislation were no doubt aware that this particular class of crime is rife with politics and danger. That is why the executive branch has chosen to limit both its effectiveness and its usage. Allowing just such a criminal law, with such stark punishment, to be applied extraterritorially and in a black and white fashion, with no posturing or politicking allowed, could potentially wreak havoc on international relations.

\begin{footnotes}
\footnote{See Brenner & Crescenzi, \textit{supra} note 65, 432.}
\footnote{Fink, \textit{supra} note 15, at 42.}
\footnote{\textit{Id.} at 44.}
\footnote{\textit{Id.} at 43.}
\end{footnotes}
Economic espionage is engaged in by the United States’ rivals, allies, and even the United States itself. One issue rarely discussed with regards to § 1831 is that every country engages in espionage one way or another, even the United States.\textsuperscript{108} Economic espionage is just a fraction of the espionage activities rival nations undertake in their continuous quest of one-upsmanship. For that reason, the United States’ attempt to sanction espionage within its borders—even if it is only economic espionage—sort of rings hollow. There is no doubt that the United States engaged in espionage and other grey-area illicit activities during the Cold War, as did most of the other twenty-three countries that the CIA recently reported to be currently conducting active economic espionage programs. Further, there are allegations, by France and other European nations, that the United States has in fact commandeered some of its vast counter-intelligence network, namely the Echelon system, to engage in economic espionage for the benefit of its own industries.\textsuperscript{109} Recently, there have been some commentators encouraging the CIA and other U.S. intelligence agencies to engage in more aggressive counter-economic espionage activities going forward,\textsuperscript{110} in effect suggesting the United States should fight fire with fire.

Since every country does it, the singular EEA seems like a feeble and misguided effort to police an activity that is more or less commonplace the world over. In that sense, it is woefully insufficient to affect the kind of widespread change in conduct that it seeks to. The EEA is unique in the fact that it specifies and sanctions an activity specifically within the United States that countries undoubtedly partake in in other countries. It is thus unlikely that the EEA would effect a broad change in other governments’ behavior.\textsuperscript{111} The most likely outcome is that they would merely shift their efforts to other countries that either do not police against economic espionage as effectively, or do not sanction it as severely. Granted, such a change would be perfectly acceptable to the U.S. corporations besieged by industrial espionage within U.S. borders, but recognizing the fact that many of the international companies with the most valuable IP are based in the United States, it is doubtful such a large scale shift of espionage activities to overseas will ever be effected, even if the DOJ ups its enforcement zeal. But as it is now, the U.S. is more likely to seek a politically appealing solution to a really explosive § 1831 case then it is to seek to vindicate rights to the fullest extent allowed by the law.

\textit{iii. Political interference hinders effective enforcement}

EEA prosecutions are commonly tied up by political posturing. While the EEA provides for quite severe punishments, both financially and through incarceration, the legal system is oftentimes not the mechanism the government would most prefer to employ when dealing with apprehended spies. The EEA does not provide for the punishment of foreign governments or their sub-entities—how could it?—so countries have little incentive to cooperate and even less to fear in the form of punishment.\textsuperscript{112} Israel, for example, enjoys a long-term and very strong

\textsuperscript{108} Nasheri, supra note 18, at 23-24.
\textsuperscript{109} Id. (describing an episode where the Echelon system was implicated in Saudi Arabia’s decision to give a large airliner contract to Boeing instead of Airbus); Robert C. Van Arnam, Comment: Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection, 27 N.C.J. Int’l L. & Com. Reg. 95, 130 (2001) (noting that former CIA Director James Woolsey admitted that the United States spied on foreign corporations to protect U.S. companies from bribery and corruption).
\textsuperscript{110} Fink, supra note 15, at 41.
\textsuperscript{111} See Rustmann, supra note 2, at 110.
\textsuperscript{112} Danielson, supra note 20, at 516.
positive relationship with the United States, but has made no secret of its willingness to flout U.S. policies concerning, for instance, trade with certain enemy countries and confidentiality of certain military projects. Yet when Israeli spies are caught misappropriating U.S. trade secrets and brought before the authorities—either legal or political—the records of such transgressions are typically sealed. That is the case, regardless of the outcome.

When it comes to enforcement, the EEA is likely only being used as another chip in political bargaining between international actors, while victimized corporations simply want the return—or in case of unauthorized duplication, the destruction—of the pilfered proprietary information and, if possible, financial redress. But for certain private industries that have Department of Defense contracts, like arms manufacturing and high-tech telecommunications, Congress “discourages parties from seeking redress in the courts system or formal USTR remediation processes.” This is not the case for industries that do not deal with defense or in high-tech; the pharmaceutical industry has not faced the same roadblocks to bringing formal cases to the USTR. This is especially problematic because much international economic espionage is aimed at technologies that have at least some military uses, from new microchips to aircraft designs that have applications for fighter jets. The 2008 criminal case of Ben-Ami Kadish case underscores this point.

It is possible that the only reason the Kadish case developed the way it did was because of Israel’s unique position as “America’s strong ally.” Between 1979 and 1985, Kadish held a security clearance allowing him access to classified documents covering various U.S. weapons systems. In the April 2008 criminal complaint, he was accused of delivering between fifty and one hundred national defense files about nuclear weapons, fighter jets, and missiles to Israeli intelligence operative Yosef Yagur, covering confidential projects by such respected companies as McDonnell Douglass, Hughes, and RCA. Prosecutors had the evidence to support a grand jury indictment of Kadish under § 1831 of the EEA, but instead allowed him to plead guilty to the meager charge of acting as an unregistered foreign agent, punishing him with a fine of $50,000 and no jail time. The corporations that were injured throughout and as a result of the espionage seemingly had strong damage claims against Israel, but, mysteriously, none were pushed forward. The oddly anemic resolution to the case remains a mystery, but according to Grant Smith, despite the Obama administration’s “executive order calling for a new ‘presumption of openness,’ government agencies thwart the release of sensitive information about Israel, possibly fearful of retaliation.”

---

113 See infra note 140 and accompanying text.
116 Smith, supra note 24, at 79.
117 See id.
118 Id.
119 Id. at 80.
120 Id.
121 Id.
122 Id.
123 Id. at 84.
economic losses and negative impact on U.S. national security, the criminal justice system faces institutional barriers in regulating the Israel lobby.\textsuperscript{124}

3. \textit{In the post-Cold War world, economic espionage is not only fair, but prized}

The EEA has not enjoyed much international support. Historically, trade secrets law was a relatively unsettled area of law in international agreements. As a general matter, economic espionage provisions were not included in the major treaties that it could have been included in, such as the GATT or the Paris Convention for the Protection of Industrial Property.\textsuperscript{125} The EEA attempted to criminalize a behavior that had previously been fairly standard procedure. It was a radical, unilateral attempt at imposing U.S. standards on the rest of the world. So far, there has not been as much progress at stemming the tide of this conduct because the U.S. is alone in this crusade, while the other side is populated by a host of other nations. Moreover, the EEA has failed to alter the incentive structure foreign nations are faced with when contemplating beginning or continuing these espionage operations.

i. \textit{Foreign government’s don’t share the United States’ position that they shouldn’t be involved}

Government involvement in corporate competition is not seen in the same light in all countries. The U.S. government putatively maintains a hands-off approach, leaving such matters to the actors themselves. Other nations, some political allies and others rivals, do not share that sentiment.

Outside of the United States, it is possible that the EEA is widely seen by other governments as another “quaint” product of the United States’ interest in policing commercial morality and leveling the corporate playing field, similar to how European firms viewed the Foreign Corrupt Practices Act.\textsuperscript{126} This was the overarching mood surrounding the passage of the Foreign Corrupt Practices Act in 1977, which proscribed bribery and other common but unethical practices by American companies operating abroad, while their competitors freely and beneficially partook in such conduct.\textsuperscript{127} In the matter of trade secret theft, there has thus far been little to no cooperation or collaboration between countries to stop this sort of conduct. Quite the contrary, trade secret misappropriation has often been regarded by multi-national corporations as a part of some countries’ national policy, and therefore, just another cost of doing business.\textsuperscript{128}

More generally, the EEA runs aground because it is attempting to take on an activity that is not even recognized as wrong—ethically or legally—in many other countries. Certain Asian countries have a different, more communal perspective on intellectual property. The predominant conception, rooted in Confucianism, is that knowledge is to be shared and built upon by the community, not walled-off and privatized.\textsuperscript{129} Though it is doubtful that this moral conception is the chief motivating factor for, say, the Chinese’ continued efforts at economic espionage against foreign corporations—it is still more likely the profit motive above all else—this idea does remain in the background and could be at least an obdurate sticking point should the global community ever attempt a large-scale treaty-based endeavor to counter international economic espionage coming from the East. With regards to France, the view there is that economic

\begin{flushright}
\textsuperscript{124} \textit{Id.} at 85.
\textsuperscript{125} See Danielson, supra note 20, 518-19.
\textsuperscript{126} Rustmann, supra note 2, at 127.
\textsuperscript{128} See Brenner & Crescenzi, supra note 65, at 401-13 (2006) (describing the deliberate, government-backed efforts of several nations to misappropriate foreign trade secrets).
\textsuperscript{129} See Danielson, supra note 20, at 514-515.
\end{flushright}
Espionage is a legitimate government activity; as former French DGSE director, Claude Silberzahn, put it, “the state is not just responsible for law making, it is in business as well.”

Governments help their domestic industries, both private and state-owned, because doing so, as a general matter, benefits their entire economy. Such assistance is invaluable because few nations rival the U.S. in having a domestic economy robust enough to support the international aspirations of its domestic companies. U.S. corporations are not as reliant on government assistance, especially when compared to developing nations and the nascent industries therein. But that is not to say that the problem is centered on the Chinas of the world. Israel and France, two of the world’s wealthiest nations and the United States’ most consistent allies, are also at the top of the list as countries actively engaged in espionage activities against U.S. corporations.

Economic espionage is an economically efficient means of developing and competing in new industries. Foreign governments also see such involvement as politically expedient way to further profit the polity. It is also necessary to note that these activities are not uniformly directed at the U.S.; it is just as likely, for example, for a nation to be engaged in espionage operations against the U.S., Japan and another while simultaneously being targeted by yet a fourth. The global playing field is by no means as ordered as it used to be during the Cold War era.

**ii. Foreign governments engage in such activities because the costs are minimal**

Continuing on from the previous point, foreign nations engage in this activity not only because it is arguably legal, but because their cost-benefit analysis of engaging in such activity is heavily weighed towards doing so and the EEA has yet to alter it. Often, the technologies being targeted are of extremely great value, for both military and consumer applications. This thievery may be the most direct path to wealth and national prosperity. “Israel,” it is noted, “became a top-10 arms exporter by tapping U.S. military know-how, shadowing U.S. overseas military deals, and…Israel will soon occupy a top-five slot in global arms exports.” Israel is a representative example of just how invaluable such activities can be to a nation, and how problematic it can be to the United States’ interests.

The U.S. is simultaneously targeted by its allies and rivals. Pierre Marion, another former head of the French spy agency Direction Générale de la Sécurité Extérieure (DGSE) acknowledged this incongruity by explaining, “[i]t would not be normal that we do [sic] spy on the (United) States in political matters; we are really allied. But in the economic competition, we are competitors; we are not allied.” It is no wonder some experts describe economic espionage as kind of “national policy” for some countries. In addition to the French and Chinese, Israel has made no secret of its espionage activities, and can legitimately be described as the country with “the most aggressive program of economic espionage against the United States of any U.S. ally.” Indeed, current Israeli president Shimon Rustmann, supra note 2, at 107. Brenner & Crescenzi, supra note 65, at 399. Danielson, supra note 20 (“[Economic espionage] profits participants and saves the time and the financial resources required to develop technologies independently.”)

Peres explained Israel’s “Uzi Diplomacy,” stating “[b]y not selling an Uzi to a certain country, we are not implementing an embargo against that country, but against ourselves. It is absolute nonsense to embargo ourselves on an item that can be acquired elsewhere.” Israeli espionage has successfully altered the strategic and military balance of power between China and the United States, yet

“in spite of massive economic losses and negative impact on U.S. national security, the criminal justice system faces institutional barriers in regulating the Israel lobby. Political pressures—and the threat of systemic risk—render law enforcement incapable of properly executing its public interest mandate. Because the U.S. government refuses to declassify many of its most sensitive reports about Israeli activity, including espionage, there has been no widespread outcry from industry and the public for more criminal prosecutions or sanctions under treaties.”

One would expect that at least Western ally nations would not be leading the charge of stealing from U.S. corporations. The aforementioned activities of the French and Israelis serve to illustrate a most glaring weakness inherent in EEA enforcement: the DOJ, the CIA, and any other government agency assigned to enforce it will be totally outmatched by the resources and efforts of entire nations who seek to pilfer U.S. trade secrets. It is one thing to catch so-called “two-bit criminals,” foreign or domestic, contracted by and working for foreign governments. But with the level of professionalization and skill in these covert operations, the United States requires at least equal investment in resources and skill by its enforcement agencies if there is to be any headway made against the well-funded corporations and agencies that are the real threat.

The costs associated with failed § 1831 operations really are minimal, when applied to foreign nations. For example, § 1831 of the EEA provides for no punishment against Israel, or any other country, should it be caught red-handed violating the parameters of the Act. Thus, the decision-makers in the Mossad, Israel’s national intelligence agency would include little in the form of total agency legal and financial risk when contemplating an operation targeting U.S.-owned confidential information. The decision-makers may consider some risk to the corporate entity that may ultimately incorporate the misappropriated technology into saleable goods, whether they be weapons for sale on the international market or consumer goods like new chemicals or telecom technology for inclusion into new products that would likely or at least possibly be marketed in the U.S. They may also, but to a lesser extent, consider the risks that would be visited upon the Mossad’s own individual agents who executed the operation, and to an even lesser extent, the anonymous assets that the Israeli agents would employ for furtherance of the plan. Still, due to the fact that the EEA has no tangible effect against the foreign governmental entities that may be at the very top of these criminal operations, it is unlikely foreign governments will ever take the Act seriously and purposefully adjust their activities.

The EEA does not impose costs on foreign nations because foreign nations are not subject to the jurisdiction of U.S. federal courts. Even if a corporation succeeded in bringing a case in U.S. district court against a foreign nation for trade secret misappropriation, they would be barred from recovering by the doctrine of sovereign immunity, which the United States recognizes almost absolutely. Foreign nations are subject to the jurisdiction of international

---

139 Smith, supra note 24, at 82.
140 Id. at 85.
legal regimes, such as the WTO’s Dispute Resolution Body, and treaties. Violation of an agreed upon international agreement would subject the violating nation to sanctions, which the Office of the United States Trade Representative (“USTR”), Department of State, or other competent bureau of the federal government could pursue. These sanctions could be fines, retaliatory quotas or import bans, or some other punishment that would be imposed on the nation itself.

4. **The reasons not to report espionage attacks are legitimate**

As noted earlier, the EEA suffers from a peculiar problem in that the victims of the crimes are commonly not particularly eager to come forward and pursue legal recourse. This peculiarity may be unique to the crime, but the more likely reason is because the EEA—and therefore Congress by extension—failed to provide protection to the victims to support their coming forward.

Companies unfairly face market disincentives for alerting shareholders to security breaches.\(^\text{142}\) This is especially unfair since even the most wealthy and efficient company is at a stark disadvantage when “targeted for clandestine action by some country’s intelligence service,” like the extremely sophisticated French DGSE or the Israeli Mossad.\(^\text{143}\) Regardless, when such information does enter the public knowledge, the results are easily forecasted. The specific facts will be lost in the news media as the newspaper headlines and articles reduce the incident to a smaller and smaller report merely stating that the firm suffered a breach, the possible value lost, and the party behind the breach, if known. As rumors emerge or confidential information gets leaked—like foreign countries or high-level executives involved—the implicated parties get smeared. The first result would naturally lead to decrease in stock value and reputation of the firm and its management; the second result risks fanning the flame and elongating the controversy.

Congress should have provided mechanism to insulate victimized companies from these effects. In the case of § 1831 cases reported to the authorities, protocol for keeping reports confidential and protecting the victims of security breaches from further damage should have been included.

**IV Conclusion**

The Economic Espionage Act cannot simply be fixed. It is not that Congress drafted a poorly designed law, though it did. It is not that the various law enforcement agencies tasked with executing the law have fallen short, though they have. It is that Congress attempted to address a problem much greater than any law could effectively cover. The United States, even with its globally dominant political and economic position, cannot by sheer influence and force mold the behavior of its peers, yet that appears to be the idea behind the EEA. Commentators have suggested that the more effective solution would be to seek binding treaty agreements that specifically address the issue.\(^\text{144}\) Foreign nations, it is argued, do not see economic espionage as a

---

\(^{142}\) Smith, supra note 24, at 83.

\(^{143}\) Id. at 82.

\(^{144}\) See e.g., Mark E. A. Danielson, Economic Espionage: A Framework for a Workable Solution, 10 MINN. J.L. SCI. & TECH. 503, 511 (2009).
violation of international law, and quite possibly, not a violation at all. A treaty would certainly address that gap, and could be the first positive step towards arresting economic espionage.

A treaty—or treaties, should the agreements be bilateral and several—could provide an enforcement mechanism, similar to the DSB provided by the WTO. It could also provide a forum for nations to air grievances against rival nations that fail to adhere to the agreements that they pledged to. And importantly, a treaty could finally change the discourse surrounding economic espionage, or the lack thereof. In particular, a treaty making economic espionage illegal as between the signatories would supplant customary international law and tell the rest of the world that such activity is no longer tolerated. Holdout nations would be smeared, because failing to sign-on would be a tacit endorsement of what its peer nations have proclaimed to be illegal. Signatories would therefore have grounds to punish violators and non-signatories. It is not hard to imagine how a treaty would be effective against say, Israel, if the U.S. had entered a multilateral agreement with several of its European peers specifically addressing trade secrets and Israel steadfastly refused to join, or joined and was caught violating it. The next step in the battle against economic espionage has to be the beginning of treaty negotiations between influential nations with an actual desire to arrest this activity.