# ECONOMIC ESPIONAGE ACT – THE FEDERAL GOVERNMENT SEEKS TO PROTECT CONFIDENTIAL INFORMATION

**Presented by:**

**W. Neil Eggleston**

*From ACCA's European Chapter Annual Meeting 2000*

**Economic Espionage Act – The Federal Government Seeks to Protect Confidential Information**

Until 1996, the federal government enjoyed only a limited ability to protect trade secrets. Applicable statutes were unwieldy when used to prosecute trade secret theft: the Interstate Transportation of Stolen Property Act, for instance, requires a "physical taking" of the goods in question, and the wire and mail fraud statutes require use of the mail or wires. Congress attempted to address those problems with the Economic Espionage Act (EEA), codified at 18 U.S.C. §§ 1831-1839.

## I. Overview

The EEA criminalizes both what it terms "economic espionage," the misappropriation of trade secrets involving a foreign government, and the domestic theft of trade secrets. The EEA is a criminal statute; it creates no civil cause of action for the victim.

### A. Domestic Theft of Trade Secrets—Section 1832[1]

To obtain a conviction for domestic trade secret theft under section 1832, the government must prove beyond a reasonable doubt that the defendant (1) stole, or, without authorization of the owner, obtained, destroyed or conveyed information; (2) knew that this information was proprietary; (3) intended to convert the trade secret to the economic benefit of anyone other than the owner; (4) intended to harm the owner; (5) the trade secret was used in interstate commerce; and (6) the information was, in fact, a trade secret.

#### (1) Misappropriation

[1] In addition, Section 1831 criminalizes "economic espionage," the theft of trade secrets intended to benefit a foreign government or instrumentality. The EEA defines "foreign instrumentality" loosely; a foreign corporation would qualify, if "controlled, sponsored, commanded, managed, or dominated by a foreign government." To date, the government has brought no prosecutions under Section 1831, though several foreign nationals have been indicted and convicted under Section 1832.

While the physical removal of the object of the crime clearly constitutes theft, the Act may be violated though the property never leaves the

control or custody of the owner. The EEA proscribes the unauthorized copying, duplication, sketching, drawing, photographing, downloading, uploading, transmission, sending, mailing, and communication of a trade secret as well. The EEA also requires proof that the defendant acted without authorization, either to obtain a trade secret or to destroy or convey it. Thus, an employee who has legitimately obtained a trade secret would still violate the Act by conveying it without permission. Buying a trade secret with the knowledge that it was obtained in this manner constitutes a violation as well.

**(2) Intent Requirement**

Under section 1832's intent requirement, the government must prove that the defendant knowingly misappropriated the trade secret. The government cannot prosecute a person who mistakenly, ignorantly, or accidentally misappropriates a trade secret.

**(3) Economic Benefit**

The simple destruction or theft of a trade secret perpetrated out of spite or for revenge would not violate section 1832, so long as no one received any economic benefit from the act. The government must prove that the defendant intended to economically benefit someone other than the owner.

**(4) Intent to Injure**

Section 1832 requires that the government prove an intent to injure the owner of the trade secret. Proof of malice or evil intent is not; however necessary. Proof that the defendant "knew or was aware to a practical certainty" that his action would harm the owner will satisfy the knowledge requirement.

**(5) Interstate Commerce**

The government must also establish that the stolen trade secret was "related to or included

in a product that is produced for or placed in interstate or foreign commerce." While it may be difficult to establish that a product in the research and development stage is involved in interstate commerce, the ultimate potential for interstate sales should be sufficient. The interstate commerce requirement also raises the question of whether the EEA protects trade secrets relating to services, rather than products. The issue is yet to be litigated, but it seems unlikely Congress would have thus limited the EEA's protections.

**(6) Stolen information must have been a trade secret**

The EEA adopts a more expansive definition of trade secrets than the Uniform Trade Secrets Act definition used by most states. Under the EEA, trade secrets include 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," however stored or preserved, if two conditions are met:

- The owner has taken "reasonable measures" to keep the information secret. To determine "reasonableness," the U.S. Attorney's Manual instructs prosecutors to examine whether the security measures are commensurate with the value of the trade secret. Examples of reasonable measures can include advising employees of the existence of a trade secret, limiting access thereto to only those necessary, and requiring employees to sign confidentiality agreements.

- The trade secret derives "independent economic value from not being generally known to … the public." Value may be determined by what a buyer would pay on the open market, or, absent such a legitimate market, by the black market value. Where the value of a trade

secret is indeterminate—it is still in development, for instance—economic value may be determined through

consideration of development, research, and production costs.

Trade secrets do not include general knowledge, skill, or abilities acquired while employed, nor can an employee be prosecuted based simply on the assertion that he was exposed to a trade secret while employed. The distinction between general business knowledge and protected trade secrets has not been addressed by the courts, but presents a likely source of dispute in future cases.

**B. Attempt and Conspiracy**

Both sections 1831 and 1832 criminalize attempts and conspiracy to steal trade secrets. The Third Circuit has held that the offenses of attempt and conspiracy to steal trade secrets do not require the existence of an actual trade secret as an essential element of the offense.

**C. Extraterritorial Application**

Section 1837 expressly provides that the EEA covers conduct outside the United States if the offender is a U.S. citizen or permanent resident, or, if the offender is a corporation, organized under U.S. laws. The EEA also reaches the activities of foreign nationals and corporations acting in the United States. Under this provision, sale of a product containing a stolen trade secret within the United States would violate the EEA, regardless of where the product was manufactured. The United States has not attempted to apply the EEA extraterritorially.

## II. Remedies and Penalties

An individual convicted under the EEA may be sentenced to a maximum of 10 years and a $250,000. A corporation similarly convicted may be fined up to $5,000,000.

### A. Civil Proceedings

Section 1836 allows the government to seek a civil injunction. While this provision may allow the government to halt further dissemination of the trade secret in the initial stages of a prosecution, the ability to enjoin a putatively criminal act adds little additional force to the EEA. The EEA does not, however, create a civil cause of action for victims.

### B. Criminal Forfeiture

Section 1834 provides that the sentencing court "shall order" the forfeiture of "any property constituting, or derived from, any proceeds the person obtained, directly or indirectly," from the theft of the trade secret, and incorporates existing forfeiture laws. The court may also order forfeiture of any property used to commit the offense, with due consideration to the proportionality of forfeited property to the magnitude of the offense. The United States would obtain title to any forfeited property, but the legislative history suggests that victims could petition the Attorney General for restitution from the forfeited property under 28 C.F.R. § 9. Potentially, the sale of forfeited property could result in further dissemination of the stolen trade secret, but it is likely the government would deal with such property as it does seized counterfeit goods, and destroy the property.

## III. Prosecutions

To date, the government has brought eleven separate cases under Section 1832 of the EEA. One prosecution has gone to trial, several have resulted in

guilty pleas, and an interlocutory appeal in another resulted in one reported decision. Prosecutions thus far have been relatively straightforward: each case has involved a defendant offering his own company's trade secrets for sale, or attempting to buy or sell the trade secrets of another company. Commentators have suggested that the government is initially pursuing only relatively clear cut violations of the EEA to build a body of case law with lesser offenders and "work out the bugs" before pursuing more difficult cases. The government has yet to invoke section 1831, despite the indictment of several foreign nationals employed by foreign corporations—no involvement of foreign governments has been demonstrated.

**A. Recent Cases**

Until 2001, U.S Attorneys seeking to prosecute EEA violations must, under an agreement with Congress, obtain personal approval from either the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

**United States v. Davis (D. Mass)**
In September 1997, a Nashville grand jury indicted Steven Davis for attempting to sell design information for the Gillette Mach 3 razor to competing razor manufacturers. The engineer, employed by a design firm assisting Gillette with development of the new razor, emailed and faxed copies of the technical diagrams for the Gillette razor to Warner Lambert, American Safety Razor, and Bic in hopes of selling the information. Davis, arrested after Bic disclosed the theft to Gillette, pled guilty, and was sentenced to 27 months and order to pay $1.2 million to Gillette.

**United States v. Trujillo-Cohen (S.D. Tex.)**
In the first case in which the EEA provided the sole ground for indictment, the Houston U.S. Attorney indicted a Deloitee-Touche employee after she converted and sold a proprietary accounting software program. Tujillo-Cohen pled guilty, and was sentenced in October 1998

to 27 months in prison. She was further ordered to pay $337,000 in restitution.

**United States v. Campbell (N.D. Ga.)**
The circulation manager of the Gwinette Daily Post and another employee were arrested and charged with both mail fraud and violation of the EEA after offering to sell their papers' marketing plans and circulation lists to the Atlanta Journal-Constitution. Carroll Campbell pled guilty, and was sentenced to three months in prison, four months' home confinement, and ordered to pay $2,800 in restitution. His accomplice received a sentence of three years' probation, a $1,000 fine, and $500 in restitution.

**United States v. Fulton (W.D. Penn.)**
After Joy Mining fired John Fulton from his position as the manager of its electronics service center, Fulton began his own mining repair business. The FBI arrested Fulton in November 1997 after he attempted to purchase proprietary information from a Joy Mining employee. Fulton pled guilt to violation of the EEA, and received five years' probation, with 12 months of home confinement.

**United States v. Camp (D. Maine)**
Caryn Camp, a chemist for Indexx Laboratories, pled guilty after being charged with conspiracy to steal trade secrets, wire and mail fraud, interstate transportation of stolen goods, and conspiracy to transport stolen goods. The chemist was arrested in July 1998 after the FBI found on her computer over 200 emails containing trade secrets that had been sent to a California businessman whom she met over the Internet.

**United States v. Krumrei (E.D. Mich.)**
Wilsonart hired Krumrei, a Michigan attorney, in a non-legal capacity to assist in the

developmen
t of a new
process of
laminating a
formica-like
coating.
After
learning key
details

about the process, Krumrei offered to sell them to one of Wilsonart's Australian competitors. After the Australian company notified Wilsonart, Wilsonart contacted the FBI, which arrested Krumrei after he met with an agent of the Australian company in Hawaii.

**United States v. Hallsted & Pringle (E.D. Tex.)** In April 1998, five prototype Intel CPUs were stolen from Corollary, Inc. during a burglary. After an Intel security officer noticed the CPUs for sale on the Internet, Intel attempted to purchase the CPUs. Steve Hallsted refused, and attempted to sell the chips to Cyrix, Inc. Cyrix reported the offer, and the FBI arrested Hallsted and Brian Pringle when they drove to Cyrix's Texas plant with the CPUs. Both Hallsted and Pringle pled guilty. Hallstead received a sentence of six years and five months in prison, and ordered to pay $10,000 in restitution. Pringle was sentenced to five years in prison and ordered to pay $50,0000.

**United States v. Pei (D. N.J.)**
A former research scientist for Roche Diagnostics was arrested in July 1998 under the EEA after attempting to by from a current employee information concerning a Roche hepatitis diagnostic kit. The case is pending.

**B. Trade Secret Confidentiality**

Three cases have raised the issue of trade secret confidentiality. The EEA creates a dilemma for the victim: cooperation with the government risks further disclosure at trial of intellectual property that obtains value by its secrecy, but the failure to do so may allow offenders to escape prosecution. While the government is responsible for prosecuting the offender, it lacks the inherent incentive of a civil litigant to protect its own trade secrets. Additionally, the court must balance the defendant's Sixth Amendment rights with the need to protect the trade secrets. Fears of further

dissemination of a trade secret should not discourage reporting of the theft, however. Section 1835 provides that the court "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets." In the event that the district court authorizes or directs the disclosure of any trade secrets, Section 1835 allows that an interlocutory appeal shall lie.

**U.S. v. Hsu, 155 F.3d 189 (3d Cir. 1998) (*rev'g* 982 F. Supp. 1022 (E.D. Pa. 1997))**
In 1995, the government indicted two employees of the Taiwanese company Yuen Foong Paper Company and a Massachusetts biochemist for conspiracy to steal information concerning the manufacture of the anti-cancer drug Taxol from Bristol-Myers Squibb. While one Yuen Foong employee remained safe from extradition in Taiwan, the FBI arrested the other employee and the American after they met with an undercover FBI agent who provided documents outlining Taxol production processes. The defendants made a discovery request for a copy of those documents, arguing that the documents' disclosure was essential to a defense of legal impossibility. The government responded with a request for a protective order under section 1835 to prevent disclosure of Bristol-Myers trade secrets. The district court, reasoning that a protective order would violate the defendants' Sixth Amendment right to cross examination, ordered disclosure of the documents. On interlocutory appeal, the Third Circuit reversed, noting "a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." In overturning the lower court's decision, the Third Circuit held that legal impossibility was not a defense to a charge of attempt or conspiracy to misappropriate trade secrets in violation of Section 1832(a)(4).

While the existence of an actual trade secret as defined by Section 1839(3) is a *sine qua non* of

the substantive offense, a defendant may be charged with attempt under that section, even if the trade secrets in question are not actually trade secrets. Thus, the Third Circuit ruled that it was not necessary for the government to disclose the Bristol-Meyers documents.

In February 1999, the government dropped the charges against the third defendant, the Massachusetts biochemist present at the meeting to assess the technology offered for "sale" by the undercover FBI agent. The remaining defendant, Hsu, awaits trial.

**United States v. Yang (N.D. Ohio)**

In 1997, an FBI sting netted Pin Yen Yang, chairman of another Taiwanese company, the Four Pillars Enterprise, and his daughter, Hwei Chen Yang, a Ph.D. chemist employed by the firm, for the theft of trade secrets from Avery-Denison Corporation. The FBI arrested the father-daughter duo after catching an Avery-Denison employee, Dr. Victor Lee, in the act of riffling through Avery files concerning the manufacture of Avery self-adhesive products. In return for a yearly salary of $25,000 from Four Pillars, Lee stole an estimated $200 million worth of proprietary information over an eight-year period. Lee agreed to cooperate with the government, and ultimately pled guilty to a single count of wire fraud. The first EEA defendants to go to trial, the Yangs, were tried in the U.S. District Court in Youngstown, Ohio, and convicted of conspiracy to steal and attempt to steal trade secrets under section 1832.

According to their attorney, the Yangs plan to appeal, on the grounds that the information they were convicted of attempt and conspiracy to steal was not actually a trade secret—an argument rejected by the Third Circuit in the Hsu case.

**United States v. Worthing (W.D. Penn.)**
Two men pled guilty to charges filed under section 1832 for stealing fiberglass manufacturing and production information valued at $20 million from PPG Industries. As the head of a building maintenance crew contracted with PPG, Patrick Worthing used his access to all building offices to collect diskettes, blueprints, and other proprietary materials. Alerted by Worthing's letter to Owen-Corning offering to sell PPG trade secrets, the FBI arrested Worthing and his brother, who had agreed to participate for $100. Patrick Worthing received a fifteen-month sentence, with three years' probation. PPG agreed to cooperate with the government only after receiving assurances from the FBI that its trade secrets would be protected.

**C. Potential protective measures suggested by commentators include:**

- Pretrial protective orders
- Closure of courtroom during trial
- Requesting that evidence used at trial not be displayed in open court
- Sealing of court records at the conclusion of trial
- Redaction of confidential information from trial transcript
- Jury instructions ordering jurors not to disclose information after trial

## IV. Reasonable measures

For the stolen information to receive protection as a trade secret under the EEA, the victimized company

must have taken "reasonable measures" to protect it. Though no court has ruled on the issue, the reasonableness of protective measures is likely to

require they be commensurate with the value of the trade secrets. The Department of Justice Criminal Resource Manual directs prosecutors to consider:

- Evidence that the purportedly stolen information was, in fact, a trade secret
- Whether the information was readily distinguishable from less protected information
- Whether the company restricted distribution of the trade secrets
- Whether the company had instituted non-disclosure agreements used to protect the proprietary information
- The existence of other protective measures, such as password-protection, data encryption, or physical security

Other commentators suggest that all documents and computer programs containing trade secrets should be stamped or contain a notification that they are protected as such under the EEA, and that employees and potential employees are aware of the penalties for trade secret theft.

**Defenses**

While the EEA does not expressly provide any defenses, the legislative history suggests that parallel development and reverse engineering may suffice to rebut a charge under the EEA. Additionally, the use at a new job of general knowledge and skills acquired by an employee at a previous job does not violate the EEA. To date, no defendant charged under the EEA has raised these defenses. The *Hsu* court did rule that legal impossibility is not a defense to attempted trade secret theft or conspiracy to steal trade secrets.

**Parallel Development**
According to the legislative history, the EEA does not prohibit companies from developing a product on which they know another company is working.

Faced with an allegation of trade secret theft, documentation of independent development should be sufficient to rebut a charge.

**Reverse Engineering**

It is unlikely that the reverse engineering of a lawfully obtained trade secret would be considered a violation of the EEA. The EEA's legislative history indicates a focus on whether the accused committed a proscribed act, rather than whether reverse engineering occurred.

## V. Other Options

At least one company has filed a civil RICO action against the defendants in an EEA case. Avery-Denison brought a case against the *United States v. Yang* defendants. The government, however, sought and received a partial stay of the civil action while the criminal case was pendant. Now that the trial phase of the criminal case is complete, the civil action may proceed.