Arrests and Convictions Resulting from the Economic Espionage Act of 1996

The goal of the following case summaries is to enhance counterintelligence awareness among employees at the Nevada Complex by showing that espionage involves real people in workplace situations like their own. The case summaries do not resemble glamorized fictional accounts of spy novels; rather, they tell a mundane tale of human folly resulting in tragic personal consequences. Lessons learned show that: 1) many of the situations described in the summaries might have been avoided if concerned co-workers, recognizing danger signs, had been willing to intervene; and 2) most offenders are trusted insiders, not foreign agents. Even "friendly" countries have been the recipients of stolen U.S. classified and proprietary information. These damaging betrayals can occur in government, contractor organizations, or private industry. The Fortune 1000 corporations in the USA lose more than $45 billion worth of proprietary information to theft each year, according to the American Society for Industrial Security. The number of reported incidents of thefts grows each year. The maximum statutory penalty for a conviction under the EEA is 10 year of imprisonment and a fine of $250,000 (or twice the gross gain or gross loss, whichever is greatest).

There are numerous convictions of Economic Espionage every year and the numbers continue to grow. The following representations provide insight into the kind of activities being investigated:

Timothy Kissane, New York
May 2002

KISSANE worked as a release engineer at SMARTS, and was responsible for the packaging of multiple components of the SMARTS software package, including its

source code. "Source code" is the underlying computer program that is used to create a software package that can be sold to customers. If a competitor obtained the source code for a software program, it could convert some or all of its features into its own software.

SMARTS developed and sold a custom software program called "InCharge", which monitors large computer networks, and identifies operational problems on the network. SMARTS sold "InCharge" to large telecommunications companies around the country and abroad. "InCharge" is a proprietary computer program, and its source code is a guarded secret. According to the Information, on February 21, 2000, KISSANE signed an employment contract in which he agreed to "forever keep secret" confidential SMARTS information that he had access to, including "software codes."

On November 28, 2001, KISSANE's employment at SMARTS was terminated. Several weeks later, two of SMARTS' competitors received email messages from a "Joe Friday" at a Yahoo! email account, offering SMARTS' source code for sale. According to the Information, one of the email messages stated that the sender possessed the "cvs repository of SMARTS InCharge code, from 11/20/01 as well as custom code for specific bug fixes and customer-requested enhancements." The competitors brought these email messages to the attention of SMARTS.

According to the Information, connections to the Yahoo! email account from which the "Joe Friday" email messages were sent was opened at the White Plains Library, White Plains, New York. As the earlier Complaint charged, this Yahoo! account was then accessed approximately thirty-three additional times in December 2001 from a Verizon DHL Internet account located at the Lavallette, New Jersey address where KISSANE had previously informed SMARTS that he would be living.

TIMOTHY KISSANE was sentenced on October 15, 2002 to two years in prison for theft of a trade secret in connection with his prior employment at System Management Arts Incorporated ("SMARTS"), a software company based in White Plains, New York. In imposing the 24-month prison term, United States District Judge RICHARD CONWAY CASEY determined that KISSANE's sentence should reflect his abusing a position of trust at SMARTS.

Say Lye Ow, California
September 2001

Mr. Ow, age 31, formerly of Penang, Malaysia, pled guilty to copying without authorization computer files relating to the design and testing of the Merced microprocessor (now known as the Itanium microprocessor). At the time, Mr. Ow knew this was a trade secret of Intel Corporation but wanted to use the information at his new employment to enhance his economic benefit. The Itanium microprocessor was under joint development by Intel and Hewlett-Packard Co. since 1994 and was released earlier this year. On December 11, 2001, Ow pled guilty to copying a trade secret in violation of the Economic Espionage Act of 1996.

The Judge sentenced Ow to a term of imprisonment of 24 months and a term of supervised of release of two years to follow the prison term. Ow was ordered to surrender himself to begin serving his prison sentence on January 15, 2002. The Judge previously issued a preliminary order of forfeiture regarding the criminal forfeiture of Ow's interest in the computer system, which he used to commit and facilitate the commission of the copying a trade secret offense. A final order of forfeiture will be issued in the near future.

Nicholas Daddona, Connecticut
June 2001

Daddona, age 44, while employed by Fabricated Metal Products, Inc. (FMP) began working for a competitor, Eyelet Toolmakers Inc, without FMP's knowledge. While working simultaneously for both companies, Doddona stole and duplicated from FMP unique engineering plans for the development and manufacture of a large transfer press and tooling specifications, then delivered them to Eyelet and another company working for Eyelet. These plans were stored on FMP's computers. Doddona was also charged with one count of unauthorized access to FMP's computers.

On March 11, 2002, Daddona was sentenced to 5 months of home confinement with electronic monitoring to be followed by 36 months of probation. The Judge also ordered Daddona to pay a fine in the amount of $4,000.00 and a special assessment in the amount of $100.00. Daddona previously agreed to pay restitution in the amount of $10,000 to the victim.

Takashi Okamoto and Hiroaki Serizawa, Ohio
May 2001

Okamoto, age 40, was employed by the Cleveland Clinic Foundation (CCF) in Ohio to conduct research into the cause and potential treatment for Alzheimer's disease. Serizawa, age 39, was employed by the Kansas University Medical Center. Serizawa was a close friend and peer of Okamoto from the mid-1990s. Okamoto and Serizawa conspired to misappropriate, from the CCF, DNA and cell line reagents and constructs developed by researchers at CCF. Okamoto and Serizawa did benefit upon RIKEN, an instrumentality of the government of Japan, by providing RIKEN with the misappropriated genetic material. RIKEN had given Okamoto a position as a neuroscience researcher to begin in the fall. Okamoto not only misappropriated the genetic material, but he sabotaged and destroyed the DNA and cell line reagents and constructs not removed from the laboratory. Okamoto shipped, by private interstate carrier, the four boxes of stolen material, to Serizawa in Kansas. Okamoto resigned from his research position and flew to Japan to begin his position at RIKEN. Approximately two weeks later, Okamoto flew to back to the U.S. to Kansas to retrieve the stolen materials. Okamoto and Serizawa filled small laboratory vials with tap water and made meaningless markings on the labels. Okamoto instructed Serizawa to provide the vials to officials at the CCF in the event they came looking for the missing genetic materials. Serizawa provided materially false, fictitious, and fraudulent statements in an interview with the FBI, who were investigating the theft of the genetic material. Okamoto and Serizawa were charged with economic espionage, economic sabotage, and transporting, transmitting, and transferring in interstate, and foreign commerce, stolen material.

On September 17, 2002, in the U.S. District Court in Akron, Ohio, Hiroaki Serizawa, Ph.D. of Overland Park, Kansas entered a plea of guilty to a single count Information containing the charge of making false statements (18 U.S.C. §1001). The government is seeking Dr. Okamoto's extradition from Japan.

TAL Industries, Inc., California
May 2001

A Chinese-run company, TAL Industries Inc. a California-based subsidiary of the China National Aero-Technology Import and Export Corp. (CATIC), a government-owned defense firm that is the Chinese military's main purchasing arm, entered a plea of no contest to a charge of felony violation of the U.S. export laws.

On May 12, 2001, the company agreed to pay $2.3 million in fines and penalties to settle criminal and administrative charges stemming from a business deal in which aerospace equipment purchased from McDonnell Douglas Corp. wound up in a Chinese military plant. TAL Industries Inc. agreed to pay $1 million fine and to spend five years on probation. They also agreed to pay $1.3 million in penalties to settle administrative proceedings before the Commerce Department and it will give up its U.S. export privileges for 10 years.

Criminal charges remain pending against McDonnell Douglas and its subsidiary, Douglas Aircraft Co. The charges stem from McDonnell Douglas's 1994 sale to CATIC of $5.4 million in sophisticated machining equipment used to manufacture aircraft parts.

Jack Shearer, Texas
June 2000

Jack Shearer, age 54, pled guilty and three corporations founded by Jack Shearer - - Tejas Procurement Services, Inc.; Tejas Compressor Systems, Inc.; and Procurement Solutions International - - pled guilty, by their duly appointed representatives to two counts of conspiracy to steal trade secrets. Tejas' revenues from the stolen trade secrets were in excess of $7 million. Shearer admitted that he stole intellectual property, or proprietary trade secrets, from his former employer, Solar Turbines Incorporated (Solar) headquarters in California. Shearer worked for Solar for twenty-six years until his employment was terminated in 1992. While he was employed at Solar, Shearer lived overseas and serviced a sales territory that included Libya, Jordan, Syria, Lebanon, Iraq, Iran, and Saudi Arabia. When Shearer was terminated from Solar, he started up his three corporations in Texas in order to compete with his former employer. Shearer obtained Solar's trade secret information and used that information to manufacture counterfeit Solar parts through Tejas. Shearer obtained this confidential trade secret

information through three former co-workers and friends from Solar. (All now former employees of Solar and pending trial) Tejas, at Shearer's direction, paid each of the employees to provide Solar drawings, plans, and schematics that included confidential specification describing the dimensions and manufacturing details of Solar parts. One of Shearer's and Tejas' main customers was an Iranian national businessman who operated an oil and gas parts broker business in Uppsala, Sweden. This businessman placed millions of dollars of orders per year with Tejas and orders he placed were designed for oil field applications and painted desert beige. Tejas and a number of it's employees became suspicious that the parts ordered by this Iranian national businessman were going to prohibited countries, such as Iran.

Jack Shearer was sentenced to 54 months of imprisonment and ordered to pay $7,655,155.00 in restitution. William Humes (one provider of information from Solar) was sentenced to 27 months of imprisonment and ordered to pay $3.8 million in restitution. Corporate defendants, Tejas Corporations, were each sentenced to five years probation and ordered, jointly and severally, to pay $7,655,155.00 in restitution.

Caryn Camp and Stephen Martin, Maine
December 1999

Caryn Camp, an Idexx employee, became aquatinted with Stephen Martin when she applied for a job via the Internet. The two began a friendship that eventually led to Camp sending Martin secrets about Idexx so he could start a competing company. According to prosecutors, Camp used E-mail, the postal service and commercial carriers to send proprietary Idexx documents to Martin. They were caught when Camp accidentally sent an E-mail to a co-worker saying, "They know I've been stealing, so to speak, from the company and sending information to someone. Can I go to jail for this? I'm so scared".

On December 20, 1999, Martin was sentenced to 366 days imprisonment, 3 years supervised release, $7,500 restitution and $800 special assessment. Camp pled guilty and was sentenced on December 17, 1999 to 3 years probation, $7,500 restitution and $1,500 special assessment.

Steven Hallstead and Brian Pringle, Texas
December 1998

Five "Slot II" computers were stolen from an Intel facility in April, 1998. They contained various trade secrets that were not due to hit the market until June, 1998. In May, 1998, Steven Hallstead, age 29, contacted a Cyrix representative and offered to sell the Slot II computers for $75,000. Cyrix immediately contacted the FBI who set up a sting operation. Hallstead's business partner, Pringle, age 34, was set to deliver the monitors and was arrested upon delivery. Hallstead was later detained in California.

The two men pleaded guilty and on December 4, 1998, Hallstead was sentenced to six years, five months imprisonment and a $10,000 restitution. Pringle was sentenced to five years in prison and a $50,000 restitution.

Mayra Justine Trujillo-Cohen, Texas
October 1998

Ms. Trujillo-Cohen, age 46, a former consultant for Deloitte & Touche, pled guilty to taking proprietary SAP Implementation Methodology, considered to be intellectual property, from her employer, ICS, Deloitte & Touche, and then attempting to convey that methodology as her own creation for personal financial gain after she had been terminated from ICS, Deloitte & Touche. She also pled guilty to wire fraud. She admitted to developing a scheme wherein she was able to use an insurance company's bank account to pay her American Express credit card bill through wire transfers. Over a period of several months, she transferred approximately $436,000.00. Some of the items she used the money to purchase were a Rover, Sport Utility Vehicle, furniture, jewelry, and several Rolex watches.

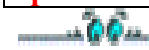
She was sentenced on October 26, 1998 to 48 month's imprisonment, 3 years supervised release, $337,000 in restitution and a $200 special assessment. The third-party company was not indicted.

Carroll Lee Campbell, Jr., Susan Campbell, and Paul Soucy
August 1998

Carroll Campbell, Jr. and his wife, Susan Campbell, were indicted for conspiring with a third party, Paul Soucy, to convert trade secrets relating to the Gwinnett Daily Post newspaper, owned by Gray Communications, Inc. In September 1997, Carroll Campbell sent a letter to the attorneys representing the Atlanta Journal-Constitution, offering to

provide the Cable Equities Agreement and other proprietary financial and business information to help them in a lawsuit against the Gwinnett Daily Post newspaper. The offering price for the information was $150,000. The FBI was contacted and a sting was set up.

Mr. Campbell pled guilty to conspiring to steal trade secrets and was sentenced on August 25, 1998, to 3 months imprisonment, home confinement for 4 months with electronic monitoring detention, 3 years supervised release, $2800 restitution, $100 special assessment.



Steven Davis, Missouri
April 1998

Steven Davis, age 47, an employee of Wright Industries, a subcontractor for Gillette, pled guilty to five counts of theft of trade secrets. Davis told the court that in anger at a supervisor and fearing that his job was in jeopardy, he decided to disclose trade secret information to the Bic Corporation and other competitors.

Davis was sentenced on April 17, 1998 to 27 months imprisonment, 3 years supervised release, and $1,271,171.00 in restitution.