

## White Paper

# Protection Under Law:

Understanding the Economic Espionage Act of 1996

## Table of Contents

2	Introduction
3	An historical view of espionage
5	Protecting trade secrets
14	Taking action

## Introduction

With business expanding globally, corporations require the establishment of an intelligence system that allows them to obtain information about competitors, analyze the information, and use it to gain an advantage in the marketplace. Business intelligence, or competitive intelligence as it is known, emerged as the result. But the tactics used to collect business intelligence should be a cause of great concern for organizations—and for good reason. Economic espionage has long been a serious potential risk for corporations, and it continues to threaten the economic well-being of virtually any size enterprise.

## The Face of Espionage

Espionage can be traced back thousands of years—from the secret processes of China’s silk industry to the Cartwright loom of Britain’s textile industry of the 1800s, and now to the chips of Silicon Valley in the new millennium.<sup>1</sup> Espionage continues because governments and commercial enterprises need to know what their friends and foes are doing and how they are doing it in order to gain the desired advantage, be it defense or economy driven.

Over the centuries, governments have invested fortunes to master the art of espionage. The former Soviet Union, for example, directed a human spy network that exceeded 900,000 human sources during the peak of the Cold War, in stark comparison to between 70–80 thousand in the U.S. intelligence community.

Today, there is still no government or corporation immune to the threat of espionage. The motives and tactics have remained constant over the years—economic gain, competition, career recognition, and vengeance. However, the methods used to collect and transmit information have significantly changed as a result of high technology, the World Wide Web, and worldwide telecommunications.

---

<sup>1</sup> The Industrial Revolution was fueled in part by the work of Francis Cabot Lowell who memorized the plans to the Cartwright loom while visiting in England in 1811.

This white paper chronicles the recent history of espionage and describes how and why global organizations are at risk of losing vital trade secrets to competitors and foreign governments. The paper goes on to explain the actions taken by the United States government to curtail espionage activity.

## **An historical view of espionage**

### **Post-Cold War**

The political change resulting from the collapse of the former Soviet Union and Eastern Block countries, combined with the globalization of commerce and the mobilization of the workforce due to advancements in technology and digital communications, has transformed the modern world. A nation's power has been traditionally defined in military terms, but now it is increasingly defined in economic terms. Even the strength of the United States is largely based on its ability to compete in a global economy.

It is because of this shift that new governments emerging out of the rubble of the Soviet era altered the focus of their intelligence services from military secrets to trade secrets, as part of a commercial modernization strategy.

Business entrepreneurs in Russia and Eastern Europe quickly realized the value of hiring ex-KGB agents, given the fact that wiretapping was rampant and there was a general belief that there were no secrets that cannot be bought. Hiring a former intelligence officer brought years of information-gathering experience, access to global networks, and technical expertise to conduct sophisticated espionage operations. Therefore, the competitive needs of a company that could not be achieved through legitimate means could be acquired through unlawful means. For instance, unethical companies that did not have the financial resources to support comprehensive R&D projects could still level the playing field by stealing R&D results from competitors (typically from the United States).

Through the 1980s and 1990s, the reduction in trade barriers and the globalization of money markets spurred unprecedented opportunity for international business. Entrepreneurs quickly advanced strategies to capture new markets, forge new partnerships, and develop joint ventures in this global economy. But the allure of globalization was accompanied by a dangerous false sense of security. This highly competitive environment poses enormous challenges and risk. "In almost every industry, globalization is leading to overcapacity, which is leading to commoditization and/or price deflation. Success therefore will go to the fittest—not necessarily the biggest. Innovation in process—how things get done in an enterprise—will be as important as innovation in the products a company sells."<sup>2</sup>

### **Post 9/11 Era**

The unconscionable act of terror that occurred on September 11 has awakened America and the nations of the free world to the fact that our national security and economic security are at risk. The cornerstone of the terrorists' success was—and continues to be—the acquisition and use of information by whatever means. They are strategically targeting American industries to acquire dual use technologies that may be used in biological, chemical, and nuclear weapons delivery systems. George Tenet, Director of the Central Intelligence Agency, stated it well: "Today we must still deal with terrorists, insurgents, and others who have hundreds of years of history fueling their causes—but chances are they will be using laptop computers, sophisticated encryption, and weaponry their predecessors could not have even imagined."<sup>3</sup>

In a global community in which information and communications technologies have transformed the way spies collect, analyze, and transmit information, America faces an unprecedented challenge to survive. The war on terrorism is a matter of grave importance to our nation. Winning this war is largely contingent on the containment of weapons technology and insuring a healthy economy. Democratic society must stop the safe passage of hostile enemies traveling the information highway of America to gain access to companies and their databases of knowledge.

---

<sup>2</sup>Lou Gerstner, *Who Says Elephants Can't Dance?*, November 2002

<sup>3</sup>Report to Congress, CIA Director, February 1999

## Protecting trade secrets

Given all the global changes, the United States government recognized the dangers of economic espionage and trade secret theft to national security.

After all, trade secrets are the lifeblood of most process-driven companies and play an integral part of trade, commerce, and industry. Those who control information amass power and competitive advantage in the global marketplace, and ultimately economic superiority. It naturally follows, then, that organizations that fail to safeguard their intellectual assets lose ground. William Boni, Global Director of Information Protection for Motorola and co-author of *Netspionage: The Global Threat to Information*, explains:

*“Because most organizations don’t have a means of tracking the loss of proprietary information, they go on constantly hemorrhaging, constantly losing market share. Gradually it takes the vitality out of the organization because it’s hard to invent and create things faster than people are leaking it or stealing it.”<sup>4</sup>*

Because of the importance of keeping trade secrets safe from competitors, foreign agencies, and opportunists, the United States government enacted the Economic Espionage Act of 1996 (EEA).

The EEA can be viewed by a CEO as both a proscription of what cannot be done in the conduct of business, and a prescription of what must be done to have protection under the law. The EEA was not enacted to stifle business or employees’ careers, but to help them.

The EEA statute broadly defines a trade secret as “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, programmed 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 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.” 18 USC §1839(3).

### Prohibited acts—a proscription of what cannot be done

The EEA has two main components that criminalize the misappropriation of trade secrets:

- Section 1831 is directed against entities and individuals sponsored by foreign governments.
- Section 1832 is directed against all individuals and entities regardless of whose behalf they were acting upon.
- Both sections prohibit the same misconduct regarding trade secrets, punishing anyone who:
- Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information.
- Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information.
- Receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

Both sections also expressly prohibit attempts and conspiracies to accomplish the above.

The statute therefore makes illegal what was once only considered an unethical business practice. Penalties under this statute include incarceration, substantial fines, and forfeiture of business assets. That is, the United States may seek the forfeiture of all proceeds from any violation of the statute and any property used to facilitate the violation (18 USC §1834).

The EEA also contains provisions that strengthen its enforceability. It is not, for example, confined in application to activity occurring within the U.S. borders. The statute can be enforced against 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

<sup>4</sup>CSO Magazine, Snooping, by Hook or by Crook, Sarah D. Scalet, May 2003

(2) an act in furtherance of the offense was committed in the United States” (18 USC §1837).

If the government cannot establish that a party acted, attempted, or conspired to violate one of the prohibited acts to the benefit of a foreign government, instrumentality, or agent, which would violate section 1831, the defendant can still be found to have violated section 1832 if it can be established that (a) the defendant intended to convert a trade secret for the economic benefit of anyone other than its owner; (b) the defendant knew or intended that the owner of the trade secret would be injured; and (c) the trade secret was related to or included in a product produced or placed in interstate or foreign commerce. The Avery Dennison case is a good example:

### **The Avery Dennison Case**

**Profile:** Avery Dennison (AD) is a global leader in adhesives technology and manufacturer of adhesive products such as postage stamps and diaper tape. AD has over 16,000 employees worldwide.

**Predication:** AD was informed by a Four Pillars employee (a competitive organization) that an insider at AD was being paid in exchange for trade secret information. An internal investigation identified Tenhong Lee as the “mole” and the case was referred to the FBI.

**The Recruitment:** Lee went to Taiwan to visit family and made a presentation at a Taiwanese technology convention. Was introduced to Pin-Yen Yang, president of AD competitor Four Pillars, and was recruited as a “consultant” for \$25,000 per year. Lee provided trade secret information from 1989 through 1997 and was paid approximately \$160,000.

**The Defendants:** Tenhong “Victor” Lee, PhD., of Taiwanese descent, earned three postgraduate degrees in the U.S. He was hired as Senior Research Engineer by AD in 1986. He specialized in pressure-sensitive materials and emulsion silicon technology, becoming a world-renowned authority in rheology (the measurement and science of how well labels stick to, and peel off of, a variety of surfaces). He was a rising star at the company’s Concord, Ohio, research facility for 11 years.

*Pin-Yen Yang*, president, Four Pillars. Yang had a shady background in counterfeiting.

*Hwei Chin (Sally) Yang*, daughter of Pin-Yen, was the Director of R&D for Four Pillars. Sally holds U.S. citizenship.

**The Investigation:** An FBI sting was initiated with the intention of catching Lee in the act. A trap was set and Lee was caught on video going for the bait. He wore gloves to insure his fingerprints did not appear on any of the trade secret documents he handled. Lee thought he was stealing a confidential Southeast Asia business plan. The FBI confronted Lee who confessed to the trade secret thefts and agreed to cooperate in the investigation.

Pin-Yen and Hwei Chin Yang came to the U.S. and met Lee, who was wired for audio and video, at a hotel. Lee presented Avery documents that were reviewed and acknowledged as “confidential.” They were observed removing Avery logos and placing them in his briefcase.

**Foreign sponsorship:** Inasmuch as there was no evidence that the Taiwanese government directed or coordinated the espionage activity, section 1832—theft of a trade secret was correctly charged in the case.

**Arrests:** On September 4, 1997 at Cleveland Hopkins airport, the Yangs were arrested and the trade secret documents were recovered.

**Indictment:** October 1, 1997, 21-count indictment including mail fraud, wire fraud, money laundering, receiving stolen property, and attempted theft of a trade secret.

**Value:** 12,000 R&D documents, 71 adhesive formulas, 37 adhesive tapes, and 20 label primers that are valued at \$60 million.

**Disposition:** Pin-Yen Yang and Hwei Chin Yang were convicted of stealing trade secrets from AD. A \$5 million fine was levied against Four Pillars.

**Case status:** Department of Justice and Defense appeals pending

## Fraud

EEA prohibits the theft of trade secrets by fraud. Therefore, if an information collector obtains trade secret information from an employee through a false representation of identity and purpose, and such representation misleads the employee to believe that the recipient has legitimate access and authorization by company policy to use the information, that person may be liable under the law and subject to prosecution. An intelligence-gathering mission of the Schwan's corporation sheds light on this aspect:

### Schwan's vs. Kraft

Schwan's Food Company learned that Kraft Food was planning a major marketing campaign to position its new DiGiorno frozen pizza as the only frozen pizza with a fresh-out-of-the-oven pizza-parlor taste. Schwan's knew the secret of the "rising crust," but needed to know how fast Kraft planned to roll out the product nationwide in order to develop a counterstrategy.

To do this, they needed to know the location and capacity of its plant, type of equipment, number of production lines, sizes and types of pizzas, and the number of pizzas produced on the assembly line each day.

Schwan's retained the services of a competitive intelligence professional to answer these questions. Due to a stringent deadline, the work was sub-contracted to a third party or "kite" that would do what was necessary to get the job done, without implicating Schwan. The kite obtained the information in 36 hours by posing as a reporter for the *Wall Street Journal*, an environmentalist writing an article for *EcoNews* on fluoro-hydrocarbon emissions from a Kraft plant, a student conducting research for a term paper, the president of a corrugated box company, and an employee of Kraft.

The kite posed as an employee of the purchasing department of Kraft's Tombstone pizza plant and said he needed to reconcile a discrepancy in paperwork. This fraudulent representation opened the door to a series of actions that enabled him to obtain trade secret information from an employee who released the information in the belief that the collector was authorized to access the information. In this scenario, the conduct of the kite bordered on criminal, and although he was not prosecuted, he used a fraudulent tactic that falls under the purview of the Economic Espionage Act of 1996.

## Destruction

There are increasing reports in the media of employees conducting intentional and malicious acts of destruction against employers.

Disgruntlement on the job has prompted some employees to access the company's computer network and delete sensitive and proprietary files for the purpose of injuring the company's ability to compete. In some instances, employees have gone so far as to disclose a company's trade secrets by placing them on the Internet for public consumption. The EEA prohibits the destruction of trade secret information, as revealed in the Cleveland Clinic indictment, which alleged the defendants destroyed DNA reagents used in highly competitive research projects with the intent of impeding the clinic's ability to continue its research.

### The Cleveland Clinic Case

**Profile:** The Cleveland Clinic Foundation (CCF) is a leading nonprofit medical and research institution located in Cleveland, Ohio. The Lerner Research Institute (LRI) conducts leading-edge medical research.

**Predication:** In July 1999, LRI researchers determined that critical DNA and cell line research materials were missing from the laboratory. The lab was shut down pending an internal inquiry and shortly thereafter referred to the FBI when criminal activity was suspected.

**Defendants:** Takashi Okamoto, lead scientist at LRI, was conducting promising research into the cause of and cure for Alzheimer's disease. Okamoto had a staff of five postdoc scientists under him. Okamoto returned to Japan days after the lab was shut down.

**The Investigation:** An investigation determined that Takashi Okamoto accepted employment at Riken Brain Science Institute (a competitive organization) outside Tokyo, Japan, to continue the research projects stolen from the CCF. FBI search warrants were executed in Cleveland and Kansas City, producing evidence of the espionage activity. Japanese authorities conducted an internal investigation and Okamoto suddenly resigned from Riken.

Hiroaki Serizawa, a friend of Okamoto and research scientist at Kansas University Medical Center (KUMC), assisted Okamoto by storing CCF research materials in his laboratory until Okamoto retrieved

them and transported them to Japan. Serizawa pled guilty to lying to an FBI agent.

**Trade Secrets:** Specific Alzheimer’s disease research projects combined with DNA reagents were affirmed as trade secrets by U.S. District Court for the Northern District of Ohio. The DNA reagents were novel in design and exclusively constructed to support experimentation. Until such a time as the results of scientific research are published for the benefit of the scientific community, projects and DNA reagents may be protected as trade secrets.

**Foreign sponsorship:** Riken was a government sponsored research facility. Under the EEA, foreign sponsorship does not require evidence that the government directed or coordinated the espionage activity, so the 1831 offense was charged. Okamoto was considered an agent of a foreign government that stood to benefit from the theft. According to the statute, the prosecution must only prove the agent intended for the foreign government to benefit. There was no evidence supporting the active participation of the Japanese government.

**Indictment:** Defendants were indicted for economic espionage (section 1831) in connection with the theft of Alzheimer’s disease research projects and trade secret DNA reagents uniquely designed to conduct the research. The indictment alleged that Okamoto stole the DNA from the CCF and arranged delivery to his new employer’s research laboratory—Riken Brain Science Institute.

**Destruction:** In addition to the theft of DNA reagents, Okamoto allegedly destroyed samples left behind at the CCF. Prosecutors believed that acts of destruction were intended to hinder the progress of the CCF research in this highly competitive field.

**Value:** \$2.5 million. The loss of the trade secrets ended Alzheimer’s disease research at CCF, which was considered a promising avenue of research that could have eventually produced pharmaceutical therapies to prevent or control the effects of Alzheimer’s disease. The monetary value of such therapies would be in the billions—not to mention the adverse impact caused to those afflicted with Alzheimer’s disease and their families.

**Case status:** Four years after the crime, extradition proceedings are continuing with the Japanese Ministry of Justice for the return of Okamoto to the U.S. for prosecution.

It is important to note that the EEA does not prohibit legitimate means of obtaining the information and was not intended to deny employees the use of general knowledge, skills, and experience derived from their tenure with a particular company. Rather the act was designed to punish the theft or misappropriation of a trade secret.

### **Reasonable measures—a prescription of what must be done**

Because trade secrets derive value from the fact that they are generally unknown in the public domain or industry with which they are associated, it is the responsibility of the owner or company to document, manage, and protect them. Unfortunately, many companies do not take this responsibility seriously, and trade secrets merely exist within the company—undocumented, un-leveraged, and unprotected under the law. Consequently, company know-how and innovative methodologies are lost, stolen, or dissipated into thin air.

*“More opportunity is lost and liabilities incurred because people don’t pay enough attention to the art of documenting invention. It is the ability to enable and document invention, including never losing sight of the constantly evolving requirements of IP [Intellectual Property], that creates the envelope of protection.”<sup>5</sup>*

While the EEA was drafted to protect a wide range of business and technical information of economic value, it still requires the trade secret owner take reasonable measures to keep such information secret. What constitutes reasonable measures is fact-driven and case-specific, depending upon the nature, value, and importance of the information, as well as the size, ability, and sophistication of the owner. Reasonable measures by Microsoft to protect the latest version of its operating system would presumably involve far greater measures than those taken by a small, start-up software development company.

Nonetheless, reasonable measures to protect a trade secret should, at the very least, include the following:

---

<sup>5</sup> Julie L. Davis, Suzanne S. Harrison; “Edison in the Boardroom”, John Wiley and Sons, Inc., 2001, p. 27.

- Nondisclosure agreements with employees, licensees, vendors, consultants, customers, and contractors.
- Employee education, training, and documentation of nondisclosure obligations.
- Access controls, including physical security, visitor identification and escort, and restricting access to sensitive areas.
- Computer security, including the use of passwords, encrypted data for extra-sensitive information, Internet firewalls, and security banners.
- Policy and practice for document creation, retention, and destruction.
- Secret/confidential markings on storage facilities, rooms, and file cabinets.

Corporate leaders must understand the law and institute awareness training at all employee levels of the company in order to be afforded protection under the EEA. Such training would educate employees on the company's intellectual asset management model and convey a clear understanding of the types of information that contributes to competitive advantage. Uninformed employees are highly vulnerable and put a company's best interest at risk.

## Taking action

### Categorizing of information

There are two categories of information recognized under the law: information in the public domain and information that constitutes intellectual property. The first category, public information, is information that is unprotected and available for public use without restriction. Ownership rights do not exist. It is also referred to as open source information.

Information that constitutes intellectual property includes patents, copyrights, trademarks, and trade secret information. Unlike public information, the owner of this type of information may obtain protection under the law. For example, an inventor must disclose details of the invention to the U.S. Patent Office or comparable government office in foreign countries in a formal application process to gain protection. Upon review of the application, the government patent authority grants or denies a certificate. If a certificate is issued, the invention is

protected for a specified period of time prescribed by law.

With regard to trade secret information, there is no government interface through which the invention is identified and disclosed in an application process. Therefore, this type of information tends to be under-managed and vulnerable. State and federal law does, however, provide protection for trade secret information provided the information meets the definition of a trade secret, and the owner has protected it as a secret.

### Recognizing trade secrets

Many companies have observed that the rapid pace of technology has reduced the life cycle of an invention. This factor, combined with the realization that an invention is publicly disclosed in the patent process at considerable cost, is causing many companies to choose trade secret protection over patent protection.

However, some companies do not understand that business information compilations and databases within the company that add to competitive advantage may be protected as trade secrets, provided they are captured as such and reasonable measures have been taken to protect them. This often proves difficult because organizations may not even recognize that information they possess can be classified as a trade secret under the law. For instance, a customer list containing details about sales preferences, practices, and activities that have been compiled over a period of time has competitive value to the company. Other examples include computer databases, supplier lists, and compilations of technical information.

Through the process of trial and error, a company may also learn what doesn't work. This knowledge, called negative know-how, can also be protected as a trade secret because it can help a company maintain competitive advantage.

### Trade secret management

For many companies, little attention is paid to trade secret management practices and policies until a problem occurs. At that point, a law firm must be retained to initiate a comprehensive trade secret audit to document the origin and existence of trade secrets, establish value, document how they were handled and protected, who had access to them and what employee agreements have been executed. Supporting documentation must be collected and

compiled in support of legal proceedings. These public proceedings may also prove detrimental because additional trade secrets can be lost through exposure in court litigation, as well as the negative impact through public exposure.

Fortunately, there are ways to prevent these types of situations. Through effective trade secret identification, protection and management, companies can greatly reduce the risk of information theft and loss.

Once trade secrets have been identified and protected, they must be managed so companies can use them to extract greater value and profitability. This is an extremely important task—especially considering the Gartner Group found that 80% of a company's useful knowledge is unstructured and may be found on desktops, filing cabinets, personal e-mails, and internal documents.<sup>6</sup> Additionally, much of a company's experience, know-how, skills, and creativity reside in the heads of employees, which makes it difficult to leverage for profitability. A company cannot gain competitive advantage from this type of information if it is not recorded and captured by the company. Proper management of the intellectual property and trade secrets, therefore, allows the company to extract value from them.

A secondary benefit of effective trade secret management is that it protects competitive advantage and reduces the risk of espionage. Bear in mind that this secondary objective is not legal protection to win in a court of law, but rather legal protection that prevents espionage and averts the need to enter a court of law. After all, there is no guarantee that a company's losses can be recouped through civil or criminal proceedings.

A formalized trade secret management system allows for contemporaneous management of intellectual assets, including the classification, de-classification, archiving, and destruction of trade secret information. After all, what is valuable today may be of little value tomorrow and some trade secrets may need protection for short periods of time, while others need protection permanently. Every organization is different and therefore requires a unique trade secret strategy, but the following outlines some common objectives of trade secret management and protection programs:

## **Next steps: trade secret protection**

**Adaptation of a new security culture and mentality**—Instilling a sense of trust and loyalty in the workplace galvanizes security practices in the enterprise. Global change requires the integration of security concepts and application to empower all employees to play a part in the trade secret management process. Reasonable security measures must reflect a balance of solutions involving people, process, and technology. A team must be set up to take the lead, headed by an executive with authority.

**Implementation of a trade secret identification and management system**—A company's practice in identifying, managing, and protecting trade secrets must be consistently applied within the organization's goals and objectives. The plan must be documented and enforced—anything less does not exceed good intentions.

**Utilization of technology**—A good information security strategy will have a balance of prevention, detection, and response. Perimeter security measures must be enhanced by technologies that detect suspicious activities within the enterprise by persons with access.

**Education and employee awareness**—Employees must be informed as to the nature and threat of economic espionage. Training informs employees as to the motivation, tactics, effects, and cost of espionage to the company (monetary and competitive advantage loss) and to individuals (loss of jobs). Employees must understand the protocols of interacting with non-employees such as contractors, vendors, consultants, contractors, and temporary employees in order to protect trade secrets and confidential information.

**Understand the Law**—The Economic Espionage Act of 1996 was enacted by Congress to provide corporations with a road map from which they can manage their trade secrets. Knowing what companies must and must not do helps with the decisions of day-to-day operations. Knowing, following, and working within the law is the best way to ensure trade secrets are protected from theft or loss.

---

<sup>6</sup> The Gartner Group (Get cite)

**Author: Dave Drab**

The Federal Bureau of Investigation has exclusive jurisdiction in investigating crimes of economic espionage. Dave Drab is a 32-year law enforcement veteran. During his 27 years at the FBI, he specialized in the investigation of organized crime and economic espionage.

Xerox Global Services helps companies streamline and digitize their document-intensive business processes—everyday processes like customer communications, billing, training, or records management. Our people work closely with clients to identify, quantify, and realize hidden opportunities to save money, find new sources of value, and simplify how work gets done.

For more information on how Xerox Global Services can apply Six Sigma methodologies in your organization, call 1-800-ASK-XEROX ext. XGS or visit [www.xerox.com/contactglobalservices](http://www.xerox.com/contactglobalservices).