Running Head: CI, TRADE SECRETS, AND THE ECONOMIC ESPIONAGE ACT

Competitive Intelligence, Trade Secrets, and the Economic Espionage Act of 1996

Michael Stoler

San José State University School of Library and Information Science

LIBR 287 – Summer, 2006

Amelia Kassel

Abstract

Trade secret law should be of great concern to competitive intelligence practitioners. This paper examines traditional law governing trade secrets, and the 1996 law to govern them at the Federal level, the Economic Espionage Act. The effect of both sets of laws on the profession of CI is described, and recommendations are made to CI practitioners in light of the laws.

In any line of work, it is crucial to understand any laws governing it. This applies in every occupation, from fast-food servers, who are required to observe certain sanitary precautions, to physicians, who need to be aware of what constitutes malpractice. Competitive intelligence practitioners are no different. They are engaged in finding out information about companies on behalf of those companies' competitors, and it is very possible that the companies do not want that information widely known. Because of this, they may have sought to protect it as a trade secret, or, once it has passed to their competitors, claim that it represents a trade secret, which the competitor has no right to make use of, or even know, and the obtaining of which constitutes a civil or even criminal violation on the part of the competitor, or the hired competitive intelligence professional. In this paper, I will discuss the law governing trade secrets, and how it applies to competitive intelligence gatherers. There are three main ideas to understand:

1. Trade secrets have traditionally been governed by state law and common law, as a tort, or civil wrong against a company, for which damages were to be paid;

2. The passage of the Economic Espionage Act of 1996 federalized and criminalized trade secret violations;

3. While those who engage in more "adventurous" forms of competitive intelligence may find themselves at risk of suits or prosecutions under trade secrets laws, those who abide by a code of ethics, such as that of the Society of Competitive Intelligence Professionals, have little to worry about.

Traditional Notions of Trade Secrets

Unlike other forms of intellectual property such as trademarks, copyrights, and patents, which are generally governed by federal law, and require (or recommend, in the case of copyrights), public registration, trade secrets have been governed by accumulated case law and state law, and by their very nature, are not subject to public registration. They are thus somewhat harder to define. The case law on trade secrets was summarized in the legal encyclopedia Restatement of Torts in 1939. In 1979, a group called the National Conference of Commissioners on Uniform State Law, which writes "uniform" laws which it suggests to state legislatures and which many of them adopt, drafted and submitted the Uniform Trade Secrets Act to the states, and over 40 have adopted it, though sometimes with modifications. The UTSA was in most respects identical to the common law as expressed in the Restatement, and the more recent version of the Restatement has takes into account the UTSA, so the descriptions are pretty much interchangeable.

The definition of a trade secret in the Restatement runs thus: "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." (Restatement, Section 39) The key ideas are 1. information, 2. used in business or other enterprise, 3. of value, and 4. secret.

Let us look at each of these requirements. A trade secret can be any sort of information; as the Restatement puts it, "A formula, pattern, compilation of data, computer program, device, method, technique, process, or other form or embodiment of economically valuable information … [it] can also relate to other aspects of business operations such as pricing and marketing

techniques or the identity and requirements of customers." This is important, because while formulae and methods, for example, can be patented, and computer programs copyrighted, for such information as customer lists and business moves such as acquisitions, only trade secret protection is available. An important type of trade secret that is not protectable any other way is customer lists and other information. This was confirmed by the case *Aloi Electric Service v. ASAP Fire Equipment*, 1996 Conn. Super. LEXIS 1564 (Superior CT., June 18, 1996)

The information must be specific and capable of precise definition. Vague notions, or ideas, are harder to protect, partly because it is easier to come up with them independently, and partly because it is harder to prove to a court that the competitor obtained this particular information.

The information can be used "by businesses and other commercial enterprises, nonprofit entities such as charitable, educational, governmental, fraternal, and religious organizations … such as [for] lists of prospective members or donors." (Restatement, Section 39) (We will see below that the Church of Scientology has been quite aggressive in protecting its "trade secrets", which others might think of as religious scripture.)

The requirement that the information be of value means that it must give the owning company a competitive advantage over other companies which is lost if the information is divulged. The owning company need not actually be using the information; it might be in development, or represent something the company has learned NOT to do. And the advantage need not be monetary; courts have recognized that the Church of Scientology's trade secrets convey a "spiritual advantage." (*Religious Technology Center v. Netcom On-line Communications Services, Inc.,* 907 F. Supp. 1361 (N.D. Calif. 1995).

Finally, the information must really be secret. Something that is generally known, or readily discoverable independently, for instance, a mathematical model, cannot be protected. (*Ashland Management v. Janien*, 82 N.Y.2d 395 (1993)) Neither can an idea which has been proposed to a municipality and been made public under state law. (*Jensen v. Sandy City Redevelopment Agency,* 998 F.2d 1550 (1993)) A customer list cannot be protected if it is obvious, given the business a company is in, who its customers would be, or if they can be readily inferred, as the advertising customers of a publication can be by anyone reading it. (*Leo Publications, Inc. v. Reid*, 458 S.E. 2d 651 (Sup. Ct. Ga.1995). In the version of the UTSA adopted by the California Legislature (Civil Code, Section 3426), the provision that the trade secret not be readily ascertainable is somewhat weakened; fairly obvious information can be protected if no one else has actually figured it out and used it yet. And just how much effort a competitor must put into learning the information, say, by reverse engineering from a legally purchased product, is subject to debate.

Once something has been exposed, has entered the public domain, by fair means or foul, it can no longer be protected as a trade secret, although the original owner can still seek damages for the loss of secrecy and unique control. Thus, for instance, information that has been published on the Internet loses its trade secret status. The person who actually put it up there can be liable for misappropriation, but not anyone who subsequently uses or publishes it. This was established by a series of cases involving the Church of Scientology: in *Religious Technology Center* [another name used by the Church] *v. Lerma*, 897 F.Supp. 260 (E.D.VA.,1995), the court ruled that the Washington Post could not be prevented from publishing documents about the Church that had been posted online, though the person who posted them could be held liable for

damages. A Colorado District Court made a similar ruling in *Religious Technology Center v. F.A.C.T.NET, Inc.,* 901 F.Supp. 1519 (D. Colo.,1995), and a California one in *RTC v. Netcom.*

Furthermore, the owning company must work to maintain the secrecy of the information, to prevent its disclosure to competitors. This does not mean that it cannot be disclosed to anyone, such as a customer, provided that third party is also willing to maintain its secrecy. But the owning company must, for instance, take steps to guard the physical security of the information, such as by putting it in a safe or a secure computer; informing its employees that the information is to be kept secret, and marking it as such; and restricting it to those who need to know it. The measures taken must be "reasonable", so that obtaining the information requires unusual or unforeseeable, though not necessarily illegal, means. For instance, in a case that has great resonance for CI practitioners, chemical maker Du Pont was able successfully to sue a pair of brothers who, on behalf of a competitor, had rented a plane, and flown over and photographed a Du Pont factory that was under construction. They argued that they had flown in public airspace and had broken no trespassing laws, but Du Pont was able to argue that it had taken reasonable measures to protect its trade secrets, since it could not anticipate that its competitors would resort to such extraordinary means to learn about it. (*E. I. DuPont deNemours & Company, Inc. v. Rolfe Christopher et al.* 431 F.2d 1012 (5th Cir. 1970)).On the other hand, courts have ruled that if a company puts confidential documents in a publicly accessible Dumpster, its competitors can legally dive in and obtain them, because the company has not taken reasonable precautions for handling them (shredding, or keeping them on its own site until a disposal company picks them up. (Fitzpatrick, 2003))

Trade secret protection is not designed to give an exclusive right to, say, a process, the way a patent does. Whereas a patent would give the first person to register an invention all rights

to it, even if someone else developed it as well, trade secret laws allow anyone who discovers useful information to use it. It is permissible, even encouraged, to reverse engineer from a competitor's product, or to draw conclusions from an analysis of published materials or through observation of publicly accessible objects or events. What trade secret law is designed to prevent is unfair competition, waiting for someone else to develop useful information and then swooping in and stealing it. The law of trade secrets is not so much about property as about conduct, about the *means* by which information is obtained. The owner of a trade secret must make a good faith effort to protect it, but if someone else acquires it through his own smarts or the honest sweat of his own brow, rather than theft, fraud, or the unauthorized interception of communications, that's OK, in fact, laudable. The idea, as the Restatement explains, is to encourage innovation by securing to inventors the ability to profit from their work, and improving the workings of businesses by allowing them to spread information throughout their organizations to various employees with the confidence that those employees will not exploit it themselves or sell it.

To prove "misappropriation" of trade secrets, the plaintiff must show that the information was a properly constituted secret, and that the defendant knew or should have known that it was, so that it used "improper means" to obtain it, or that the person from whom he obtained it used improper means. Thus, if a competitor comes into possession of information which has been accidentally disclosed but that a reasonable person could tell was meant to be a secret, and then takes advantage of it, he can be liable for misappropriation. As to what it means to "use" misappropriated information, the Restatement gives several examples: "Any exploitation of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant … marketing goods that embody the trade secret, employing the trade secret in manufacturing or production, relying on the trade secret to assist or accelerate research or

development, or soliciting customers through the use of information that is a trade secret**."** (Restatement, Section 40)

People to whom trade secrets are disclosed have a duty to keep them in confidence if they make an express promise to do so, or if from the circumstances of disclosure, they had reason to infer that it was intended to be kept in confidence, or the discloser had a good reason to believe they understood that it was. Employees are generally held to have this duty towards their employers, and former employees to have it as well if they have signed an agreement to that effect. Inducing someone who is bound such a duty of confidence to violate it constitutes misappropriation in itself. (*Bryan v. Kershaw*, 366 F.2d 497 (5th Cir.1966))

A company that believes its secrets have been misappropriated has two remedies. If the material has not been widely circulated yet, the company can seek injunctive relief, a court order that the appropriator not reveal the information. However, once the cat is out of the bag, the company can only seek damages to compensate it for its loss of value in its secret.

The Economic Espionage Act of 1996

Before 1996, misappropriation of trade secrets had sometimes been prosecuted under Federal laws against transporting stolen property, but this could only work when the secrets were in some physical form that had been stolen (such as a book or a computer disk); it could not protect the information itself. Also used were wire and mail fraud statutes, but these did not apply in cases involving face-to-face meetings. But the impetus for Federal protection of trade secrets did not come from these sources, but rather, foreign ones. In the speeches by House and Senate sponsors of the bill, such as Rep. Charles Schumer (D-NY), Sen. Herb Kohl (D-Wisc.),

and Sen. Arlen Specter (R-Pa.), and the articles they had inserted into the Congressional Record, this is the constant theme: with the end of the Cold War, foreign countries, both former adversaries and heretofore allies, were no longer interested in our military secrets, and had turned their freed-up attention instead to our economic ones, causing billions in losses to American companies. (Congressional Record, October 2, 1996; Congressional Record, September 28, 1996), the Economic Espionage Act of 1996 was passed in the House by a vote of 399 to 3, and unanimously in the Senate; it was signed by the President and became law on October 11.

The provisions of the law (Public Law 104-294, United States Code 18, Sections 1831 ff.) are as follows: Trade secrets were defined (Section 1839) as "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." This is a somewhat broader definition than the common law and UTSA practice, including more technological and intangible material. (Dilworth, 2005)

Section 1831 provided for fines of up to $500,000 (for individuals; up to 10 million for organizations) and prison sentences of up to 15 years for anyone who "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; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of the conspiracy." It was now a Federal crime, not a civil tort, to obtain trade secrets improperly, to get them from someone who had, or even to try or conspire to – if one were working for a foreign government, a business substantially controlled by a foreign government. (Section 1839, Definitions).

Section 1832 applied domestically: to undertake any of the actions in Section 1831 for any trade secret "related to or included in a product that is produced for or placed in interstate or foreign commerce [since only those areas can be regulated by Congress], 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" could get a person up to ten years in prison. A further provision, Section 1837, made 1831 and 1832 applicable to conduct occurring outside the U.S. by U.S. citizens and businesses, or furthered by activity inside the U.S.

Some business leaders feared this measure might unduly restrict competition, giving too much protection to holders of trade secrets, a worry which Schumer, for instance, tried to address in his address on the bill. "First, some Members thought that this legislation might inhibit common and acceptable business practices … Our bill was carefully drafted to avoid this problem. The very high intent requirements and the narrow definition of a trade secret make it clear that we are talking about extraordinary theft, not mere competition." (Congressional

Record, September 28, 1996) The Attorney General of the United States, Janet Reno, promised in a letter to Congress that for five years after the passage of the Act, no prosecution would be undertaken under it except with the express authorization of the A.G. or her deputy. And in fact, there have been relatively few prosecutions under the EEA, only a few dozen by 2003 (and by then, the Justice Department had other priorities, such as terrorism.) However, despite the apparent legislative intent directed at foreign espionage, most of the prosecutions were under Section 1832 rather than 1831. The EEA has a high standard of proof. "Prosecutors must prove beyond a reasonable doubt that a defendant intended to personally benefit from the theft, and knew of the harm to the owner." (Kaltenheuser, 2003) Often prosecutors resort to the using the same laws, such as those for stolen property and fraud, which they used before the EEA.

Competitive Intelligence and the Law

The question is, how does all this law affect CI practitioners? Under common law and the UTSA, the CI community had certain things to look out for. Many of the types of information valuable in CI, such as the future plans of a business or the identities of its customers, are clearly trade secrets – if they are protected as such. Trade secret law, remember, governs conduct, not the information itself. As long as a CI practitioner sticks to "proper means", especially by analyzing publicly available information, he or she is probably safe. Since the owner of the trade secret is obligated to take measures to protect it, if he or she hasn't, again, the CIer is probably safe; the clearest indication of whether or not the target company has done this is, somewhat circularly, whether the CIer can obtain the information by proper means, although, remembering Du Pont v. Christopher, not all legal means are proper means. Even if the information was kept

secret, if it has become public through some means unconnected to the CIer, he or she has the right to use it. If it's on the Internet, for instance, it's fair game, as long as it was not the CIer who convinced someone to put it there. The CI practitioner must be aware that an inside source at a company is bound by a duty of confidence to his or her employer if the employer has made it clear that certain information is regarded as a trade secret, and aware as well that a former employee of a company may be bound by a non-disclosure agreement not to tell what he or she knows.

Other pre-EEA laws and practices also affected the activities of CI professionals. Many companies must file reports with the EPA or other government agencies, from which much about their business activities could be learned or inferred. Other companies reveal their secrets in applications for government contracts. In theory, these are public documents, obtainable by simple request, or through the Freedom of Information Act (FOIA). However, several court rulings have affirmed the duty of the government to protect such information from release (although once it has been released, for whatever reason, it loses its protection.) The FOIA contains a specific exception for trade secrets. (5 United States Code, Section 552(b)(4)) The 1988 Trade Secrets Act (18 United States Code, Section 1905) forbids any government employee from disclosing information in a way not authorized by law (of course, certain kinds of information release, such as some EPA material, is authorized to be disclosed. (*RSR Corp. v. Browner*, 924 F.Supp. 504 (S.D. N.Y., 1996).) Legal filings and discovery can also be an important source of information for competitive intelligence researchers. Under state law, and the EEA, however, companies can ask that documents be kept under seal, in order to maintain their trade secrets.

Under the EEA, there are more dangers to steer clear of. Although the same rules about proper means still apply and give some measure of safety, a CI professional should also be sure he or she knows something about the ownership of his client, whether it is in some way linked to a foreign government. This may not be so obvious; many companies in China, for instance, are partly owned by the armed forces or other government agencies, and in fact, in an authoritarian system like that, almost any company could be argued to be under government control. But then, many energy and aviation or defense businesses in Europe and Latin America are also partly or entirely government owned. Even some American companies are subject to foreign ownership, either directly or through parent companies that fall into the categories described above. In a time when the U.S. government is particularly worried about foreign influence, careful CIers might want to avoid such clients. Since a CI person is paid for his work (unlike, say, an investigative journalist who may just want to put information before the public), he, and not just his employer, derives economic benefit himself for obtaining it.

In his 2003 article, William Fitzpatrick distinguishes between "basic" and "creative" CI methodologies. "Basic" methodologies "consist primarily of archival and published works, government documents, on-line competitive databases, and on-the-record interviews with corporate personnel or industry experts." "Creative" methodologies "strain the legal and ethical limits of professional conduct." They include direct observation of the target company, which can include going through their trash or taking tours of their facilities, as Apple did at Xerox PARC to learn the secrets of the mouse-activated graphical user interface. These actually can be legal if no trespassing was involved and if the target company did not take reasonable measures to protect itself. Another "creative" method involves interview techniques, or going after current or former employees of the company, who may have an obligation of confidence, using pretexts

to get them to talk, or preying on their weaknesses (having an attractive woman chat up a sexually desperate computer nerd in a bar at a convention, for example.) According to Fitzpatrick, basic methodologies pose no danger of running afoul of trade secrets laws, but "creative" strategies can get iffy.

Two years after the passage of the EEA, SCIP published a statement and a white paper discussing its effects on the CI profession. (Horowitz, 1999) It concluded that there basically were not any, since conduct banned by the EEA was already illegal under state laws, and against the SCIP code of ethics. "In other words, the rules are fundamentally the same but the consequences of violating them are different." It quotes attorney Mark Halligan as saying "the EEA does not materially affect competitive intelligence activities and companies should not curtail competitive intelligence activities based on a 'misplaced fear' of the EEA." Rather than talking of "basic" and "creative" CI methods, the SCIP document discusses "gray zones", such as "such as finding a lost document in the street, overhearing competitors talk about a plan, having a drink with a competitor knowing you are better at holding your liquor, removing your name tag at a trade show, or even falsely identifying yourself as a student" which (although inconsistent with the SCIP Code of Ethics) are situations that alone will not trigger trade secret liability. This is where the Code is particularly useful. It is there not just to ease the consciences of CI practitioners, but actually serves as a guide to how to avoid legal entanglements.

References

142 Congressional Record 12201, October 2, 1996. Retrieved through Lexis-Nexis database.

142 Congressional Record 12137, September 28, 1996. Retrieved through Lexis-Nexis database.

Bouchoux, D. (2000). Intellectual property: The law of trademarks, copyrights, patents, and trade secrets. Albany, New York: West/ Thomson Learning.

Dilworth, Toby. (2005). The Economic Espionage Act of 1996: An overview. Retrieved on August 7, 2006, from http://www.justice.gov/criminal/cybercrime/usamay2001_6.htm

Fitzpatrick, W. (2003, Summer). Uncovering trade secrets: The legal and ethical conundrum of creative competitive intelligence. *Advanced Management Journal*, 68, 4-13. Retrieved through WilsonWeb database.

Halligan, R. (2006) The trade secrets home page. Retrieved August 7, 2006, from http://mhallign.fp.execpc.com/

Horowitz, R. (1999). Competitive intelligence and the Economic Espionage Act: A policy analysis adopted by the SCIP Board of Directors and written by Richard Horowitz, Esq., with letters of endorsement. Retrieved on August 7, 2006, from http://www.scip.org/Library/white.pdf

Kaltenheuser, S. (2003, July-August). Stealing trade secrets: will U.S. crack down? *Financial Executive*, 19, 25. Retrieved through WilsonWeb database.

Lam, M. (2004, July). Stop giving away your secrets. *Pharmaceutical Executive*, 24, 42-50. Retrieved through WilsonWeb database.

Restatement of the Law, Third, Unfair Competition. (1995). Retrieved through Lexis-Nexis database.

.