



Technology & Intellectual Property *Legal Trends*

Third Quarter 2006

Protecting Your Business Advantage

By Kevin Oliveira

Your Trade Secrets in Business and Customer Information and Research and Development.

Recently, it was reported that some of the world's most valuable trade secrets were offered to Coca-Cola Co.'s principal competitor by the company's own employees. These employees had been given access to the information as part of their job to benefit the marketplace advantage the company has as the largest manufacturer, distributor and marketer of nonalcoholic beverage concentrates and syrups in the world. Sources say that PepsiCo Inc. was approached with an offer to provide Coca-Cola's confidential business information, including information about new products, in exchange for millions of dollars. PepsiCo tipped Coca-Cola executives about the situation, and with the assistance of an undercover sting operation by the FBI, these offers were identified, and are now the subject of a criminal prosecution.

Internally, Coca-Cola has responded by reviewing security procedures, conducting information briefings and sending letters to the company's employees. In press statements, the Department of Justice has confirmed that commercial trade secret protection is a major issue. In addition, by using its resources, the DOJ confirms that protecting trade secrets is of national importance.

In a letter to employees, Neville Isdell, the chairman and CEO of Coca-Cola shared "While this breach of trust is difficult for all of us to accept, it underscores the responsibility we each have to be vigilant in protecting our trade secrets. Information is the lifeblood of the company."

Every year numerous lawsuits are filed by businesses alleging that their competitors are attempting to misappropriate trade secrets providing business advantages. While PepsiCo acted as a responsible competitor and informed Coca-Cola about being approached, companies can't be certain that all competitors will act as responsibly.

Trade secrets come in many forms, and providing for their protection generally fits within a common structure of laws in the United States. Most states have adopted a version of the Uniform Trade Secret Act. State legislatures have been fairly uniform in defining trade secrets to be information that is the subject of reasonable efforts to preserve confidentiality and that has value because it is not generally known in the trade. Such information can include pricing information, consumer information, prospects and lead information, know-how, formulae, processes, and confidential practices, methods, processes, designs, or other information that is not disclosed as public information. As confidential information used by a company to compete with other businesses, it is protected against those who gain access to it through improper methods or by a breach of confidence. Infringement of a trade secret is considered unfair competition.

There are two keys to protecting trade secrets: confidential treatment and the use of reasonable security procedures. Most companies implement basic protection such as locks, security access requirements, employee policies and confidentiality agreements. However, proper enforcement of these protections is often haphazard or ignored. Further, many companies fail to inform employees of applicable security requirements. Still other companies never have employees affirm their responsibilities by signing the appropriate confidentiality agreements.

The most important factors in determining whether information owned and used by the business is a trade secret are:

- the specific information itself

See *Trade Secrets* page 2...

Felony Spamming Conviction Affirmed

By Jonathan Frieden

In September, the Virginia Court of Appeals affirmed the conviction of Jeremy Jaynes of three counts of violating the unsolicited bulk electronic mail provisions of the Virginia Computer Crimes Act (the VCAA). Jaynes is the first person in the nation to be convicted of a felony for illegal spamming and was sentenced to nine years in prison.

At trial, prosecutors demonstrated that Jaynes had used computers in his North Carolina home to send over 10,000 unsolicited e-mails, on each of three days, to AOL subscribers. Among the evidence found in Jaynes' home were digital media containing 283 million e-mail addresses and the stolen personal and private account information for millions of AOL users. Jaynes was convicted under the VCAA, which prohibits the use of

"a computer or computer network with the intent to falsify or forge electronic transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers."

Because his e-mails were sent from his home in North Carolina, and he had no control over the path by which those e-mails reached the recipients, Jaynes argued that the VA trial court had no jurisdiction to convict him of a crime. In rejecting this argument, the Court noted that all of the e-mails at issue in the case were addressed to AOL users. "Thus," the Court held, "while the e-mails could have taken any number of pathways to reach the intended recipients, each pathway ended at AOL's servers [in Loudoun County]."

Jaynes also argued that the VCAA is unconstitutionally invalid because its language prohibits anonymous speech of a non-commercial nature, which is protected by the First Amendment. Though the Court

See *VCAA* page 2...



Trade Secrets continued...

- the extent to which the information is known outside the owner's business;
- the extent to which it is known by those involved in the owner's business;
- measures taken to guard the secrecy of the information;
- the value of the information to the owner or to his/her competitors; and
- the ease or difficulty with which the information could be properly obtained by others.

Identifying and protecting trade secrets should be a regular and ongoing process. Simply creating a trade secret policy in an employee manual does not create a continuing and valid trade secret right for the company. A company's trade secrets will regularly change as some information becomes obsolete and as new information is created. Throughout this dynamic process, companies must pay equal attention to what information should and is properly protected.

A reasonable starting point for the development of a trade secrets protection program is an intellectual property audit. The audit will identify the company's intellectual property, including its trade secrets, and pair it with protection methods that take into account the asset, the company's requirements and the company's budget. The audit should be done in conjunction with counsel so that, through the attorney-client privilege, the results of the audit can be protected from discovery by others.

On average, audits should be conducted annually to keep pace with the innovations in the corporate world and the ever-increasing pace of business. When completed, policies and procedures can then be initiated or modified, where necessary, to protect the information identified as trade secrets in the audit.

Kevin Oliveira is a principal with Odin, Feldman & Pittleman. He represents companies and individuals in a range of transactions including international and domestic marketing and distribution agreements, franchising, mergers and acquisitions, strategic alliances, joint ventures and intellectual property issues. He can be contacted at 703-218-2138 or Kevin.Oliveira@ofplaw.com.

Technology & Intellectual Property Legal Trends is a quarterly publication of Odin, Feldman & Pittleman, P.C. The information contained herein is provided for informational purposes only, and should not be construed as legal advice on any subject matter. No recipients of these materials should act or refrain from acting on the basis of any information contained herein without seeking appropriate legal advice.

VCAA continued...

noted that "the right to speak anonymously has a long and respected history in First Amendment jurisprudence," it held that Jaynes' First Amendment argument was meritless because the "VCCA proscribes no speech."

Jaynes also argued that the VCCA violates the Dormant Commerce Clause of the United States Constitution because it places an impermissible burden on interstate commerce. The court opined that the VCCA, and anti-spam laws generally, produce unquestionable local benefits and that the VCCA presented no significant burden on interstate commerce.

Finally, Jaynes argued that the VCCA is unconstitutionally vague. The appellate court held that, as applied to Jaynes' actions, the VCCA is not unconstitutionally vague in that it gives a person of "ordinary intelligence a reasonable opportunity to know" what conduct is prohibited.

Legally, the opinion of the Court is not surprising but the case is newsworthy because it is the first of its kind. Time will tell as to whether the nine-year prison sentence will deter other potential spammers.

Jonathan Frieden is a litigator and principal with Odin, Feldman & Pittleman. Mr. Frieden's practice encompasses intellectual property litigation, the defense of corporations against federal and state consumer claims, representation of management in employment discrimination claims, the resolution of commercial contract disputes and other complex commercial matters. He can be contacted at (703) 218-2125 or Jonathan.Frieden@ofplaw.com.

Odin Feldman Pittleman PC

9302 Lee Highway
Suite 1100
Fairfax, VA 22031
703-218-2100
703-218-2160 fax
www.ofplaw.com