DisputeSoft
Software Dispute Experts

Examining and Protecting Trade Secrets in IT Litigation

Jeff Parmet | Founder & Managing Partner
Tom Ashley | Manager

Many software products incorporate trade secrets – algorithms or arrangements of data deriving economic value due to their confidential nature.

Intellectual property disputes thus often involve allegations of trade secret misappropriation. In such disputes, software experts play a valuable role in assisting the finder of fact determine whether a plaintiff owns a valid trade secret and, if so, whether the secret has been misappropriated. The protection of secret information may also be a major concern to litigants in cases not involving allegations of trade secret misappropriation. When evaluating any intellectual property dispute, software experts must diligently protect proprietary information while analyzing the relevant factual questions. In this article, we discuss the issues a software expert must address when supporting litigation in which trade secrets are involved.

1. Overview of U.S. Trade Secret Law

The vast majority of states have adopted the Uniform Trade Secrets Act ("UTSA"), originally published in 1979 and amended in 1985.[1] The UTSA defines a trade secret as information that "(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[2]

Trade secrets may exist individually or in combination. A combination trade secret consists of elements that, although independently in the public domain, maintain economic value due to a secret method for combining them.[3] "Misappropriation" occurs when a trade secret is used or

"Misappropriation" occurs when a trade secret is used or disclosed, without the owner's consent, by a person who has acquired it through improper means.

disclosed, without the owner's consent, by a person who has acquired it through improper means.[4] Examples of improper means include theft, bribery, misrepresentation, espionage, or breach of a duty to maintain secrecy.[5]

Although trade secret law was historically a state matter, in recent years the Federal government had expanded its role in restricting trade secret misappropriation. In 1996, Congress passed the Economic Espionage Act, making trade secret misappropriation a federal crime.[6] Subsequently, the Defend Trade Secrets Act ("DTSA") of 2016 created a federal civil cause of action for the misappropriation of trade secrets related to interstate or foreign commerce.[7] The DTSA was heavily influenced by the Uniform Trade Secrets Act and contains similar provisions.[8]

2. Analytical Approaches in Trade Secret Disputes

In evaluating allegations of trade secret misappropriation, software experts have a variety of techniques at their disposal. They will often begin by examining the plaintiff's source code and related documentation to determine if the alleged trade practices are present. For instance, if a plaintiff has alleged misappropriation of a combination trade secret, the expert will examine the plaintiff's software to determine whether it contains every element of the combination. This can be verified by examining a running version of the plaintiff's software to determine whether all elements of the alleged combination are identifiable. If relevant, the expert may also review user manuals or training documentation to verify that the entire combination is present. If the investigation reveals that any element of the alleged combination is absent from the plaintiff's software, the expert will conclude that the plaintiff does not own a protectable combination.

After verifying that the plaintiff's product contains the alleged trade practices, the software expert will investigate whether the plaintiff made reasonable efforts to keep the practices confidential. If the plaintiff did not do so, the expert will conclude that the practices are not protectable as trade secrets. For example, if a software developer discloses information to testers without requiring them to sign a non-disclosure agreement, the expert will likely conclude that

trade secret status has been lost. Similarly, if a copyright filing or patent application discloses a trade practice, the expert will conclude that the practice is not a protectable secret. The expert may therefore review copyright deposit material to determine whether the trade practices were disclosed in non-redacted portions of the plaintiff's source code. Software experts may also review product documentation such as user manuals or training materials to determine if they depict relevant trade practices.

Another approach is to examine third-party materials to determine if an alleged trade secret had been publicized before the defendant's software was developed. For instance, a software expert may use the Internet Archive's "Wayback Machine" to search archived websites for product sheets, press releases, and white papers describing software with similar functionality.[9] If the archival material reveals that the plaintiff's trade practices were already well-known at the time of development, the expert will likely conclude that the practices are not protectable trade secrets. Similarly, the software expert may review relevant patents, patent applications, white papers, and articles to determine if the alleged trade practices were well-known or in common use before the defendant's software was developed. If so, the expert will likely conclude that the plaintiff does not own a valid trade secret.

The software expert may review relevant patents, patent applications, white papers, and articles to determine if the alleged trade practices were well known or in common use before the defendant's software was developed.

Once a software expert verifies that a plaintiff owns a protectable secret, the next step is to determine whether a defendant has misappropriated the secret. The expert may begin by examining contractual language and correspondence between the litigants to determine if the alleged trade secrets were jointly-owned. If so, the expert will typically conclude that misappropriation has not occurred as the use of jointly-owned information for individual business purposes is generally permissible.[10] Another tactic is to examine the programming languages used in the respective products. If the products contain identical programming languages, an expert is more likely to conclude that misappropriation has occurred than if significant portions of code are written in different languages. Finally, if the plaintiff's software contains a combination trade secret, software experts will examine the defendant's software to determine whether it contains every element of the combination. If the expert cannot verify that

the defendant's software contains the entire combination, the expert will likely conclude that misappropriation has not occurred.

3. Protecting Confidentiality

Outside the context of misappropriation litigation, intellectual property litigants often desire to maintain the secrecy of valuable information. Software experts must therefore remain sensitive to trade secret considerations even in software disputes not involving allegations of misappropriation. In copyright infringement cases, for example, a software expert may be required to analyze source code that has been stripped of variable names and comments to protect trade secrets.[11] Further, in evaluating authorship of copyrighted software an expert may review source code for evidence that comments have been removed. The removal of secret information within source code comments may prompt the software expert to conclude that portions of the work have been authored by third parties rather than by the copyright owner. Finally, in determining whether a plaintiff's copyright registration is valid, the software expert may investigate whether the plaintiff has submitted a cover letter with the Copyright Office stating that its software contains trade secrets. If not, the expert will likely conclude that the plaintiff's copyright registration is invalid.[12]

Regardless of a client's litigation strategy, software experts must take special precautions when handling cases involving trade secrets. The expert should abide by all measures the parties and the Court agree are necessary to safeguard secret information. For instance, it is standard practice to analyze the parties' hardware and proprietary software under a strict protective order. Such orders may prohibit connecting computers containing client source code to the Internet, restrict physical access to the premises in which the computers and source code are located, or require computers to be locked so that data cannot be added or removed. In all cases, the software expert should observe rigorous evidence-handling procedures to ensure that confidential information is stored securely and accessed only on a "need-to-know" basis. All documents and computer media received from counsel must be carefully catalogued and tracked. Finally, when an investigation is completed, the expert should certify that it has returned or destroyed all confidential information relating to the matter.

Conclusion

Software experts employ a variety of analytical tools when handling disputes involving individual or combination trade secrets. In particular, the examination of user interfaces, product documentation, and third-party products can shed valuable light on whether a plaintiff owns a protectable trade secret. The examination of source code, user manuals, and executable software is often critical in determining whether a defendant has misappropriated secret information. Regardless of whether misappropriation has been alleged in a software dispute, software experts must remain aware of potential trade secret considerations.

—

[1] See Uniform Law Commission, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited Nov. 28, 2018).
[2] Unif. Trade Secrets Act § 1(4) (1985).
[3] Tait Graves & Alexander Macgillivray, Combination Trade Secrets and the Logic of Intellectual Property, 20 Santa Clara Computer & High Tech. L.J. 261, 266 (2004).
[4] Unif. Trade Secrets Act § 1(2) (1985).
[5] Unif. Trade Secrets Act § 1(1) (1985).
[6] See 18 U.S.C. § 1831 (1996).
[7] See 18 U.S.C. § 1836 (2016).
[8] See H.R. Rep. No. 114-529, at 14 (2016).
[9] See Internet Archive: Wayback Machine, http://archive.org/web/web.php (last visited Nov. 28, 2018).
[10] See B.F. Gladding & Co., Inc. v. Scientific Anglers, Inc., 245 F.2d 722, 729 (6th Cir. 1957).
[11] In computer programming, a “comment” is a programmer’s annotation in the source code added for the purpose of making the source code easier to understand. Comments are ignored by the computer when translating the source code into executable form.
[12] See U.S. Copyright Office, Circular 61, “Copyright Registration of Computer Programs,” https://www.copyright.gov/circs/circ61.pdf (last visited Nov. 28, 2018).

Jeff Parmet

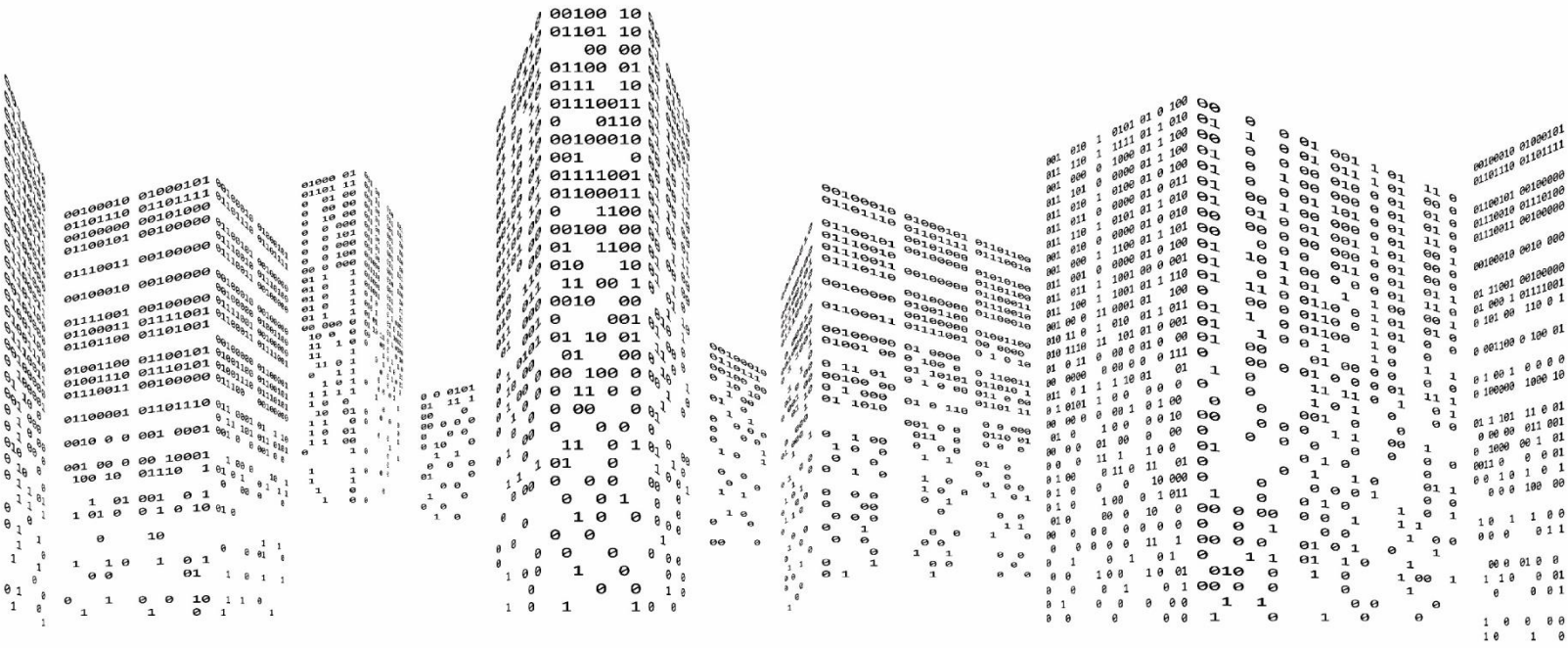
Founder & Managing Partner

Jeff Parmet is a widely respected IT dispute resolution specialist who has served as a consulting or testifying expert on more than 200 software-related disputes. Jeff serves DisputeSoft clients in the capacity of software failure expert, software intellectual property expert, Internet/E-commerce expert, or computer forensic and electronic discovery expert, depending on the requirements of the particular matter. The hallmark of Jeff's practice is independent and objective technical consulting services leading to advice and/or expert witness testimony involving information technology.

Tom Ashley

Manager

Tom Ashley applies his expertise in a wide range of software-related matters, including copyright and patent infringement, trade secret misappropriation, and system implementation failure disputes. Tom has significant experience with software project failure cases, including conducting in-depth investigations of various issues of fact in software failure disputes, such as requirements elaboration, requirements traceability, test planning and execution, defect remediation, and project planning and scheduling.



If you are an attorney in need of a trade secret expert, we invite you to consider DisputeSoft.

Contact Information

Jeff Parmet, Managing Partner

301.251.6182

jparmet@disputesoft.com

12505 Park Potomac Ave. | Suite 475 | Potomac, MD | 20854