FENWICK & WEST LLP

Litigation Alert

California Court Blocks Subpoenas Aimed at Bloggers' Source of Trade Secret Information

JUNE 1, 2006

On May 26, 2006, the California Court of Appeals, Sixth District, issued a unanimous decision striking down subpoenas to Internet "news" sites seeking the source of leaked trade secret information. See *O'Grady et al. v. The Superior Court of Santa Clara County*, Case No. H028579 (Cal. App. May 26, 2006).

The 69-page opinion, which has been certified for publication, is significant because it extends the same constitutional protections to online "news" reporters, editors and publishers, including amateur bloggers, that have traditionally been reserved to print publications, such as newspapers, magazines, radio and television broadcasters. In so doing, the court dealt a blow to efforts by trade secret owners to protect proprietary and confidential information. The court did not view this simply as a trade secrets case:

> "[t]his case involves not a purely private theft of secrets of venal advantage, but a journalistic disclosure to, in the trial court's words, 'an interested public.' In such a setting, whatever is given to trade secrets law is taken away from the freedom of speech…it seems plain that where both cannot be accommodated, it is the statutory quasi-property right that must give way, not the deeply rooted constitutional right to share and acquire information."

The decision demonstrates the importance of strictly enforcing and auditing compliance with company policies, practices and procedures to guard against the unauthorized disclosure of confidential and trade secret information. It also shows the need to review current policies to ensure that they adequately deal with the unique dangers presented by the proliferation of electronic information and the ease of disclosure over the Internet. Finally, the opinion highlights the need for trade secret owners to conduct an extremely thorough internal computer forensics analysis as a precondition, or indeed alternative, to civil discovery.

Case Background

Apple Computer, Inc. brought an action in California Superior Court alleging that unknown persons caused the wrongful publication of Apple's trade secret product information related to a device code-named "Asteroid" or "Q97." Asteroid was an add-on device that would allow users to plug musical instruments into Apple computers and create digital audio recordings. Two Internet "news" sites devoted to Apple products posted verbatim excerpts of technical specifications and a reproduction of a copyrighted rendering of the product design.

Suspecting that some of its own employees had disclosed the alleged trade secrets to these Web sites, Apple conducted an internal investigation led by its corporate security department to determine the source of the leak. The investigation led Apple to believe that the documentary source of the leak was a particular set of electronic slides. However, the identity of persons responsible for the leak remained a mystery, despite interviews of approximately 29 employees and forensic searches of Apple's e-mail servers for communications regarding the disclosed product information. In an effort to identify the source of the leak, Apple sought and obtained authority to issue civil subpoenas to the operators of the two Web sites where the information appeared and to the e-mail service provider for one of the publishers. Nfox, the e-mail service provider, later confirmed that it in fact had in its possession copies of e-mails sent to the Web site operator about Asteroid. The operators of the Web sites sought a protective order to prevent Nfox from handing over any e-mail records to Apple.

Appellate Court's Decision

The appellate court issued a writ of mandate directing the trial court to grant the motion for protective order for the following reasons.

(1) The subpoenas violated the federal Stored Communications Act because they sought the content of private e-mail communications (18 U.S.C. §§ 2701-2712);

(2) The bloggers that operated the Internet "news" sites were entitled to protect their confidential sources and unpublished information under California's reporter's shield in the same manner as printed news publications (CAL. CONST. ART I, § 2(b), CAL. EVID. C. § 1070); and

(3) The Internet "news" site operators could invoke the qualified reporter's privilege under state and federal constitutional guarantees of a free press, which the Company failed to make a sufficient showing to overcome (U.S. CONST. AMEND. I; CAL. CONST. ART I, § 2(a)).

Federal Stored Communications Act

The court initially held that the subpoenas for e-mails sent to the third party Web sites were unenforceable under the federal Stored Communications Act ("SCA"). (18 U.S.C. §§ 2701-2712.) The SCA prevents an electronic communications service provider from knowingly disclosing the content of an e-mail stored by the service provider. The court rejected Apple's primary argument that there was an implied exception under the Act permitting the limited civil discovery at issue. The Act aims to encourage innovative forms of communications, like e-mail, by granting them the same protections from unwanted disclosure as the more traditional means.

The court distinguished this case from so called "John Doe" lawsuits in which litigants are permitted to subpoena Internet service providers to obtain the identities of subscribers who posted anonymous defamatory messages on Web sites. Here, the source of the leaked information did not post the information directly himself or herself, but rather provided the information to the operators of the blog, who in turn made the disclosure. The specific content of the e-mails being subpoenaed therefore remained private and protected from disclosure under the Act.

California Reporter's Shield

The court next determined that the operators of the Internet "news" sites qualified under California constitutional protections afforded to traditional media. The California reporter's shield provides an "absolute protection to nonparty journalists in civil litigation from being compelled to disclose their information sources or any unpublished information obtained in the course of gathering information." The court refused to set forth any test or principle for drawing a line between "legitimate" versus "illegitimate" journalism. The court held that the shield laws are intended to protect the gathering and dissemination of news and that is exactly what the Web site operators did in this case. The sole purpose of the Web sites was to provide its readers with information and news about a particular type of information. The fact that the Web sites simply reprinted "verbatim copies" of Apple's internal information instead of distilling or editing the information in any way did not justify a denial of the reporter's shield protection.

The court also held that operators of news oriented Web sites fall within the ambit of "publishers" and thus the reporter's shield extends to such Web site operators. Finally, the court determined that digital media sources like Web sites are equivalent to newspapers and magazines and thus covered by the law. The court reasoned that the shield is intended to protect the gathering of news for dissemination to the public. Limiting this shield only to traditional print media would not advance this basic purpose of the law. Indeed, the law explicitly covers two non-print sources of news: television and radio. However, the court did indicate that the shield likely does not cover non-recurring publications such as books, pamphlets, or flyers.

Qualified Reporter's Privilege

Finally, the court determined that the operators of the Internet user sites could invoke a qualified constitutional privilege, which protects news reporters, editors, or publishers from compelled disclosure of the identities of confidential sources and unpublished information supplied by such sources. Such reporter's privilege is lost where there is a need sufficient to outweigh the inhibitory effect of such disclosure upon the free flow of ideas and information. See *Mitchell v. Superior Court*, 37 Cal.3d 268 (1984). The court balanced the following five factors and concluded that the reporter's privilege was *not* overcome in this case:

i. ***"Nature of litigation and whether reporter is a party"***. The need for information outweighs the rationale for free press privilege where the reporter or publisher is a party to the litigation. Compelled disclosure is particularly appropriate in a libel action against a reporter. Since Apple had not named the Web site operators as defendants in its trade secret action, the court held that this factor weighed against compelled disclosure. The court was not persuaded by the fact that the petitioners might be named as defendants in the pending trade secrets suit.

ii. ***"Relevance of information sought"***. The court held that this factor favored disclosure because the identity of the misappropriator goes to the heart of a trade secret misappropriation claim. Such information was critical to Apple's case. The court however reduced the weight given to this factor because there was no guarantee that Apple would learn the identity of the misappropriator even if it obtained the discovery it sought. Apple's trade secrets could have been disclosed to the Web sites unanimously.

iii. ***"Exhaustion of alternative sources"***. Compelled disclosure of sources requires a showing that there are no other practical means of obtaining the information. Such disclosures are considered by the courts as a "last resort." This factor was considered *dispositive* in the court's decision not to compel disclosure. In concluding that Apple's investigatory efforts to identify the misappropriators were lacking, the court held that "Apple has failed to establish that there is *any* information that it cannot obtain by means other than the present discovery." Although Apple questioned employees who were known to have access to the documentary source of the leak, the court complained that none of the Apple employees were deposed or questioned under oath. The court also felt that the Company should have follow up with two individuals who were known to have contributed to the drawings in the challenged articles. Finally, the court also focused on the absence of any investigation of how the source files were subsequently processed and handled by the individuals who initially had access to them. Overall, the court thought there was a failure to fully exploit "internal computer forensics."

iv. ***"Importance of preserving confidentiality"***. The importance of preserving confidentiality of a reporter's sources is high when the information relates to matters of great public importance and when the risk of harm to the source is a substantial one. While the court recognized Apple's obvious interest in protecting its own trade secrets, it reasoned that such a "quasi-property" right must give way to the constitutional right of free speech. The court noted that "[t]he newsworthiness of petitioner's articles thus resided not in any technical disclosures about the product but in the fact that Apple was planning to release such a product, thereby moving into the market for home recording hardware." The court appears to have been influenced by its doubt as to whether the information at issue was truly a trade secret. The court openly questioned "[w]hether or not confidential marketing plans constitute trade secrets under the governing statutory language." The court also gave less deference to a trade secret relating to a plan to release a product as opposed to a trade secret relating to how the product was made.

v. ***"Prima facie case"***. The prima facie case factor relates to the demonstrated strength of the plaintiff's case on the merits. The court held that this factor weighed in favor of disclosure because it was reasonable to infer that someone had violated their duty of confidentiality owed to Apple and that the information leaked to the Web sites was a trade secret.

Impact of Decision on Trade Secrets Protection

This decision has substantial implications for trade secret owners trying to protect their proprietary and confidential information. The appellate court has made it extremely difficult to obtain discovery against third party Internet "news" providers that have published the trade secret information. Thus, it is imperative for trade secret owners to institute and adhere to strict internal controls to prevent such disclosures in the first place. They should also review current policies to ensure they adequately address the proliferation of electronic information and the ease of its transmission.

This decision also highlights the increasingly important role of computer forensics to determine the source of the leaked information. Fenwick & West's Electronic Information Management Group specializes in computer forensic preservation and analysis. It has extensive in-house experience in such analysis, which often includes review of firewall logs, e-mail servers and any Web or instant messaging monitoring devices. Such forensic analysis can be far less disruptive than the interrogations under oath of company employees proposed by the court in its opinion. Oftentimes, it is also far more effective at isolating the source of the disclosure.

For further information, please contact:

Patrick E. Premo, Partner, Litigation and Electronic Information Management Groups
ppremo@fenwick.com, 650.335.7963

Gaurav Mathur, Associate, Litigation Group
gmathur@fenwick.com, 650.335.7158