

insights

TYPES NOT MAPPED YET July 01, 2016 | TTR not mapped yet | Mark Sableman

Trade secrets law in the Internet age

How do you maintain a trade secret in the Internet age? As in the punch line to an old joke, “VERY CAREFULLY.”

After all, to preserve a trade secret, you need to maintain it with reasonable confidentiality.

The problem, of course, is the way the Internet facilitates rapid copying and transmission of materials. If a trade secret leaves your building in papers in the briefcase of a renegade employee, you may be able to recover the papers and reestablish the confidentiality of the trade secret. But if it is posted on the Internet, it will likely be copied, recopied, and distributed to so many people that full recovery won’t be possible.

The Business Law Basics

The essential elements of a trade secret, under the Uniform Trade Secrets Act enacted by most states, and also under the federal [Defend Trade Secrets Act of 2016](#), are relatively simple: information used in a business, that is maintained confidentially, through reasonable and appropriate efforts, and that has independent economic value by virtue of that confidentiality. Misappropriation occurs when someone acquires a trade secret by improper means, or knowingly discloses a misappropriated trade secret.

In typical non-Internet cases, owners of trade secrets are expected to carefully protect the confidentiality of their secrets, and courts look critically at any lapses on their part that may have led to disclosures to third parties. Trade secret owners are frequently advised to track their confidential information, develop careful plans for limiting access to it (both within the organization and with suppliers and customers), use confidentiality agreements to bind all persons who have access, and periodically audit and double-check these practices.

How well do you have to maintain the secrecy of your trade secrets? Existing law excuses some carelessness by the trade secret owner, and some leakage of information. In particular, accidental disclosures do not always void trade secret protection, and courts may weigh the carefulness and appropriateness of steps taken to preserve confidentiality against the extent of a particular disclosure.

The Internet Law Twist

The Internet twist to trade secrets is the greater risk of disclosure represented by the Internet. This in turn has required courts to examine just how much secrecy is really required for a trade secret. Because if every Internet disclosure negates a trade secret, that rule would encourage malefactors to steal secrets and destroy them through Internet publication. But at the same time, in many circumstances, extensive Internet publication can be incompatible with the confidentiality component of a trade secret.

For an unusual case of an alleged trade secret distributed on the Internet, consider the 1999 case involving decryption of a DVD content protection program. An unauthorized decryption program, written by a Norwegian teenager, initially spread person-to-person on the Internet. But within a few days, scores of sites were linking to the program. And when the consortium that owned the content protection system sued to prevent further distribution, it listed in its complaint the full URLs of many websites that linked to the decryption program. Third-party postings of that complaint, with those URL references made into active links, further facilitated access to the decryption program.

When the plaintiff’s request for an injunction against further dissemination of the decryption program was heard in Santa Clara County, California, many spectators in the courtroom wore t-shirts that showed the entire text of the decryption program – a demonstration that it was no longer secret. The court granted the injunction against certain named defendants anyway, and ruled that the disseminated program was a trade secret.

The California Supreme Court upheld the injunction against a First Amendment challenge, which claimed that the decryption program was protected speech. But in its affirmance, the Supreme Court relied on the trial court’s

conclusions that the decryption program was a trade secret, and that its disclosure did not destroy the trade secret—issues that would have been strongly fought if the case had gone to a full trial. Those who copied or linked to the decryption program would have argued that it was developed through reverse engineering, in which case it would not qualify as a trade secret. And the massive disclosure of the decryption program, and media links to it, raised both First Amendment issues about the links as well as concerns about the lost confidentiality. It certainly creates problems for a trade secret owner when scores of people in the courtroom are wearing it on their t-shirts.

In cases where trade secrets are already broadly disseminated all over the Internet by the time they reach court, some courts have simply proclaimed the secrecy of the material irretrievably lost, and focus the case on damages rather than an injunction to recover the secret. The court of appeals in the DVD decryption case, in a decision superseded by the Supreme Court, expressed the view that “Widespread, anonymous publication of the information over the Internet may destroy its status as a trade secret.”

But where disclosure has been limited, particularly to sites controlled by the defendants, many courts are likely to restrain further dissemination, and overlook some leakage of the trade secret on the Internet. Specifically, as the court of appeals decision also noted, publication on the Internet may not destroy the secret if it is “sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value.” Similarly, when material is posted through criminal or tortious acts, the perpetrators can’t expect that courts will automatically award their conduct by deeming the trade secret lost. The guiding concern in determining the effect of Internet publication, according to the appeals court, is whether “the information has retained its value to the creator in spite of the publication.”

Even if courts may excuse some Internet publication, wise trade secret owners should take appropriate precautions to keep their secrets secret. It is certainly not enough to disclose them with a mere verbal request, “Please don’t tell this to anyone.”

That’s reported to have happened at a recent medical conference. Hundreds of attendees were reportedly allowed to see new data on a potential blockbuster diabetes drug, more than an hour before its official release to the public and the markets. The attendees were warned to keep the information confidential.

But you have probably guessed what happened: within minutes, key data from the conference, including pictures of charts and key slides, [were tweeted, and retweeted](#). The information was no longer secret. Had the secrecy time frame been longer, the consequences could have been serious.

As it was, the incident primarily served as a reminder of best practices: Don’t put your trade secrets on the Internet – or even in sight of anyone with a smart phone or a Twitter account – if you want to keep them secret.

[Mark Sableman](#) is a partner in Thompson Coburn’s Intellectual Property group. He is the editorial director of [Internet Law Twists & Turns](#). You can find Mark on [Twitter](#), and reach him at (314) 552-6103 or msableman@thompsoncoburn.com.

authorsTest

mark

Mark Sableman