Trade Secret Protection for Source Code

2001-07-17

In a recent and well-publicized case, a California software company and seven of its current and former employees recently pleaded no contest to trade secret theft and other criminal charges stemming from the alleged theft of source code from a competitor. The company agreed to pay $27 million in fines, plus restitution in an amount to be determined by the court. The individual defendants, all former employees of the competitor, face fines ranging up to $2.7 million, and, in some cases, prison terms. A related civil suit is still pending.

The heavy fines and prison terms imposed on the defendants emphasize the value of source code and the stiff penalties associated with its misappropriation. In order to prevent liability on grounds of misappropriation of trade secrets--and to adequately protect a company's source code--it is necessary to (a) understand what trade secrets are, (b) be aware of the legal protection given to trade secrets, and (c) take appropriate protective measures.

Trade Secrets

Trade secrets are protected under both federal and state laws. Although the statutory definitions vary somewhat, these statutes all reflect a similar understanding of what constitutes a trade secret. In determining whether information is a trade secret, the definitions consider both the nature of the information (i.e., whether it is valuable because it is confidential or secret), and the precautions taken by the owner of the information to maintain its secrecy.

Many companies view their source code as their "crown jewels" precisely because competitors do not have access to the source code. By taking proper precautions, these companies can protect their source code as trade secrets.

Penalties for Misappropriation of Trade Secrets

The Uniform Trade Secrets Act ("UTSA"), which has been enacted in approximately 40 states, and other state trade secret statutes provide civil penalties for the misappropriation of trade secrets. Liable parties can be required to pay all damages resulting from the misappropriation, as well as, in some cases, multiple damages or punitive damages. In addition, the defendants can be enjoined from using or disclosing the trade secrets.

The federal Economic Espionage Act ("EEA") (18 U.S.C. §§ 1831-1839), as well as statutes in various states, can also impose criminal liabilities, including heavy fines and prison terms, for theft of trade secrets. For example, under the EEA, individuals convicted of misappropriation of a trade secret can face severe fines and imprisonment for up to ten years, while liable organizations face up to $5,000,000 in fines. As the California case described above demonstrates, the penalties under some state statutes may be even more severe.

Civil claims of copyright infringement and unfair competition, as well as criminal charges of conspiracy, among others, can also arise from theft of source code.

Preserving Secrecy: How to Avoid Being a Victim

In order both to prevent disclosure of source code and to preserve one's legal remedies if misappropriation occurs, software companies should be proactive in maintaining the secrecy of their source code. Consider taking the following steps:

Identify trade secrets. Inventory the company's information to determine what it considers to be a trade secret. In particular, unless the company plans to disclose its source code to the public--or has already done so--it should document the decision to treat its source code as a trade secret. Include confidentiality legends within source code files.

Impose access controls. First, consider who should have access to the company's source code. Then impose the proper physical and electronic barriers, such as password protection and appropriately limited remote access, to prevent unauthorized--or unintentional--disclosure of source code.

Execute confidentiality agreements. Have both employees and third parties, such as vendors, consultants, subcontractors, customers and licensees of the company's source code, execute appropriate confidentiality agreements protecting the company's trade secrets. Confidentiality agreements put the recipient on notice that the disclosed information is considered a trade secret and evidence the trade secret owner's expectation that the recipient will keep it confidential. The breach of a confidentiality agreement can also give rise to a claim of breach of contract in addition to trade secret misappropriation. Finally, under the laws of many states, a written confidentiality agreement can facilitate the imposition of an injunction against a breaching former employee. Note that such agreements must be drawn carefully and not be overreaching to be enforceable.

Inform employees of their obligations. Have newly-hired employees execute a confidentiality agreement, as discussed above. Include in employee handbooks a statement about the importance of preserving the secrecy of source code. From time to time, remind employees of their confidentiality obligations and the value of source code to the company. At exit interviews, remind terminating employees of their duties to return all physical and electronic forms of source code and other trade secrets in their possession and to keep all intangible confidential information secret. Consider having terminating employees confirm in writing that they understand these obligations.

Enforce your rights. If the company's trade secrets are improperly used or disclosed, take appropriate legal action, if necessary, to enforce your rights and prevent further disclosure.

Of course, taking these steps will not transform generally available information and make it a trade secret, subject to the statutory protections described above.

Preventing Liability: How to Avoid Becoming a Defendant

While preserving the secrecy of its own source code is critical to a company's future, perhaps just as crucial is avoiding liability for trade secret misappropriation. Instruct all new employees that the company will not tolerate violation of prior confidentiality agreements and that employees should not use any information which might be deemed to be their former employer's trade secret. Obtaining such a representation can also serve as helpful evidence in defending the employer against an EEA claim. Consider having new employees confirm in writing that they understand these obligations.

Take seriously any allegation of trade secret misappropriation. The California case described above shows that the legal remedies for misappropriation may be severe and can present a serious threat to a company's survival. An allegation of trade secret misappropriation may also seriously damage a company's reputation and value.

Summary

While the above case presents a dramatic example of the pitfalls of trade secret misappropriation, it is not an isolated case. In order to avoid the serious legal and economic consequences of trade secret misappropriation, companies should take preventive measures to avoid becoming a victim or a defendant.

Authors

Belinda M. Juran

RETIRED PARTNER

+1 617 526 6000