DEVELOPERS SHOULD BEWARE OF THE ECONOMIC ESPIONAGE ACT

A federal law, known as the Economic Espionage Act of 1996 (the EEA), could subject you to prosecution for the theft of trade secrets.

The punishment for a violation of the EEA is steep and consists of one or more of the following: (1) imprisonment for up to ten years, (2) a fine up to $500,000, (3) forfeiture of any cash or other property that the developer or anyone else received as a result of a violation of the EEA, and (4) an injunction, which is a court order requiring that a developer who is violating the EEA cease and desist from doing so.

The EEA is a criminal statute, so private individuals and companies cannot use the EEA as the basis for a lawsuit. Only the office of the United States Attorney can bring cases for violations of the EEA. Anyone believing that they are victims of a violation of the EEA will have to convince the United States Attorney to take the case. So that you can be alert to possible violations of the EEA, this article will discuss the elements of a crime under the EEA.

A crime under the EEA arises only under the following six circumstances: (1) a person took, destroyed, or conveyed information without the owner's permission; (2) the person knew the information was proprietary (i.e., owned by someone else); (3) the information was a trade secret; (4) the person intended to take the trade secret to economically benefit her/himself or anyone else other than the owner; (5) the person knew or intended that the owner of the trade secret would be injured if s/he took the information; and (6) the trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce. Attempts and conspiracies to misappropriate a trade secret, and the knowing receipt, purchase, or possession of a misappropriated trade secret may also violate the EEA if each of the above six circumstances is present. Each of these circumstances is discussed in more detail below.

1. Taking Information Without Permission

Under the EEA, a wrongful taking includes the usual methods, such as physically removing the property from its rightful location. However, because trade secrets are often kept in electronic form, theft under the EEA also occurs by copying, duplicating, sketching, drawing, photographing, replicating, transmitting, delivering, sending, mailing, communicating, or conveying. In these instances, the fact that the original copy of the trade secret never left the owner's possession is irrelevant. For example, an unlawful taking of information could occur if a person uses or discloses

information that the developer agreed to keep secret, such as in a nondisclosure agreement.

2. Knowledge That the Information Is Proprietary

A misappropriation of trade secrets will not violate the EEA unless the person knows that the information is proprietary. In other words, bona fide ignorance is a defense to a violation of the EEA. A person will have a hard time proving bona fide ignorance, however, if the information is (a) protected by security measures that are unlocked only on a "need to know basis," (b) marked as "confidential and proprietary" (or words to that effect), and (c) specifically identified in a nondisclosure agreement.

3. Trade Secret

Under the EEA, a trade secret is virtually any information with the following elements: (a) has economic value to the owner, (b) is not generally known by others (including unique compilations of information from the public domain), and (c) is the subject of reasonable security measures, such as those mentioned above that are designed to preclude a defense of ignorance.

4. Economic Benefit to the Developer or Others

Thefts of trade secrets only violate the EEA if someone misappropriates secrets to economically benefit themselves or someone other than the owner. If someone misappropriates trade secrets merely to enhance their reputation, they will not have violated the EEA. For example, a person who uploads a beta version of a hot forthcoming software product onto a Web site and gives it away for free merely for notoriety might not violate the EEA. On the other hand, the government could argue that giving away someone else’s software (even a beta version) economically benefits the recipients because, having the beta version, they might not buy the alpha release.

5. Intent to Injure the Owner

People seldom confess, so proving intent to injure the owner can be done indirectly by proof of their actions. (As the old saying goes, actions may speak louder than words.) Anyone who uses or discloses a trade secret without the owner’s permission, even merely as a lark, arguably has some intent to hurt the owner because, after disclosure, the information will no longer be secret. In other words, proof of an unauthorized use or disclosure may suffice to prove intent to injure.

6. Interstate or Foreign Commerce

As mentioned above, the final element of an EEA violation requires that the trade secret is related to or part of a product that is produced for or used in interstate or foreign commerce. *Interstate* commerce is commerce conducted in at least two states. (On the other hand, *intrastate* commerce is conducted in only one state.) *Foreign* commerce is commerce conducted anywhere in the United States with a person or business in a foreign country. This requirement exists because, under the United States Constitution, Congress can usually only regulate activity that affects interstate or foreign commerce. (In contrast, intrastate commerce is usually regulated by the state in which that commerce is conducted.) If a product involves or is distributed through the Internet, it will in all likelihood be considered interstate or foreign commerce simply because the Internet uses the telephone lines.

The EEA raises important concerns for software developers (and their employees), who will certainly want to avoid situations that could lead to criminal prosecution under the EEA. People are free to use their general skill and knowledge, including general skills and knowledge acquired while working on clients' or employers' projects, without violating the EEA. You should make sure that your clients agree with your understanding of "general skill and knowledge." To do this, your contracts should specifically identify your clients' trade secrets and should acknowledge your right to freely use all other information you acquire as a result of your work on the project. Likewise, if you have employees or if you are an employee, you should have an employment agreement that specifically identifies the employer's trade secrets.