Successfully Defending Software Audits

By Rob Scott

Shrinking IT budgets and fierce competition among software publishers have created explosive growth in the incidence and frequency of software audits—a mechanism by which software publishers investigate their customers to determine if they are in compliance with software licenses and copyright laws. In addition to developing internal enforcement operations, many publishers have engaged trade associations to perform enforcement activity under power of attorney. Industry analyst Gartner, Inc., estimates that 40 percent of all medium to large U.S. businesses will face an external software audit by the end of 2006.[1] Businesses that are most prepared and properly represented will have the greatest success in defending the inevitable software audit.

A software audit is initiated by a software publisher or a software trade association such as the Business Software Alliance (BSA) or the Software and Information Industry Association (SIIA). Although the trade associations have no independent regulatory or enforcement authority, software publishers have granted the associations power to pursue copyright infringement claims. The most common impetus for a software audit is a report of software piracy received from an informant, who is usually a disgruntled employee.[2] In some instances, these informants are awarded cash rewards tied to the proceeds of the audit. Companies targeted for audit are not required to cooperate with the trade associations or publishers, but resolution without litigation is highly unlikely without an agreement from the target company to participate in a voluntary audit.

There are a number of legal issues implicated in software audits. Although software usage is governed by a contractual license, the software industry generally relies upon the stronger protections afforded by the Copyright Act of 1976. The Copyright Act provides stiff penalties for copyright infringement—up to $150,000 per violation if the infringement is willful.[3] Additionally, courts have imposed individual liability upon officers and directors of corporations who infringe copyrights, provided that the officer or director had the ability to control the activity that constituted infringement and there was a financial benefit resulting from the infringement.[4]

Clients are generally advised to cooperate in the prelitigation audit process but in a manner that does not compromise their legal position in the event that out-of-court resolution is not possible. In light of the highly specialized issues that arise in these matters, unrepresented or underrepresented clients generally make a series of common mistakes that jeopardize their legal position.

The most common mistake we encounter in software audits is the failure to compile and produce accurate installation information. Like all technology projects, collecting the information to produce in response to a request for an audit can be very complicated and time-consuming. To begin the audit process, it is necessary for the company to select an automated software discovery tool. Even for small environments, employing a manual process to review the software on each computer is time-consuming and unreliable. Most companies choose an automated process instead. Any automated discovery that is conducted directly by the client or by a third-party provider will not be protected by the attorney-work product privilege because the privilege applies only to communications between attorneys and their clients. Discovery tool selection is critical to the success of the audit initiative. Many tools capture information related to the software installations on a computer network, but produce the results in a format that the company cannot interpret. Even worse, many companies produce the audit results from the free tools provided by the trade associations. These tools, more often than not, inaccurately report the data and fail to exclude information that is outside the scope of the audit request.

Companies also err in the audit process by relying on their IT staff to respond to the request for an audit. Members of IT departments typically prepare audit reports containing information that is incorrect or beyond the scope of what is required to adequately respond. This is particularly problematic because the release of liability contained in most software audit settlement documents is contingent on the accuracy of the results produced during settlement negotiations. If the technology department improperly reports the software installations, the monetary portion of the settlement will be inflated, and the release of liability will be jeopardized.

Another common error that audited companies make is submitting improper documentation in an attempt to demonstrate proof of ownership for software licenses. Contrary to popular belief, trade associations and publishers only accept dated proofs of purchase, with an entity name matching that of the audited company, before acknowledging that the company owns a license for a particular product. For this reason, companies should avoid purchasing additional licenses of installed software in response to a request for an audit as these purchases will be irrelevant to the audit. Companies should seek the advice of counsel regarding the purchase of additional software during the audit process and the impact that it may have on the prelitigation audit and any

Scott is the managing partner of Scott & Scott, LLP in Dallas, Texas.

subsequent litigation that may arise.

Because most clients are not able to properly interpret copyright laws and software licenses without specialized legal assistance, it is critical to involve experienced counsel in the process of interpreting the software installation information gathered by the automated discovery tool and reconciling that data with all available proof-of-purchase information. Once the installation information has been collected, it should be reviewed to determine whether it includes only information within the scope of the audit. Additionally, licensing models are often dependent on the actual use of the product in the company's specific environment. In other words, you cannot interpret the license without a thorough understanding of the computing infrastructure and how the software is being used from a technical perspective. Other licensing considerations that require specialized knowledge and expertise include client access licensing, upgrade and downgrade rights, and licensing for nonconcurrent laptop use.

Experienced counsel will be able to provide the audited company with a very accurate estimate regarding how the auditing entity will interpret the results and provide considerable visibility into the likely monetary aspects of a proposed settlement. Many companies and inexperienced attorneys underestimate the exposure and are unpleasantly surprised when the analysis of the audit materials is performed by the auditing entity. Discussing the settlement range in advance of producing the audit results helps manage client expectations and increases the likelihood of an out-of-court resolution.

In order to protect the target company's interests, it is advisable to obtain an agreement that Federal Rule of Evidence 408 governs the admissibility of the audit results prior to producing the audit materials. Furthermore, the audit materials produced should be narrowly tailored to include only the products identified in the letter requesting a selfaudit. The schedules should contain a summary with columns for product name, cumulative installations, total proofs of purchase, and the excess or deficiency per product. It is also helpful to organize the supporting materials, including the proofs of purchase, by product.

Following production of requested audit materials, the auditors may refuse to give credit for certain proofs of purchase or seek clarification of the installation information. It is important to review the auditor's analysis critically and provide additional information as necessary. Once the auditor's analysis is factually accurate, prior to engaging in monetary negotiations, experienced counsel should make legal challenges to the basis for the proposed fine calculation. A carefully reasoned, legally supported argument will expose the software publishers' weaknesses and increase the chances of a successful result.

In trade association audits, the BSA and SIIA include a draft settlement agreement with the opening settlement offer. There are a number of onerous nonmonetary provisions that should be negotiated prior to settlement. For instance, the BSA often inserts a provision in its proposed settlement agreement that the BSA can enter and inspect the company's facilities two times per year to ensure that the company is still in compliance with all software licenses. Additionally, the release in the agreement is predicated on the accuracy of the certifications, and in many cases, on future performance of the settlement obligations. Counsel must also carefully advise the client regarding the obligation to certify under penalties of perjury that its networks are in compliance as of the settlement date.

Software publishers and their trade associations are targeting companies of all sizes, accusing them of software piracy and copyright infringement. The issues arising in software audits are unique and require both legal and technical expertise. The costs associated with software audits, even those that are resolved successfully, are substantial. Audited companies that enlist experienced counsel to guide them through the process and avoid common mistakes have the greatest chance for the most cost-effective outcome.◆

Endnotes

1. OBrien, Frances, *Why IT Asset Management Is Important Now*, June 10, 2004, *at* http://www.gartner.com/DisplayDocument?doc_cd=121336 .

2. Compushare Newsletter, Volume 7, Issue 4, April 2005, www.compushare.com/docs/April%202005.pdf.

3. 17 U.S.C. § 501.

4. *See* Shapiro, Bernstein & Co., Inc. v. H.L. Green Co., Inc., 316 F2d 304 (2d Cir. 1963); RCA/Ariola Intern., Inc. v. Thomas & Grayston Co., 845 F.2d 773 (8th Cir. 1988).