Beware of the Watchdog

BY DAVID D. SPRAGUE AND GEORGE S. FISH

OVER THE LAST TWO DECADES, the Internet and new technology have enabled businesses and individuals to create, distribute, duplicate, and share enormous amounts of information in a matter of seconds. While technology has increased productivity and business efficiency and expanded the global marketplace, it also has spawned copyright infringement and an increased vigilance for software developers to protect copyrighted software. Companies like Microsoft, Adobe, Symantec, and other members of the commercial software industry have funded the growth of the Business Software Alliance (BSA), a nonprofit trade association that acts as the industry watchdog. BSA operates in over 60 countries, with offices based in the United States, Europe, and Asia, and works as an agent on behalf of its members to aggressively pursue alleged software licensing violations through the use of software audits.[1] BSA punishes piracy and educates consumers by using its successfully negotiated settlements in publicized campaigns like its recent "$2 Million Tuesday," where it released its software piracy survey results along with the news it had settled software copyright claims with 25 companies for more than $2.2 million dollars.[2]

Responding to the Business Software Alliance

Targeted Campaigns

BSA devotes significant member resources to regionally targeted campaigns. The campaigns consist of radio, print, and web-based advertisements that are largely marketed to educate and increase awareness among business owners, IT managers, employees, and vendors. Additionally, some BSA ads are directed to employees and encourage them to "report all piracy." BSA has been criticized for many of these ads because they invite disgruntled employees or former employees to allege violations under BSA's promise of anonymity. Once allegations have been made, BSA will often conduct a preliminary investigation to determine the validity of the claim.

Preliminary Investigation

Generally, BSA begins its investigation of a company based on information it receives about alleged software licensing infringement. BSA will typically attempt to collect adequate information from the source to determine the validity of the software-licensing allegation. Most investigations are conducted with the assistance of outside counsel, but BSA enforcement attorneys may independently handle investigations of small companies, or where the allegation is specific and limited to a very small number of infringements. Even if BSA learns it has obtained the information from a disgruntled employee, it will not discredit the allegation on that basis. BSA determines the credibility of the alleged infringement in two ways: (1) by getting a detailed statement from the informant regarding the alleged infringements, and (2) by verifying whether or not the company in question has purchased the software and registered licenses from the software company.

Investigation and Authority to Act

BSA initiates an informal investigation of the target business when it sends a letter stating it has received information that indicates the business "may have illegally-duplicate proprietary software installed on its computers."[3] According to the letter, BSA is attempting to avoid litigation and formal action by contacting the business and asking for its cooperation in the investigation. The letter usually provides a specific list of software applications that are the subject of the investigation. To comply with the investigation, the target business is required to contact BSA for instructions on how to conduct a software audit and preserve the software installed on its computers as evidence "in case the matter proceeds to litigation."[4] If the company does not comply with the demand, BSA may have accumulated enough information about the company's alleged infringement to pursue an audit through a court order.[5]

Additional authority for the audit may come from the software-licensing agreement itself. Most people simply click, "I agree" and skip through the software licensing agreement when installing a new piece of software. Generally, these agreements are offered to the licensee on a take-it or leave-it basis; however, in larger business transactions, written license agreements may be formally negotiated and signed.[6] Regardless of whether software license agreements are negotiated, they are legal documents that set forth the rights and duties of the parties, the purpose or capability of the software, the terms and conditions for its use, and any information regarding the software's warranty. Today, most software-licensing agreements have an audit clause that not only requires the licensee to submit to a software audit, but also may contain language requiring the licensee to reimburse the licensor for any expenses reasonably associated with the audit if the use is not in compliance with the terms of the agreement.[7] Finally, if the licensing agreement contains an explicit integration clause, it may bar all parol evidence contrary to that found in the agreement except where fraud or other grounds are sufficient to set aside a contract.[8]

Fast Facts:

BSA operates in over 60 countries, with offices based in the United States, Europe, and Asia, and works as an agent on behalf of its members to aggressively pursue alleged software licensing violations through the use of software audits.

Any litigation for software infringement is based on violations of the Copyright Act of 1976.

The quickest way to end a BSA investigation is to have proofs of purchase, certificates of authenticity, and licenses for each software installation.

Cooperation with the Audit

In general, the self-audit is an informal process set up with cooperation between BSA and the target business and coordinated through counsel. Some companies have been "raided" by BSA and U.S. Federal Marshals in an attempt to gather the necessary information for verifying the allegation, and to protect the evidence for federal indictment. A notable BSA raid occurred in December 1997, when U.S. Federal Marshals raided the Taiwan Trade Center following an investigation that showed six companies located within the Trade Center were buying, selling, and distributing counterfeit products.[9]

Unlike the Taiwan Trade Center, raids on United States-based companies are unlikely because most are considered customers of BSA members and unintentional infringers rather than distributors of counterfeit software.[10] The typical recommendation to a business receiving a letter from BSA alleging infringement is to contact legal counsel and be prepared to cooperate in the investigation. Ultimately, cooperation often puts the business in a better position to resolve outstanding issues and provides time for the business and counsel to evaluate its legal position for negotiations and, if necessary, to prepare for litigation.

Litigation

Any litigation for software infringement is based on violations of the Copyright Act of 1976 (Copyright Act).[11] To establish copyright infringement under the Copyright Act, BSA must be able to demonstrate: (1) its member is the valid owner of the copyrighted software, and (2) the target business had unauthorized copies of the software in its possession.[12] Many companies attempt to settle with BSA because the evidence of minimal infringements is enough to justify substantial damages against the company under the Copyright Act. Settlement is also often in the best interest of BSA, especially where it is clear that the infringements are unintentional. BSA recognizes the target company is a vendee of its members, even if it is not in compliance with its software licenses. By settling, BSA serves its client-members by bringing the business into software-licensing compliance, replenishes its coffers, and keeps the business as a paying vendee of its client-members. Sometimes the vendee company can secure agreements with BSA or the vendor to keep the settlement and all the surrounding issues undisclosed.[13]

Settlements Disclosed

Some BSA settlements are undisclosed; however, most companies are not so fortunate. Often, the details from settlement agreements are available as press releases on the BSA website and are also sent to the local press.[14] BSA uses the disclosed settlements as a tool to educate businesses and individuals about infringement and to further discourage the use of unlicensed software. From a company's perspective, every negotiation and settlement should require a tailored confidentiality agreement to limit or negate BSA's ability to disclose, publish, or disseminate details of the settlement. Such disclosures are often embarrassing and may damage the reputation of the business.

Damages

If litigation ensues and BSA establishes copyright infringement, BSA will be entitled to recover for its member either actual damage suffered plus attributable profits or statutory damages, and may be awarded attorneys' fees and costs under the Copyright Act.[15] In order to establish profits under the Copyright Act, the BSA is required to present only proof of gross revenue of the target business, while the target business has the burden of showing any deductible expenses or "elements of profit attributable to factors other than the copyrighted work."[16] Statutory damage penalties range between $750 and $30,000 per infringement, or between $750 and $150,000 per willful[17] infringement.[18] Further, criminal penalties may apply where a person willfully infringes on a copyright "for purposes of commercial advantage or private financial gain."[19] Criminal penalties may include a fine not exceeding $250,000, or a maximum of five years in prison if 10 copies were made within any 180-day period having a total value greater than $2,500 at retail prices.[20] Although the potential statutory penalties are staggering, most BSA settlements are well below the statutory thresholds that could have been imposed based on the number of software infringements discovered.

Defenses

In addition to being required during an investigation by BSA, self-audits are also a company's best opportunity to defend potential copyright infringement by being proactive. The Copyright Act places an affirmative duty on every business to comply with software licensing throughout its IT infrastructure on each piece of hardware owned or controlled by the business. This duty may extend to portions of the business acquired through asset purchase or to businesses acquired through merger.[21] Compliance means the business will need to adopt and notify employees of new corporate policies placing restrictions on installation and use of software by desktop users. The corporate policy should also provide a software purchasing process that keeps track of purchases, installation, and proofs of purchase.

Software Audits

Today, a number of companies offer software or services that allow a business to complete thorough audits of its IT infrastructure. Network audit products and services are relatively inexpensive and make the review of the infrastructure fairly simple. Several companies have developed network software that creates daily reports on software installed on the network and proactively monitors the network for any new occurrences of software installed on any hardware connected to the network.

The quickest way to end a BSA investigation is to have proofs of purchase,[22] certificates of authenticity,[23] and licenses for each software installation. The problem most companies have in defending an audit is finding and reviewing these documents is often the most difficult, costly, and futile task in the audit process. The inability to find documentation during a BSA audit can be costly. During an audit, BSA requires the target business to send proofs of purchase and licensing information for every software installation on every piece of hardware it owns or controls. Most companies do not keep proofs of purchase and, without them, BSA often requires a settlement payment for software that was legally purchased and installed by the business.

Privilege and Software Audits

Some states have recognized the self-critical analysis privilege as a qualified privilege used to protect businesses when they perform certain self-critical appraisals. The rationale for the privilege is to allow a business to freely assess compliance with legal or regulatory requirements without creating evidence that may be used against it in future litigation.[24] Even where the privilege is recognized, however, most courts have narrowed it to extend only to communications regarding self-critical analysis or opinion, and not to facts.

Although Michigan courts have not specifically addressed the issue of software audits, internal audits in general have not been protected by privilege.[25] Even when the Michigan Court of Appeals recognized the self-critical analysis privilege in connection with a governmental agency's evaluative or deliberative processes, it refused to shield any portion of a report that was factual in nature.[26] Thus,

practitioners should be mindful that communications with their clients regarding the underlying facts will be discoverable even in states that recognize the self-critical analysis privilege.

Conclusion

Software compliance is a growing concern, and attorneys should proactively address compliance issues with their business clients. Attorneys need to educate their clients about the problems associated with illegal software being installed on their hardware, or the potential exposure of failing to document their software installations. BSA estimates ninety percent of all companies have some exposure to software liability, so it is important to get clients to develop good software policies that may help relieve managers and owners of liability.[27] Also, attorneys should consider software-licensing compliance whenever they are handling a merger or negotiating an acquisition of another business for their client. Finally, attorneys should consider handling BSA audit letters. If a business fails to recognize the potential for liability in the BSA audit letter, the disclosure may result in a staggering request for monetary damages and the potential for embarrassing disclosures of the settlement. ◆

David D. Sprague is an attorney with Raymond & Prokop, P.C., where he is a member of the Automotive and Technology Industry Groups. His practice includes computer and information technology, real estate, commercial transactions, general corporate law, and litigation. Mr. Sprague was employed for 10 years in the automotive and information technology industries by General Motors Corporation, as a member of its Corporate Finance Staff, and Electronic Data Systems, as an Operations Manager. He is a member of the Real Property, Computer Law, and Business Law Sections of the State Bar of Michigan and is admitted to federal practice in the United States District Court for the Eastern District of Michigan.

George S. Fish is a partner with Raymond & Prokop, P.C., whose practice focuses on commercial litigation. He has substantial experience in disputes involving Article 2 of the Uniform Commercial Code, representing both majority and minority interests in shareholder disputes in closely held businesses and counseling clients on a broad range of business matters. His experience also includes employment and not-compete matters, as well as bank-related litigation.

Footnotes

1. The Software & Information Industry Association is a similar trade association that provides global services in government relations, business development, corporate education, and intellectual property protection for its member companies in the software and digital content industries.
2. Business Software Alliance press release, October 12, 2004, available at http://www.bsa.org/usa/press/.
3. Business Software Alliance Investigation Letter (quoting language from an actual initial letter sent to a business that has been targeted for a BSA software audit and investigation).
4. Id.
5. According to Robert M. Kruger, Vice President of Enforcement for BSA, BSA has applied for and received court orders in California, Arizona, Texas, Colorado, New Mexico, Florida, New York, New Jersey, Massachusetts, Kentucky, and a number of other states to perform raids based on information received from informants. Leslie Walker's .com Live, available at http://washingtonpost.com.
6. Even where the parties have unequal bargaining power, contract terms will be enforced if they are substantively reasonable. *Citizens Ins Co v Proctor & Schwartz,* 802 F Supp 133, 145 (WD Mich 1992).
7. See e.g., End User License Agreement for Macromedia Flash Player 7, available at http://www.macromedia.com/shockwave/download/license/desktop.
8. *Tibco Software, Inc v Gordon Food Serv,* 2003 US Dist LEXIS 12020 (WD Mich 2003) (holding that parol evidence is not permitted where the agreement is integrated).
9. *Microsoft Corporation v Taiwan Trade Center,* 989 F Supp 80, 82 (DPR 1997).
10. Thomas Hoffman, *BSA Pursuing 700 Software-Piracy Probes, Computerworld,* at http://www.pcworld.com (Sept. 23, 2004) ("BSA rarely raids enterprise customers with federal marshals and court orders," according to Robert M. Kruger, Vice President of Enforcement for BSA).
11. 17 USCS 101 et seq (2004).
12. *Dun & Bradstreet Software Servs v Grace Consulting, Inc,* 307 F3d 197, 206 (CA 3, 2002).
13. See, e.g., *Microsoft,* 989 F Supp at 82 (Microsoft and the Taiwan Trade Center had an agreement not to disclose the contents of the agreement unless authorized by the Taiwan Trade Center. BSA violated the confidentially agreement by immediately publishing a press release about the settlement without the Trade Center's approval. The United States District Court for the District of Puerto Rico ordered BSA to immediately comply with terms of the settlement agreement and ordered them to "pay reasonable attorney fees for all the proceedings which ensued from the publication of the press release." Id. at 84).
14. See generally BSA press releases at http://www.bsa.org/usa/press.
15. 17 USC 504(a) (2004).
16. 17 USC 504(b) (2004).
17. The Copyright Act does not define willful infringement; however, a number of circuit courts "have held that infringement is willful if the defendant 'has knowledge,' either actual or constructive, that its actions constitute an infringement or recklessly disregards a copyright holder's rights." *Lyons P'ship, LP v Morris Costumes, Inc,* 243 F3d 789, 799 (CA 4, 2001).
18. 17 USC 504(c) (2004).
19. 17 USC 506(a)(1) (2004).
20. 18 USC 2319(b)(1) (2004).
21. In Michigan, the corporation purchasing assets of the selling corporation is not generally responsible for liabilities of the selling corporation unless obligations are either expressly or impliedly assumed by agreement. *Jeffrey v Rapid Am Corp,* 448 Mich 178, 190; 529 NW2d 644, 651 (1995). However, "when two or more corporations merge, the surviving corporation generally succeeds to all the liabilities of the constituent corporations." Id.
22. Proofs of purchase may include such standard items as invoices, purchase orders and receipts, as well as distribution media, packaging material, and software documentation or a site-license agreement. In addition, the software vendor or a third-party company may issue a digital certificate that guarantees the software is from the publisher who issued it, and provides assurance that the code was not corrupt when it was issued by the vendor.
23. Personal computers purchased today generally come with some software that is distributed by either enclosing it in the PC's box or preloaded software (e.g., the PC's operating system). The proof of authenticity for software purchased with the PC may be attached to the computer chassis, included in the product manual, or located within or on packaging material for the PC or software.
24. *Reichhold Chems v Textron,* 157 FRD 522, 524 (ND Fla 1994).
25. *Siskonen v Stanadyne, Inc,* 124 FRD 610, 612 (WD Mich 1989) ("Given the state of the law it is impossible to conclude with any confidence that the Michigan Supreme Court would recognize a critical self-analysis privilege.").
26. *Ostoin v Waterford Twp Police Dep't,* 189 Mich App 334, 338; 471 NW2d 666, 668 (1991).
27. At minimum, businesses should have software policies that include a section on the ethical use of software, and an installation policy that requires all software to be installed by the company's information systems personnel.