A Trap for the Unwary

Don't Get Caught Operating without a License

By N. Kane Bennett

The best ways to prevent software compliance audits or enforcement actions for improper software use.

Operating without a license can put a company out of business. No, I am not talking about a driver's license. I am talking about something more frequently overlooked, but much more dangerous—a software license.

If you advise business owners of any size, software licensing presents a real trap for the unwary. It is a trap that can sink a business.

This article will address typical software licensing issues and the ways in which businesses can run afoul of copyright laws. This article will also present the consequences if business owners improperly use software and some practical tips to prevent costly disputes. Finally, this article will offer guidance on what to do if your business client gets caught operating software without a license.

Software Licensing and Software Piracy

When a business buys a computer, it also buys software to use on the computer. The software typically comes with a license. Examples of well-known software that come with a license are products from Microsoft, such as Word, Office, Excel and PowerPoint. When you purchase software from a publisher like Microsoft, you might think you own it, but you do not. Microsoft basically gives you permission to use it for a price. However, Microsoft does not give you the right to do whatever you want with it. Confused? So are a lot of software users.

To be more specific, when you use a software program, such as Microsoft Word, the license that comes with it restricts your use of the software. The specific restrictions are contained in the license itself and can differ depending on the software program and the purchasing terms.

A typical software licensing agreement prohibits users from illegally copying a program. For example, you cannot copy someone else's properly licensed version of the software, or install the program multiple times on several computers for use by more than one person. Similarly, you cannot install a program on a network server and let multiple people use it unless you have the proper number of licenses.

If a software purchaser breaks the terms of the license, the purchaser risks committing software piracy. The software publishing industry uses the term software piracy to mean any unauthorized copying or distribution of copyrighted software. Software piracy includes violation of federal copyright laws and the licensing agreement itself.

■ N. Kane Bennett is a DRI member and partner with the firm of Raymond & Bennett, LLC located in Glastonbury, Connecticut. Mr. Bennett's practice focuses on commercial, business, and product liability litigation in Connecticut and Massachusetts. He is also a frequent commentator, author and speaker on issues of technology and the law.

When you hear the term piracy, you get a vision of someone stealing software off of a store shelf or selling it out of the back of a truck. In reality, software piracy includes much lesser offenses, such as installing the software you purchased for your business onto your child's laptop at home.

Businesses and their managers, if found responsible for software piracy, risk criminal and civil penalties. Civil penalties include monetary damages for the software publisher's lost profits and statutory damages up to $150,000 for copyright infringement. Civil penalties also include injunctive relief preventing the continued use of the software. Software piracy further carries the risk of criminal prosecution with fines ranging up to $250,000 and incarceration for up to five years.

Other consequences for software piracy may not be so obvious. For one, managing public relations can become a problem for a company accused or found guilty of software piracy. Second, users of pirated software also run the risk of copying viruses. Third, a software pirate will not receive updates of and patches for problems with the software. Finally, a software publisher will not provide technical support to a software pirate.

How common is software piracy? The software industry claims that as much as 21 percent of software used in the United States is unlicensed. This costs about $7 billion in lost revenue annually. Imagine how rich Bill Gates would really be if everyone using a Microsoft product actually paid for it!

Potential Software Piracy Problems

Based on a variety of factors, it's likely that most businesses fail to comply with some aspect of software licensing requirements, and many times it is unintentional. Businesses can inadvertently run afoul of licensing restrictions in many ways.

In some instances, software piracy is more obvious than others. For example, generally software cannot be purchased and then resold for profit or distributed if already installed on computers. This type of software piracy tends to be an intentional or knowing violation of copyright laws and licensing contracts.

Some less obvious forms of software piracy occur inadvertently, or without full knowledge of the implications. How many of your clients actually read the license that comes with software? A business can unintentionally violate a license if it fails to determine its proper limitations, such as how many times software can be installed or how many users can have access to it.

Problems can occur when a business tries to cut corners or save costs by installing multiple copies without fully understanding the potential for fines and penalties. A business might commit software piracy by relying on the advice of IT professionals cavalier about proper licensing or philosophically opposed to paying for licensing. A classic example is the small business that uses a family friend for IT support. The friend may try to help the business trim costs by installing several copies of software programs when the business only purchased one license.

A big problem arises when a business' employees violate licensing agreements. The business can be held responsible and exposed to penalties even if management did not know of an employee's improper software use. How many of your business clients periodically audit their employees' computers for unauthorized software downloads? A business can face software piracy charges if an employee downloads software from the Internet without proper use licensing and without advising management. Problems can also arise if an employee "shares" software by installing work programs on too many home computers. The business may face piracy fines and penalties.

How Are Businesses Caught?

For most individual computer users, software licensing is an afterthought or a neverthought. Most computer users, whether at work or at home, think of computer use as a private exercise. Generally speaking, they are right. In fact, the odds remain that your average, small scale, software pirate will not face penalties. However, many businesses do, in fact, get caught operating without proper licensing.

Businesses are caught when they draw the attention of software publishers or the enforcement groups for publishers, such as the Business Software Alliance (BSA) or the Software & Information Industry Association (SIIA). The software industry and its trade groups frequently publish and broadcast collected settlements from U.S. businesses totaling in the millions of dollars on an annual basis.

How do businesses draw attention? Most of the time, scrutiny results from information from informants. Informants are the biggest source of information leading to enforcement software piracy actions. In fact, not only do software publishers seek informants, but trade groups encourage informants to report software piracy. These trade groups, such as the BSA, act on a power of attorney from software publishers like Microsoft.

> **Businesses** and their managers, if found responsible for software piracy, risk criminal and civil penalties.

Informants are encouraged by the offer of anonymity and large potential rewards. Some of your clients might think that their businesses would never be charged with software piracy. However, many times, an informer is a business' IT employee. Another category of informants is former or current disgruntled employees looking for a pay off.

What Types of Businesses Are at Risk?

Any business that uses a computer faces potential exposure to software piracy charges. This means that the risk pool is essentially *every* business. Businesses should not think that Microsoft or other software giants will not come after a small business. Many small businesses have paid substantial fines in settlement of software piracy cases. In fact, in many respects, a small business can be more vulnerable because it has fewer resources to fight an enforcement action.

The Software Licensing Audit

Once an informant provides a solid lead on software piracy to a software publisher or industry trade group, a business will typically

License, continued on page 76

License, from page 59

receive a cease and desist letter and/or a letter requesting a software licensing audit.

A software licensing audit boils down to a critical review of software assets to determine if all the software available for use is properly licensed. The audit can be self-administered or conducted by an outside party. The goal of the audit is to determine compliance with licensing agreements. The results of these audits typically form the basis for enforcement or corrective action.

After receiving an audit letter, a business will have to decide how to respond. The basic choice is to fight or cooperate. Many businesses might not understand the potential exposure involved at this stage and can face real uncertainty about the identity of the informant. Most small businesses cooperate on some level by allowing the audit in some agreed upon fashion. Cooperation can be like letting the fox into the hen house, but fighting may not be a realistic alternative, especially if licensing noncompliance is genuine.

Tips to Avoid Inadvertent Software Piracy

Given the potential criminal and civil penalties for software piracy, here are some tips to help you and your clients avoid inadvertent software licensing compliance:

- **Periodically conduct a self-audit.** Most businesses probably fail to comply with licensing terms in some area. To minimize the risk of an enforcement action or formal audit, it's best for a business to be proactive by identifying noncompliance on its own.
- **Create a software asset management plan and enforce it.** A software asset management plan should include (a) a written policy covering the terms for copying, use, and transfer of company software; (b) written advisements of the seriousness of software piracy; and (c) a written employee disciplinary policy outlining the consequences for an employee for improper software use.
- **Develop a software repository or management system.** A software repository or management system should keep adequate software records, licenses, and dated proof of purchases in a fire-proof, secure location. A business can run into problems during an official audit if the business actually purchased a proper license, but cannot adequately prove it with documentation.

If you or a client do face an enforcement action or receive an audit letter, here is some advice:

1. **Hire knowledgeable legal counsel.** It is imperative to engage knowledgeable counsel to protect your interests if you face an enforcement action for software piracy. A business' managers or IT professional should not try to negotiate with trade groups or software publishers. Too many variables requiring the input of legal counsel can substantially affect the action outcome.
2. **Do not ignore an audit letter.** Receiving an audit letter is serious, and it should not be disregarded or ignored. If you ignore the letter, you risk ending up in court and can lose the opportunity for a fair negotiation.
3. **Do not destroy or delete the software.** This one should be obvious but because the temptation exists it should be advised against.
4. **Do not fire an employee for informing about software piracy.** Firing an employee could lead to additional litigation for wrongful termination.
5. **Do not run out to buy the proper licensing**—it will not solve the problem. Any enforcement action taken pursuant to a licensing audit will insist on proof of proper licensing at the time of the offense.

Conclusion

Proactive planning and software asset management are the best ways to prevent software compliance audits or enforcement actions for improper software use. Even with the best policies, however, inadvertent licensing issues can arise for any business. When faced with noncompliance actions, you have a variety of methods to manage the situation. Most importantly, a business should engage legal counsel to assist with preventing or defending a software enforcement action or licensing audit.