

SOFTWARE ASSET MANAGEMENT

A Brief Overview

A White Paper by:

KATYA LEZIN, JD, LL.M.
For
Veriam Technologies, Inc.



COPYRIGHT NOTICE

Copyright © 2006-2008 by Veriam Technologies, Inc.
All rights reserved.

This document is protected by the copyright laws of the United States of America. It may not be reproduced, nor may any of its contents used in whole or in part, without the express written consent of the author.

ABSTRACT

Most businesses, like most citizens, are law-abiding. The majority do not knowingly break the law and most, when asked, would answer honestly that they have complied with all regulations and requirements regarding the licensing of their software. The unfortunate and costly reality, however, is that these same seemingly law-abiding businesses would not survive a software piracy enforcement audit unscathed. The available information and laws on what constitutes proper proof of license with respect to software assets is murky at best. Navigating what your legal rights and liabilities are in software asset management is worth an investment of time and finances up front because the penalties for noncompliance – even when unintentional – are onerous and swift.

SOFTWARE PIRACY

Software piracy is the illegal distribution and/or reproduction of software. The Business Software Alliance (BSA) estimates that the IT industry loses nearly 33 billion dollars annually from software piracy. According to the BSA's figures, "in the United States, one in four software programs is unlicensed." (<http://www.bsa.org/usa/antipiracy>). What this means to you is that the leading software producers take piracy seriously and pursue it vigorously.

The important caveat that every business should note is that the piracy does not have to be intentional in order for it to be punishable under the law. Whether the piracy is deliberate or not, it is still illegal. Purchasing software actually translates into the purchase of a right to use the software that was purchased within the confines of the law. Obviously, any software that is obtained illegally – either by you or someone within your employ (even if it was without your knowledge) – is pirated and the piracy is punishable under the law.

Another form of piracy is when companies or individuals who legally purchased software use it beyond the scope of the license. The license that accompanies every piece of software spells out how you may use that software within the law. Anything that is not specified as acceptable use or that falls outside of that which is deemed permissible is illegal and punishable by law.

The Software and Information Industry Association (SIIA), a trade association for the leading businesses that produce the software and information in today's digital economy, advocates legal and regulatory measures that protect its members' intellectual property. The SIIA also offers

<http://www.veriam.com>

advice to businesses who want to steer clear of inadvertently engaging in software piracy by listing “The Ten Commandments of Software Use:”

1. Thou Shalt Not Pirate Software.
2. Thou Shalt Not Buy Software From Auction Sites
3. Thou Shalt Not Install More Software Programs Onto Company Computers Than The Company Has Licenses To Use.
4. Thou Shalt Not Buy OEM or Back-Up Software.
5. Thou Shalt Not Buy Software Being Sold As ‘Academic Version’ Or “Not For Resale.”
6. Thou Shalt Not Buy Software From Someone Who Warns You Not To Register The Software.
7. Thou Shalt Not Make Proprietary Software Available On Peer-to-Peer Networks.
8. Thou Shalt Not Take Software Owned By Your Company And Install It On Your Home Computer.
9. Thou Shalt Not Copy Your Friend's Software.
10. Thou Shalt Report Software Piracy To SIIA By Calling SIIA’s Anti-Piracy Hotline At (800) 388-7478 Or Filing A Report With SIIA At [www.SIIA.net](http://www.siiia.net). (<http://www.siiia.net/piracy/education.asp>).

CONSUMER’S PERSPECTIVE

Representing the consumer’s perspective, and the fact that many individuals and businesses are fed up with what appears to be an unfair battle, is Charlotte Observer columnist John McBride. He contends, “those turgid contracts we “agree” to when we install software -- are completely out of control,,” and he is not alone in his point of view. He points to the following examples:

- The Microsoft Windows XP EULA gives Microsoft the right to download to your computer data from other, unnamed companies without telling you.
- The Google Toolbar EULA says that you -- not Google -- are responsible if anything goes wrong on your computer after using the Google Toolbar.
- Apple's iTunes EULA -- like many others -- gives Apple the right to change the terms of the EULA at any time without notice.

Mr. McBride proposes eliminating all EULAs that do more than protect copyright. And he is equally miffed about the fact that almost all software is licensed, not sold. As he puts it, in his idealized world, “You can't tell me what to do with your software after I buy it. You can't tell me I can't uninstall it. You can't change it without telling me. We own the software we buy. We own the hardware we buy. Most importantly, we own our data.” McBride, John, “5 new rules from new ruler of technology,” *The Charlotte Observer*, June 18, 2006.

Although Mr. McBride expresses an opinion shared by many consumers and although his alternative rules depict some of the injustices inherent in the rules currently governing software piracy, the fact is that you must abide by those that actually exist. Just as ignorance of the law is not an excuse nor is ignorance of the piracy in question (if, in fact, someone in your company committed the piracy without your knowledge or consent), a general agreement that the law is onerous or unfair will not protect you.

PROOF OF LICENSE

What Constitutes Proof of License?

A software product license grants you – either as an individual or as a business entity – the right to run or access a particular software program. A license agreement can take many forms but it generally governs the use of licensed software, allowing it to run on a limited number of computers and sometimes providing for additional backup copies to be made.

The type of licensing offered varies depending on the software company behind it and the needs of the user. For instance, Microsoft offers a number of licensing options depending on the size of the organization requiring the licenses, such as Volume License Programs for companies with 250 or more PCs or Full Packaged Product (FPP) or Retail Products for personal use or instances where only a few licenses are needed.

Generally, every unit of software comes with its own type of media and/or documentation that serves as its proof of license. The requirements for proving license ownership, however, also vary depending on the type of software purchased and the maker of the software.

Listed below are some guidelines and anti-piracy measures taken by some of the major players in IT software: Microsoft; Hewlett-Packard; SAP; Oracle; CA; McAfee and Norton. There are overlaps in what each software publisher requires but there are many variations as well. As highlighted below, there are as many nuances to what constitutes proof of license as there are software publishers, product and audiences for those products.

Microsoft requires the following in order to establish and prove license ownership of its pre-installed (OEM) software:

- The End User License Agreement (EULA) – this is the agreement between the PC manufacturer and the purchaser;
- The Certificate of Authenticity (COA);
- Original media and manuals (if applicable);
- The purchase invoice and/or receipt

Hewlett-Packard, on the other hand, requires only one original version of any one of the following as proof of an HP software license:

- HP Invoice listing software license;
- HP-UX and MPE-iX License Certificate;
- HP Support Agreement
- Software License Transfer Authorization;
- Authorized Reseller Invoice of Sale.

All of the items listed above should be kept on file and be documented and accessible for possible audits and when proof of license ownership is required.

Oracle's documentation is either shipped with the programs, or documentation may be accessed online at <http://otn.oracle.com/docs>. The terms of agreements explicitly state that Oracle "retain[s] all ownership and intellectual property rights in the programs. You may make a sufficient number of copies of the programs for the licensed use and one copy of the programs for backup purposes." Oracle also makes clear that it has the right to audit its customers' use of the programs.

Oracle warns its users that "much of the Oracle software sold through online auctions is pirated or otherwise unauthorized." The Oracle website cautions that pirated Oracle software, in addition to being sold (and, by default, purchased/owned) illegally, is also more likely to contain bugs, viruses or other errors that could cause serious damage to the user's computer system.

SAP distinguishes among both its products and its users in its licensing requirements. SAP products are either available as stand-alone products (CRM, SCM, SRM, PLM etc.) or as a solution suite (mySAP Business Suite). The customer licenses SAP solutions or the SAP Business Suite for a pre-defined number of named users per user category and software product. Any individual accessing SAP software must be licensed as a named user.

The SAP website provides the following terms and definitions:

- **Developer User:** licensed user who uses the development and administration tools provided with the software for the purpose of modifying, deploying and managing ERP or 3rd party applications or for the purpose of creating, modifying, deploying and managing custom developed applications. This is an SAP standard user type.
- **Professional User:** licensed user who performs operational related roles supported by the software. This is an SAP standard user type.
- **Limited Professional User:** licensed user who performs limited operational related roles supported by the software. In particular, employees of business partners are to be licensed as Limited Professional Users. This is an SAP standard user type.
- **Employee User:** licensed user who performs employee self-service related (non-job specific) roles supported by the software. This is an SAP standard user type.
- **DoD User:** licensed user type available for customers licensing SAP software via the SAP ESA. It is defined as a named user who has the rights of a Professional User as defined in the GSA Contract plus transfer rights as defined in the SAP ESA.

McAfee touts its System Protection Solutions and Network Protection Solutions portfolios as excellent tools to assure that "the technology that powers your business are security [sic] and available – from the desktop to the network core, and across the servers that you rely on to deliver your competitive advantage." It warns, however, that while it is committed to educating its authorized users, it will not hesitate to bring those violating McAfee licenses into compliance. McAfee has a program to help get its users into compliance but it requires the company/user in question to contact McAfee proactively and seek assistance before McAfee learns of the alleged piracy through other channels. It is only if McAfee is contacted first that it will work cooperatively with the company rather than pursue legal channels.

The license agreement for **Norton Anti-Virus 2006**, after delineating the user's basic rights, provides the following prohibitions on use, any of which would constitute a violation of the license agreement:

The user may not:

- A. copy the printed documentation that accompanies the Software;
- B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
- D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
- F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;
- G. use the Software in any manner not authorized by this license; nor
- H. use the Software in any manner that contradicts any additional restrictions set forth below.

CA (formerly Computer Associates) is bound to be even more stringent with licensing conditions and piracy pursuits having recently grappled with the toppling of its chief executive due to a fraud case. (*CA Inc. scoops up maker of software for managing data* by James Bernstein, www.newsday.com/business, June 16, 2006.) CA's master file license agreement, available on its website, provides a standard two-year term at which point CA has the right to refuse to renew the license agreement if any of the conditions were not met. CA also reserves the right to periodically audit each licensee's performance under the license agreement. CA notes that it will pay for the audit unless it determines that the licensee has underpaid for its CA software by 5% or more, in which case the licensee will have to pay for the cost of the audit as well as any additional amounts owed to CA as determined by the audit.

Most license agreements are available online at the publisher's website or are included with the products at the time of purchase. Navigating their terms and restrictions, however, is often an exercise in both futility and frustration. As evidenced by the many variations listed above, one cannot assume that what qualifies as proof of license for one software publisher will suffice for another. Similarly, what is acceptable usage of the software for one publisher might constitute unauthorized usage for another. These variations depend not only on the software publisher at issue and the type of software being used, but on the user as well.

The advent of shrinkwrap licensing agreements:

Hewlett-Packard's website notes that, for shrink-wrap licenses, "the original license Agreement is accepted as proof of a software license for HP's shrink-wrap license agreements. For these products, the holder of the shrink-wrap license is considered to be the licensee provided the shrink-wrap license agreement was acquired through legal means."

The advent of shrink-wrap licensing agreements has generated legal questions, as Apik Minassian notes in “The Death of Copyright: Enforceability of Shrink-wrap Licensing Agreements,” 45 UCLA L. Rev. 569.

“The mass marketing of computer software has induced software producers and vendors to replace negotiated contracts with shrink-wrap licensing agreements. Although these licenses were initially considered to be unenforceable contracts, the modern trend has been to enforce the licenses as valid contracts under the UCC.” (The UCC refers to the Uniform Commercial Code, which is legislation passed by Congress and adopted in every state to govern all commercial transactions.) “With the development of on-line software distribution and the new direction taken in the proposed revision of Article 2 of the UCC, the creation of shrink-wrap licensing agreements that are enforceable under state contract law has become relatively easy.”

No doubt additional case law will be written as traditional contract and copyright law struggles to catch up and encompass issues such as these, heretofore unimagined in the traditional world of binding written contracts. For now, legally purchasing a software program also binds you to the conditions printed on the shrink-wrap. What companies may not be aware of, however, is that simply clicking the “accept” button when purchasing/installing software online can constitute acceptance of the electronic version of the shrink-wrap license agreement. Clicking “I accept,” which one must do in order to continue with the purchase/installation, is the legal equivalent of signing a binding contract.

Why a License Matters:

When you purchase software, you are essentially entering a one-way contract. While few requirements are placed on the publisher, certain key restrictions are placed on you, the buyer, and these rules that make up the license are described in the documentation accompanying the software. As purchaser, you are not the owner of the copyright; that belongs to and remains the property of the software manufacturer. You are essentially purchasing the right to use the software – and even then, you are only doing so under certain conditions and with certain restrictions, all of which are imposed by the copyright owner (who is most often the software publisher).

These rules that make up the software license carry serious penalties for noncompliance. They often state that you have the right to load the software onto a single computer and make a single backup copy. Anything outside of the licensing agreement, such as making multiple copies or installing the software on more than the allotted number of computers, is an infringement of federal copyright law.

Auditing / Enforcement

The Key Players:

The software industry figured out early on that it needed strong intellectual property protections to ensure it was able to recover the considerable investment it made in the development of new products. Two organizations, the BSA and the SPA, are the primary license enforcement organizations. The SPA (Software Publisher's Association) was the original anti-piracy organization and was formed by many of the larger software publishers. It now operates as the anti-piracy arm of the SIIA (Software & Information Industry Association). The BSA, the more prominent organization of the two anti-piracy organizations, claims on its website that its goal is "promoting a safe and legal digital world." Suffer the consequences of one of its audits, however, and you might have a different take on its primary objective. According to Andrew Grygus, author of several online articles on Software Licensing, BSA operates essentially as Microsoft's private police force.

BSA and SPA Audits:

Random audits pose a very real and constant threat to any business using multiple computers and software programs/licenses. Anything less than total and complete compliance places your business at risk, and just how great that risk is will be described shortly.

Another source of licensing violation information is disgruntled employees who are no longer in a business's employ. According to Andrew Grygus, the BSA and SPA "advertise widely for disgruntled or discharged employees or others with a grudge. Their ads even imply turning you in is the honorable thing to do." He goes on to warn that even when it was the disgruntled employee himself who installed the unlicensed software and then blew the whistle on his unsuspecting employer, the employer is still liable. Computer dealers and system builders have also been known to turn in customers who have ordered computers without Windows or some other operating system pre-installed. (Grygus, Andrew. Software Licensing. www.aaxnet.com.)

What happens once an audit occurs:

Based on relatively minimal evidence, such as the report made by a former employee or the inability to produce documentation to support a claim of compliance, the BSA or the SPA (or a large software publisher, such as Microsoft) can trigger an audit. Most businesses comply because failure to do so could result in computers being seized or the business being shut down entirely while the case is resolved.

Possible Violations:

Even the most well-intentioned, law-abiding business is likely to have violations crop up during an audit. Some of the possible violations that can occur are as follows:

Inaccurate record keeping. Many businesses and organizations have been penalized tens of thousands of dollars for licenses they legally purchased but couldn't prove that they had done so. It is essential to keep accurate records and to maintain them in such a way that they are easily accessible.

Inability to Understand the terms of the License. The terms of the license can be complex, especially when dealing with a large business and a large software installation. A failure to understand what constitutes a violation of the license, even if adherence to the terms of the license was attempted in good faith, is not a legal excuse and will not diminish the consequences of the inadvertent violation.

- *Concurrent v. Non Concurrent Licenses:* While some software publishers offer concurrent licensing, Microsoft licenses are non concurrent. This means that you must purchase the number of licenses that match the number of operating computers in your business, even if they do not all run the software in question at the same time.
- *Transferable v. Non Transferable Licenses:* Some licenses (such as OEM Windows licenses that come with a new computer) are not transferable. This means that the license must be retired when that computer is no longer in use and cannot be transferred to a new computer. Similarly, if the computer is given to charity, Microsoft requires the removal of Windows before the donation of the computer.

Liability for Employees' Actions. Under the law, a company can be held liable for its employees' actions, even if the company's management was unaware of what the employee did (or failed to do, as the case may be). If an employee is installing unauthorized software copies on company computers or acquiring illegal software through the Internet or some other means, the company can be sued for copyright infringement even if it had no knowledge of the employee's actions. As mentioned earlier, the company can even suffer the extreme irony of being turned in to the BSA or SPA by the very employee who broke the law.

Penalties / Repercussions of Non-Compliance:

If your company is caught copying software, whether the copyright infringement is intentional or not, you may be held liable under both civil and criminal law.

According to BSA's website, the possible consequences are swift and severe:

“If the copyright owner brings a civil action against you, the owner can seek to stop you from using its software immediately and can also request monetary damages. The copyright owner may then choose between actual damages, which included the amount it has lost because of your infringement as well as any profits attributable to the infringement, and statutory damages, which can be as much as \$150,000 for each program copied. In addition, the government can criminally prosecute you for copyright infringement. If convicted, you can be fined up to \$250,000 or sentenced to jail for up to five years, or both.” www.bsa.org/usa/penalites.

Pirated software can also now result in Sarbanes-Oxley violations, which can translate into millions in fines and as much as 20 years in prison for executives. The Sarbanes-Oxley legislation, initially drafted to develop a stricter accounting standard for all business, applies to software asset management as well. The new standard of accountability and accuracy with respect to business records means that any business that cannot prove the entirety of its software was legally purchased will be assumed to be using pirated software and the full extent of the Sarbanes-Oxley penalties will apply.

Consider the example of the city of Virginia Beach, VA which was asked to answer a random audit demand by Microsoft in November 2000. Information services were practically shut down for over a month and the city eventually paid \$129,000 for missing licenses it may very well have purchased but simply couldn't produce the paperwork to prove that they had done so.

As noted by Joe Barr, a contributing editor at LinuxWorld.com, “even the small minority of organizations that can produce the requested inventory and matching proof of purchase are not

safe. They will still have to use time and effort to produce the paperwork, and their productivity will be negatively affected.” He estimates that a small firm with approximately 100 employees would be out of commission for two weeks and expend between \$4000 and \$8000 in additional labor costs to produce the information demanded of Virginia Beach, and that’s the cost if everything pans out. If anything is missing or undocumented, there is the additional cost of replacing missing licenses, and incurring the fines and penalties assessed by the BSA. (Barr, Joe. “Microsoft unleashes piracy police: Are you safe?,” LinuxWorld.com 12/8/00.)

The McAfee website warns consumers that civil penalties can be assessed in addition to the fines and possible prison terms stemming from criminal prosecutions. In civil cases, McAfee points out that it can obtain “its lost profits *plus* the infringer’s profits, or statutory damages of up to US\$150,000 per product. In addition, McAfee may seek to recover its attorneys’ fees.” As if that weren’t threatening enough, McAfee adds one final piece of cautionary advice. “As many companies know,” McAfee warns, “the press loves covering a company [that] has been forced to pay significant fines for having illegal software. Don’t be one of them.” www.mcafee.com.

Just ask any company forced to endure both the costs associated with an unforeseen audit of its software licensing and the resulting fines and penalties, and it will confirm that these costs add up quickly. A \$150,000 fine may not seem onerous to some companies, but keep in mind that the \$150,000 applies to *each* product for which proof of license cannot be documented and produced. For many businesses, even an audit that unearths only a small percentage of violations among its software inventory could result in fines in the millions.

CONCLUSION

It is essential to get licensure information in order now, on your own timetable, rather than scrambling in response to an unforeseen audit. As noted above, ignorance of the law or the conditions of the license agreement in question will not serve as an excuse for failure to comply with the terms in question. Make sure that IT information is well understood and that compliance is not simply taken for granted. Paying up front for expertise is a wise investment because the prophylactic cost pales in comparison to the penalties and lost work on the other end of the audit. All future purchases should be well documented and processed so that the licensure is organized and accessible

About the Author

Katya Lezin is a graduate of Brown University (BA in Psychology) and Georgetown University Law Center (JD and LLM in Advocacy). She is the published author of a nonfiction book on the death penalty (FINDING LIFE ON DEATH ROW by Northeastern University Press) and several law review articles.

All papers can be viewed and downloaded from the publication section of www.veriam.com.