Use of Licensed Software: Policy and Policy Analysis

by

Benjamin Tomhave

October 11, 2004

Prepared for:

Professor Daniel J. Ryan
EMSE 315
The George Washington University

This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources which I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____Benjamin L. Tomhave_____

Use of Licensed Software: Policy and Policy Analysis

by

Benjamin L. Tomhave

Abstract

This paper includes two main sections. In Part I, a policy is articulated on the use of licensed software within a commercial company ("the company"). The goal of the policy is to provide maximum coverage and minimal loopholes while being fair in its application and limitation of liability. In Part II, the policy is discussed in terms of its ethical, moral and legal implications. Part II also provides rationale for decisions made in the policy development process.

Table of Contents

Use of Licensed Software: Policy and Policy Analysis

by

Benjamin L. Tomhave

I.POLICY: USE OF LICENSED SOFTWARE[1][2][3][4]

All software must be used in accordance with its license as well as applicable federal, state and local laws. Use may include, but is not limited to, installation, copying, possession, distribution, redistribution or other methods for taking advantage of the work in its original or derived format. This policy applies to all persons accessing computer or network resources provided by the company. As a matter of practice, no software should be installed on company assets without proper authorization.

A.Definition of "Licensed Software"

All authors and publishers of software are protected by U.S. Copyright Law. Licensing use of that software is at the discretion of the author and publisher. These rights are afforded by the U.S. Constitution and subsequent Copyright Law (such as 17 U.S.C.). Unless the software is released into the public domain, it is subject to the licensing terms set forth by the author and/or publisher. All software should be handled under strict copyright restrictions until indication is given otherwise or until the copyright expires.

1.Commercially licensed software

Commercially licensed software is software that falls under traditional licensing models. Specifically, use of the software is contingent upon acceptance of a license and equates to paying a fee for use of the software. This fee and license acceptance occurs prior to the granting of permission for use. A common example would be shrink-wrapped software purchased through a retail outlet. Many commercial software packages will include an End User License Agreement (EULA) that details terms and conditions for use of the

---

[1] EDUCOM, *Information Policies: A Compilation of Position Statements, Principles, Statutes, and Other Pertinent Statements*. (Washington, DC: EDUCOM and ADAPSO, 1987, accessed 08 October 2004); available from http://www.cni.org/docs/EDUCOM.html; Internet.

[2] Information Security Policy and Disaster Recovery Associates, *Using Licensed Software*. (Cheshire, UK: Information Security Policy and Disaster Recovery Associates, accessed 08 October 2004; available from http://www.yourwindow.to/security-policies/ref040104.htm; Internet.

[3] Northwestern University, *Information Technology Policy: Use and Copying of Computer Software*. (Evanston, IL: Northwestern Univeristy Information Technology, June 2003, accessed 08 October 2004); available from http://www.it.northwestern.edu/policies/software.html; Internet.

[4] University of Pennsylvania, *Policy on Unauthorized Copying of Copyrighted Media*. (Philadelphia, PA: University of Pennsylvania Information Systems and Computing, <no date>, access 08 October 2004); available from http://www.upenn.edu/computing/policy/copyright.html; Internet.

software. Failure to comply with these license agreements may be a violation of federal, state and local laws.

In addition to use of the software, most commercially licensed software includes a certain level of user support. This support role is unique to commercial software in that the cost of the support is often included with the price of the software for at least an initial period of time.

It should be noted that some commercially license software can be obtained through a "site license" or a "bulk license." A site license is a single fee that an organization pays for unlimited use of the software directly on its computing assets. Similarly, a bulk license allows an organization to install more than one instance of the software under a single license. However, in contrast, a bulk license allows only a limited, predetermined number of instances of installation of the software.

2.Shareware licensed software

Software that is distributed under a shareware license may be installed without first paying a license fee. However, use of the software is still subject to the licensing set forth by the author or publisher. Oftentimes the author will allow the use of the software for a set period of time, after which it is required that the software be completely removed or that a license fee be paid. Paying the licensing fee may equate to receiving limited support, patches and upgrades for the software. The terms and conditions of use should be carefully read and understood prior to installing the software.

3.Open-source licensed software

Some software is provided for free use with limited or no direct support from the author. The author or publisher may choose to publish this software under a license, such as the GNU Public License.[5] The open-source licensing initiative has been created to protect the work of authors who do not wish to charge a licensing fee for their software, but who also do not wish to release their work into the public domain. The *Copyleft*[6] program provides free support to authors of software who wish to protect their works while offering them to the public for free without fear of having their works violated by commercial entities.

4.Software in the public domain

Software that has been released into the public domain by its author or publisher is considered free for use and copying. By making such a release, the author or publisher is officially waiving the rights afforded under copyright law.

*B.*Policy Enforcement and Limitation of Liability to the Company

[5] The GNU Public License (GPL) is available online at http://www.gnu.org/copyleft/gpl.html.
[6] The Copyleft program can be found on the web at http://www.gnu.org/copyleft/.

The company will take all reasonable measures to ensure that software provided for use with company assets is in compliance with the applicable license and laws. Any software that is not provided by the company, but is instead supplied by an individual, will be the sole responsibility of the individual. Any installation of software by an individual on company assets without explicit authorization is a violation of policy and will be subject to disciplinary review and action. Any installation of software by the company on company assets without proof of proper licensing should be refused by the employee and reported to management for immediate resolution.

1.Reporting violations or seeking clarification

All suspected violations of this policy must be reported to management or through the communication methods provided by the company. Failure to report knowledge of a suspected policy violation will itself be considered a violation subject to disciplinary review and action. It is the responsibility of all employees to help minimize risk to the company as a whole.

As a general practice, the rule of "when in doubt, ask first" should be followed when considering installation of software that may be subject to licensing, fees and copyright laws. All employees are responsible for seeking out and receiving explicit permission to install software not provided by default on company assets. The company will provide a method for submitting questions about the application of this policy in specific scenarios that are otherwise unclear.

2.Automated methods for license inventory and enforcement

The company will implement automated methods for monitoring company assets for the installation of software. These automated methods will assist the company in taking reasonable measures to ensure that violations do not occur. Disabling or tampering with these automated methods is strictly prohibited and may result in disciplinary action. These tools are intended strictly to monitor company assets for the confirmation of proper licensing and inventory of software. These tools are not intended as a method for "spying" on employees or to violate any privacy protections afforded employees.

3.Procedures for remediating violations

All potential violations will be considered through due process. Ownership for the violation will be determined and the need for disciplinary review and action will be addressed. If the company finds that it is in violation of this policy, immediate actions will be taken to bring the company into compliance. If the company finds that the violation is the result of individual actions that were not properly authorized, the individual or individuals directly responsible will be referred for disciplinary review.

*4.*Process for levying disciplinary action

Once a determination is made that a violation has occurred as a result of the actions of an individual or individuals, management will refer the matter to Human Resources for

consideration and action under the disciplinary plan. Disciplinary actions may include, but are not limited to, levying of fines, suspension or termination of employment. In all cases, the violating software must be either removed or brought into compliance immediately.

If a determination is made that the company caused the violation, the software in question will be immediately removed or licensed appropriately. The employee will not be held in direct responsibility for the violation, though the employee will be reminded of the inherent responsibility of all employees to vigilantly protect the company from unnecessary risk and liability.

II.ETHICAL, MORAL AND LEGAL IMPLICATIONS OF THE "USE OF LICENSED SOFTWARE" POLICY

The hierarchy of order, as established in class, is as follows: Ethics → Morals → Constitutions → Treaties → Legislative Law → Regulatory Law → Court Law → Standards. As a result of this taxonomy, the company policy would fall under the category of a Standard from a high-level perspective, which means that it is responsible for being aligned with the bodies of Law above it. To this end, the true ethical and moral questions here – in essence that of fairness and right vs. wrong – have already been decided and stipulated by higher authorities. The policy statement itself, then, does not have direct ethical or moral implications in the broad sense of the term.

However, this macro view overlooks the localized view within the company. Within a given organization a streamlined hierarchy also applies. In this sense, policies are ethical statements meant to articulate rules for expected behaviour. Ergo, the "Use of Licensed Software" policy does not only have ethical implications, it is a matter of ethics, particularly with respect to the proper application of the "fair use" doctrine contained within copyright law. Thus, the policy must serve a dual purpose of being aligned with the overall ethical framework set forth in laws, regulations, treaties, constitutions, et al., but also by setting the expectations for behaviour within the company's own environment.

In addition to being subject to higher ethics and setting ethical standards within the company, the implementation and enforcement of the policy also has ethical implications. Specifically, fair and consistent application of the rules, without discrimination, is an ethical problem. This problem is not addressed within the policy, but is instead addressed by other policies established by departments such as Human Resources or Professional Standards of Conduct. These are not matters of professional ethics (which are actually moral issues), but true ethical matters having to do with proper behaviour and application of morals. Therefore, there may be indirect ethical implications as a result of the implementation and application of the policy.

Besides these ethical questions, there are definite moral and legal implications for the policy. In terms of the moral implications, the policy must clearly light the path to the "proper" choice, creating consequences for making the "wrong" choice, and providing an open mechanism for assigning blame and resolving problems. In other words, the moral

implications are in ensuring that the policy not only clearly states the ethical guidance, but that the policy is easily and concisely translated into a course of behaviours whose actions are deemed proper. For those choices that are in contravention to the intended result of the policies, clearly defined rules for identification and mitigation of violations must be (and have been) specified.

From this standpoint, whereas the policy is like a law, the sections addressing violations and remediation of those violations speak to the moral issues. This approach equates to defining a justice system on the micro scale within the company in order to address questions and concerns. Whereas the policy does not contain specific "sentencing guidelines" for various degrees of violation, it does go so far as to highlight some of the options for punishing violations. Additionally, the loose definition of the punishments related to a violation offer the company an opportunity to first rehabilitate an offender before moving to a more severe form of punishment, such as termination of employment.

Finally, the legal implications to the policy are, perhaps, the most obvious piece of the puzzle. First, in the case of “Use of Licensed Software,” the legal requirements directly addressed concern copyright law, and specifically the “fair use” doctrine contained therein. Second, through the stipulation of monitoring company assets that are being used by employees, a concern exists in terms of privacy rights and laws. Third, the challenges of fairness and due process with respect to the treatment of employees are also addressed. Finally, the ultimate goal of the policy is to indemnify the company against liability that may be incurred through a display of wanton disregard for the law by an employee or even by the company itself.

A.Legal Implications: Copyright Law

Whereas copyright law creates provisions for the fair use of copyrighted materials, it also stipulates protections for authors of original work, entitling them to control of their creations. In the computer age, enforcement of these copyrights (and their subsequent licenses) becomes a significant challenge because tracking uses of software, copying of software, and reuse of software is a tremendously difficult task. In order to mitigate the risks associated with the transitive nature of digital media, copyright holders have set a precedent for tracking down major offenders (such as businesses with large deployments of unlicensed software) and extracting dues in recompense.

For this reason, the company is not only obligated to state in policy the expectation for use of properly licensed software, but it is also its responsibility to implement methods for detecting, reporting and resolving such violations. Thus, simply relying on employees to adhere intuitively to the policy and applicable laws is not adequate. This fact not only necessitates the creation of the policy, but puts responsibility onto the shoulders of the company to properly educate and train employees about the policy and its application. It is also the responsibility of the company to implement additional measures for monitoring and inventorying software installed on company assets, as well as establishing guidelines for quick and proper resolution of violations.

B.Legal Implications: Privacy

In order to protect themselves against litigation stemming from the installation of unlicensed software, businesses have taken it upon themselves to create and enforce policies prohibiting personnel from introducing unlicensed software into their environment. These measures are designed to limit the risk burden born by the company due to the actions of unauthorized individuals. For large organizations, this is a daunting challenge. As a result, it is necessary for the introduction of automated tools that "snoop" on company assets (such as personal workstations) to monitor and inventory installed software.

The monitoring of personal workstations introduces new concerns regarding employee privacy. Whereas employees will have agreed to policies sublimating their privacy to the needs of the company, it is still contingent upon the employer to ensure that employees are aware that no such expectation for privacy should realistically exist. Assuming that employees are aware of their limited rights within the workplace, the only other problem concerns the introduction of assets into the company environment that are not owned by the company. In those specific cases, additional indemnification must occur to transfer the responsibility of liability from the company to the non-company resource. Various measures, both technical and non-technical, should be pursued by the employer to limit the ability of employees to introduce non-company assets into the company's environment.

C.Legal Implications: Fairness and Due Process

The third legal implication from the policy does not result directly, but indirectly, and is applicable broadly to all policies and not just this specific policy. This implication has to do with the fair and consistent application of rules to all employees without discrimination. These rules must be applied to every employee in the company, regardless of title, race, gender, etc. If the policy is not applied fairly and consistently, then the legal issue of discrimination may arise. Whereas the question of fairness speaks to an ethical concern, it also speaks to legal concerns because the codes of law, to which this policy must be aligned and compatible, stipulate fair application of rules, such as within the business environment.

D.Legal Implications: Indemnification

Finally, the ultimate goal of this policy is to limit the amount of liability that can be attributed to the company should the presence of unlicensed software be detected by the license owner. Specifically, if a company can demonstrate that reasonable measures are being taken to enforce the policy and that the company is neither encouraging nor turning a blind eye toward illegal, prohibited behaviour, then the amount of responsibility assigned to the company should be much less than the level of responsibility for the violation assigned to the individual(s) who perpetrated the violation. This

indemnification is a necessary part of the overall risk management framework for an organization and is designed to minimize the overall exposure that requires defending.

There may also be occasion where the employee requires indemnification against the actions of the company that are in direct contradiction to the law. In this case, this policy also provides protections to the employee, limiting their responsibility, while also making it contingent upon them to identify violations and make them known to management immediately. Whereas it is not specifically stated, it should be noted that it is the responsibility of the employee to go outside the chain of command when necessary to help protect the company from risk when his/her direct management has no interest in resolving policy violations.

REFERENCES

1. Business Software Alliance, *Piracy and the Law*, Washington, DC: Business Software Alliance, accessed 08 October 2004; available from http://global.bsa.org/usa/antipiracy/law/; Internet.

2. EDUCOM, *Information Policies: A Compilation of Position Statements, Principles, Statutes, and Other Pertinent Statements*. Washington, DC: EDUCOM and ADAPSO, 1987, accessed 08 October 2004; available from http://www.cni.org/docs/EDUCOM.html; Internet.

3. Information Security Policy and Disaster Recovery Associates, *Using Licensed Software*. Cheshire, UK: Information Security Policy and Disaster Recovery Associates, accessed 08 October 2004; available from http://www.yourwindow.to/security-policies/ref040104.htm; Internet.

4. Northwestern University, *Information Technology Policy: Use and Copying of Computer Software*. Evanston, IL: Northwestern Univeristy Information Technology, June 2003, accessed 08 October 2004; available from http://www.it.northwestern.edu/policies/software.html; Internet.

5. University of Pennsylvania, *Policy on Unauthorized Copying of Copyrighted Media*. Philadelphia, PA: University of Pennsylvania Information Systems and Computing, <no date>, access 08 October 2004; available from http://www.upenn.edu/computing/policy/copyright.html; Internet.