

Protecting Intellectual Property Rights through Information Policy

In today's electronic world, an organization's intellectual property is sometimes its biggest asset. Much time and money can be saved, and frustration and litigation avoided if company policy dictates ownership and use of intellectual property.

By Karthik Raman

The advent of the Internet has revolutionized the way information is exchanged between people. Few other tools have changed our perceptions about quick access to information as the Internet has. However, the spread of computing and the Internet have made it difficult to apply traditional intellectual property laws. Despite popular belief, just because it's easy to distribute information using the Internet does not mean that it's right to do so.

In this paper I argue that writing corporate policy protecting intellectual property rights is essential for many reasons.

First I define intellectual property. Next, I explain why corporate security policy is central to information assurance within an organization. Then I survey computing policy at a few institutions of higher education and examine their efforts to protect intellectual property rights through computing policy. Next, I examine violations of intellectual property rights using examples from academia and business. Finally, I present some methods for protecting intellectual property rights through computing policy.

Intellectual Property

Intellectual Property (IP) is defined as any "original creative work manifested in a tangible form that can be legally protected" [1]. When we speak of IP rights, we refer to controlling the way IP is used, accessed or distributed [2]. The World Intellectual Property Organization (WIPO), an organ of the United Nations, suggests laws to enforce IP rights worldwide. The convention establishing the WIPO concluded on July 14, 1967 that [3]:

"Intellectual property shall include rights relating to:

- * literary, artistic and scientific works,
- * performances of performing artists, phonograms and broadcasts,
- * inventions in all fields of human endeavor,
- * scientific discoveries,
- * industrial designs,
- * trademarks, service marks and commercial names and designation,
- * protection against unfair competition, and all other rights relating to intellectual activity in the industrial, scientific, literary or artistic fields."

IP is divided into two categories:

- a) Industrial Property - patents, trademarks and industrial designs.
- b) Copyright - includes works of art, literature, music and more recently computer programs [4].

Why IP Rights Should Be Protected: The Classic Argument

One reason for IP laws is to allow IP creators to benefit from their work [5]. If artists create paintings after months of labor, then they deserve credit for painting them and the income from selling or exhibiting them. If a business comes up with an attractive marketing logo, then no other businesses should be allowed to use that logo to promote their own products without permission.

Protecting IP is also seen as a method of promoting creativity [6]. If no one is allowed to copy another person's work without permission then creativity is encouraged for everybody.

A flyer on IP rights protection published by Los Alamos National Laboratories, one of the premier research facilities in the nation, notes the financial value of intellectual property accrued from licenses and patents as a reason to protect IP rights [7].

IP Protection in the United States

In the United States, IP rights are protected by:

a) Industrial property

- * Patents - United States Code, Title 35
- * Trademarks - United States Code, Title 15
- * Industrial designs - As above, under Patents

b) Copyright and related rights

- * Copyright - United States Code, Title 17, the Digital Millennium Copyright Act (DMCA)
- * Related rights - As above, under Copyright

c) Other

- * Design protection - Vessel Hull Design Protection Act
- * Computer programs - Semiconductor Chip Protection Act of 1984
- * Plant variety protection - United States Code, Title 7

In addition to these laws, the US abides by WIPO and other international treaties relating to IP rights [9].

It is important to note that copyright is a time-limited right. This means that the rights to any copyrighted work pass into the public domain after a period of time specified by law. Currently in the US, works produced after January 1, 1978 are protected during the author's lifetime and for a period of 70 years after his/her death. For works created before January 1, 1978, the period of protection varies [10].

Copyright in the Electronic World

In "Cyberspace Law for Non-Lawyers", Larry Lessig, David Post and Eugene Volokh state that the copyright law applies in the electronic world as in the physical world. Therefore, they argue that "copying something in cyberspace can be just as much an infringement -- assuming the copyright owner doesn't allow you to do it -- as copying something on paper" [11]. The assumption that anything on the Web is free to take is plain wrong.

Copyright laws have protected the rights of book authors and publishers, and in this electronic age, new laws like the Digital Millennium Copyright Act (DMCA) have been introduced to protect the rights of digital media [12]. A related law, the Technology, Education, and

Copyright Harmonization (TEACH) Act, addresses the issue of copyright in the digital classroom [13].

Computing and Security Policy

Policy

The Merriam-Webster Dictionary defines policy as, "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions" [14]. In an organization, "policy is the rules and regulations set ... " [15]. It is important to note the difference between policy and procedure because these terms are often used imprecisely. Whereas policy is a set of rules reflecting the organization's beliefs, procedure outlines how people should act policy out.

Every organization that depends on computers should have a computing policy. At the most basic level, a computing policy can be the acceptable usage policy that lists the dos and don'ts of computer and network usage.

Computer Security Policy

Computer security policy is a subset of an organization's computing policy. It must seek to preserve the six security fundamentals -- confidentiality, integrity, authenticity, availability, utility and possession of your organization's information.

When you develop policy, make sure that you do not repeat work that has already been done. Unless you are told to start from scratch, or your organization has never had a computing policy, refer to the organization's existing policy documents before development.

Policy Resources

For an introduction to security policy, refer to these white papers from SANS:

* Jarmon, David. "A Preparation Guide to Information Security Policies."

Available at <<http://www.sans.org/rr/papers/index.php?id=503>>

* Guel, Michele D. "A Short Primer For Developing Security Policies"

Available at <http://www.sans.org/resources/policies/Policy_Primer.pdf>

* Kaleewoun, Philip J. II "An Overview of Corporate Computer User Policy"

Available at <<http://www.sans.org/rr/papers/50/535.pdf>>

It is a good idea to use Internet resources if you are starting from scratch [16,17].

Resources on policy development:

* "Site Security Handbook", from the Internet Engineering Task Force

<<http://www.ietf.org/rfc/rfc2196.txt?Number=2196>> can be used as a template

* Charles Cresson Wood's *Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies* (Version 8. Houston, TX: Pentasafe Security Technologies, 2001).

Wood justifies each policy template.

* Tom Peltier's *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management* (Auerbach, October 2001).

* "Security Policy Guidelines" by M.E. Kabay in the *Computer Security Handbook*, 4th ed. (New York: John Wiley & Sons, Inc., 2002). A review of strategies for effective policy writing.

Survey of Computing Policy in Academia

IP Rights Protection in the Higher Education Environment

In an academic institution, respect for IP rights is central to the spirit of learning and teaching [18]. Intellectual property is no longer physical materials alone; therefore, respect for IP rights must extend to software and Web-based materials.

Many colleges and universities are members of Educause, a "nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology" [19]. In a directive titled, "Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community," Educause dictates academic institutions' responsibility in preserving the IP rights of information [20]:

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the

right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

My surveys will show that to a large extent colleges have made an effort to incorporate the principles of this directive in their computing policy. For example, Georgia Institute of Technology's computer and network usage policy Webpage contains the above lines from the EDUCOM code [21]. During Napster's heyday, when the legalities of file-sharing were being debated, Georgia Tech was among schools not blocking Napster [22]. Exhibiting the EDUCOM code is an indication that Georgia Tech has reversed its stance on blocking Napster. This adds to the argument that policy cannot be rigid -- it must be reviewed regularly and updated to reflect the changing information landscape.

IP Rights Protection in Computing Policies in US Colleges

IP Rights Protection Initiative

Carnegie-Mellon University has distinct policies for computing, copyright and other IP. The policy indicates compliance with US Copyright Law as the reason for policy creating. The section on IP defines who owns IP created at Carnegie-Mellon [23].

John-Hopkins University indicates compliance with the Digital Millennium Copyright Act (DMCA) as the reason for creating their copyright policy [24].

Some colleges defined IP Rights Protection in their acceptable usage policy. For example, Bucknell University lists copyright protection in computer acceptable usage policy section on ethics [25]:

Do not violate copyright laws. This includes using Bucknell computing facilities and resources to receive, retransmit, duplicate, destroy, or tamper with software or data, whether stored or transmitted, unless authorized by copyright, license, university policy, and all other applicable laws. Examples of protected materials include written

material, sound files, pictures, photos, animations, and software not originally created by you.

Bucknell University's initiative to protect IP rights is demonstrated through a circular to its community titled, "Do you know that most music and movie sharing is illegal? Are you aware of the risks you are taking when you do this?" [26] In this message, downloading copyrighted music illegally using peer-to-peer programs is discouraged.

The University of Chicago has a similar circular to its community titled, "Unlicensed distribution of copyrighted materials" in which compliance with government copyright laws and other federal laws is outlined as a reason to stop using peer-to-peer software [27].

Cornell University articulates similar reasoning in their "Responsible Use Of Electronic Communications" document [28]:

The university seeks to enforce its policies regarding harassment and the safety of individuals; to protect the university against seriously damaging or legal consequences; to prevent the posting of proprietary software or the posting of electronic copies of literary works in disregard of copyright restrictions or contractual obligations; to safeguard the integrity of computers, networks, and data, either at Cornell or elsewhere; and to ensure that use of electronic communications complies with the provisions of the Campus Code of Conduct for maintaining public order or the educational environment.

The Chicago Loyola University asks users to not use peer-to-peer software for fear of copyright violation and because those programs suck up network bandwidth. Users can explore the college's policy documents from this Webpage [29].

IP Rights Protection Measures Illustrations

It is not enough to publish policy documents and not explain them. Employees and users will forget policy easily if the justification for policy and punishments for policy violation are not explained close to the actual policy document.

A few colleges whose computing policies I surveyed went beyond publishing policy and outlined punishments and internal college procedure for policy violations.

Brown University's computing policy shows the college's awareness of the legal issues connected with downloading illegal music and video files. After explaining the context of this policy document -- compliance with federal laws such as the DMCA -- the issues related to downloading illegal MP3 files using peer-to-peer software are articulated in a question-answer format. Questions like, "Specifically, is sharing and downloading MP3 files and videos illegal?" and "How do you get caught violating copyright law?" lead to "If the IP address leads to my computer, what happens next?" The answer to this last question outlines disciplinary procedures for a student or staff member getting caught for downloading music the first time, second time, and later [30].

Baylor University's policy on backups is an example of a thoughtful technical IP right protection measure. This policy selectively excludes "digital multimedia files such as MP3's" from being backed up from student machines onto the university's server. It is possible, if necessary, to get around this technical measure: if a student has created his/her own content, and wants those files backed up, then the network administrator can arrange it [31].

Enforcing the use of a fair-use checklist document in computing policy is a sound non-technical measure to preserve IP rights. The Copyright Management Center of Indiana University and Purdue University provides a Fair Use checklist form for students and faculty to document all the works they cite or derive from. This document is available at <http://www.copyright.iupui.edu/checklist.pdf>.

Examples of Copyright Protection Policies

Yale University's copyright policy provision is [32]:

Users must observe intellectual property rights including, in particular, copyright laws as they apply to software and electronic forms of information.

Bucknell University statement on appropriate use of university resources focuses on digital media sharing [33]:

Most commercially produced music and movies are copyrighted and cannot be freely shared. This is the law.

Bucknell does not examine the information content that is being transmitted (e.g., the music itself) but does monitor the type of information (e.g., that is an MP3 file) in order for us to give priority to academic uses of our network. Members of our community must follow university-defined policies for appropriate use of technology resources.

The California State University at Chico's policy covers both plagiarism and file-sharing [34]:

Academic Honesty. Users must respect the intellectual property of others and adhere to University standards of academic honesty. Examples of academic dishonesty include accessing or using the files of others without their permission, altering or destroying their files or messages, violating standard citation requirements for information accessible electronically, or using copyrighted software in violation of the copyright agreement.

Dartmouth University's policy on copyright covers Fair Use and peer-to-peer file sharing [35]. Its statement on IP rights is [36]:

No member of the community shall use another's content or property in a way that violates copyright law or infringes upon the rights held by others. The unauthorized duplication or use of any software that is licensed or protected by copyright may constitute violations of civil and criminal law, and is prohibited by this policy.

The Necessity for IP Rights Protection in Policy

Vint Cerf, WorldCom Senior VP and one of the pioneers of the Internet feels that "[P]olicy problems are harder to solve, and probably more important than the technology ones. Policy doesn't have a simple answer ..." [37].

Time Warner CEO Richard Parsons spoke of impact of Napster being shut down as follows [38]:

"I think this is a very profound moment historically. This isn't just about a bunch of kids stealing music. It's about an assault on everything that constitutes the cultural expression of our society. If we fail to protect and preserve our intellectual property system, the culture will atrophy. And corporations won't be the only ones hurt. Artists will have no incentive to create. Worst case scenario: The country will end up in a sort of cultural Dark Ages."

When summed up, the above statements stress the importance of protecting IP rights and having good information policy. The following case studies illustrate some reasons for protecting IP rights through policy.

Dangers from Popular File-Sharing Software

Illegal music- and file-sharing are items of concern at almost every college campus across the continent. The phenomenon of downloading MP3 files took root with Napster. After Napster was shut down, services like Kazaa, Grokster and Gnutella took its place.

Researchers of the music-sharing phenomenon in colleges have made the point that using peer-to-peer software by itself is not illegal; however, using the software to download copyrighted materials without permission is [39].

In a white paper titled, "Peer-to-Peer File-Sharing Networks: Security Risks" from the SANS Institute, William Couch discusses the technical risks associated with using file-sharing networks such as Kazaa, Grokster and Morpheus [40]. Couch observes that users and employees will use such tools from a "because it's there" mentality, without giving much thought to the issues and consequences to themselves and their organization. Ordinary users do not realize that using peer-to-peer software is fraught with threats to computer security.

Threat of Viruses/ Trojan Horses

No one monitors peer-to-peer networks because they are, by definition, decentralized [41]. The file-sharing program Kazaa's Website acknowledges the threat of malicious code spreading using their software [42]:

Most files that are accessible using Kazaa Media Desktop originate from other users.

This means that there will always be the risk of irresponsible users introducing viruses.

William Couch expands on this threat in his paper. He notes that an attacker could spoof the address of a peer-to-peer client, hijack a session, and insert malicious code into a user's computer [43].

Being Hacked by the RIAA

Consider this scenario: one of your employees uses Kazaa to download the latest Britney Spears song. The Recording Industry Association of America (RIAA) traces his/her IP address to your organization's network. Depending on your network's configuration, it might even be possible for the RIAA to pin down the IP address of the employee who downloaded the song. The RIAA discovers that your employee's computer was a super-node that uploaded and downloaded thousands of MP3s every day, so they hack into your network trying to down the super-node. They manage to crash the super-node, but in the process they also down 200 production machines (or laboratory computers).

Although the RIAA's right to engage in such hacking has been debated in court, the danger of losing the availability and utility of your systems from being hacked by them is very real [44].

Threat of Lawsuits

In a paper titled, "Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks", researchers for the Joint Committee of the Higher Education and Entertainment Communities discuss ways in which US copyright laws are violated by peer-to-peer file sharing. In addition to copyright infringement, they say file sharing raises issues in anti-bootlegging, electronic theft and trademark laws [45].

The recent string of lawsuits against individuals shows us the RIAA's readiness in using scare tactics to dissuade file-sharers from downloading music illegally. It does not take a leap of the imagination to think that organizations could be targeted next if so many laws are potentially being violated by file-sharing.

Legal Requirements

Copyright Laws

The above section on the threat of lawsuits points to a good resource on copyright law in the context of computing policy [46]. The US government's Website on copyright law is an obvious other resource [47].

With business interactions becoming increasingly international, the new European Digital Copyright Laws are worth paying attention to as well [48].

Software Piracy

The Business Software Alliance (BSA) is a consortium of the biggest software manufacturers in the world, with programs in more than 60 countries. The BSA "educates consumers on software management and copyright protection, cyber security, trade, e-commerce and other Internet-related issues" [49]. It also works with government to set punishments for creating and using illegal software.

A study by the BSA in 2000 found that close to 37 percent of all business software worldwide was pirated [50]. With software piracy being widespread, it is expected that punishments for violations will be harsh. In a flyer titled, "Software Piracy and the Law" the BSA outlines the punishments for pirating software as follows [51]:

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 choose between actual damages, which includes 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.

In recent years, one of the biggest cases of software piracy occurred in August 1998 when the BSA found 1,400 illegal copies of software in use in the Los Angeles School District. The cost of replacing software or purchasing licenses was reported to be approximately \$5 million [52].

To an organization, the cost of replacing illegal software is staggering, and the financial drain of lawsuits from software piracy can be devastating. Furthermore, a lawsuit against a high-profile company portends losses in partner trust and company reputation. Lesson to take: make it clear in your information policy that illegal or pirated software is not allowed on your organization's systems.

Other Legal Requirements

Security vendor Symantec lists a set of computing-related laws that an organization should comply with (as it pitches for its security management products) at <http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html>. Not all these laws pertain to IP rights protection, however.

Defining the Scope of IP Created In-House

In today's electronic world, an organization's intellectual property is sometimes its biggest asset [53]. So far, the discussion has focused on protecting IP not owned by one's organization; it is as important to protect an organization's own intellectual property through policy.

Patents, Trademarks, Trade Secrets

Industrial espionage, theft, and disputes with employees are ways by which IP rights produced in-house can be compromised.

On May 5, 1997, the *Wall Street Journal* reported that Novell Inc. was suing three of its former employees for stealing "technology they helped develop while Novell employees" [55]. This lawsuit eventually prevented Wolf Mountain, the new company formed by the three ex-Novell employees, from using "source code authored during their employment" [56].

Programmer Evan Brown signed an agreement with his employer DSC Communications of Plano, Texas ten years before being fired in 1997 that gave the company "all ideas related to DSC's line of business." Brown then refused to reveal how to "automatically convert old software code into newer languages", for which he was sued by DSC57. As of this writing, this lawsuit is still pending in the Texas 5th Court of Appeals at Dallas [58].

On August 6, 2000, *The Washington Post* reported that Qwest sued AT&T over AT&T's threat to prevent one of its employees from "leaving it to work for Qwest" over fears that the employee might carry with him "AT&T's confidential information or trade secrets" [59].

The above cases hint at the importance of IP rights preservation. Surely much time and money can be saved, and frustration and litigation avoided if company policy dictated ownership of intellectual property.

E-Mail Ownership

E-mail is a company resource. It is not an employee right; rather e-mail is a privilege and a service provided by the organization. Your computing policy should have provisions defining acceptable e-mail use. Policy should also define disciplinary actions for e-mail abuse.

A report from Edupage dated February 2, 1998 read [60]:

A Florida circuit court judge has been asked to decide whether 200 e-mail messages taken by an employee from her former employer contain proprietary information that should be protected. The employer is American Family Publishers, the magazine sweepstakes company represented by celebrities Ed McMahon and Dick Clark, which is being accused of alleged deceptive sales practices.

In the week of March 31, 2003, Intel and ex-Intel employee Ken Hamidi were fighting over the usage of Intel's e-mail resources. Intel was unhappy that Hamidi kept sending massive volumes of e-mail critical of Intel to close to 30,000 Intel employees. Intel spokesperson Tracy Koon stated her company's stance as [61]:

Ken has been very persistent and creative in exercising his right to speak out. But our view is that, in exercising his rights to free speech he needs to protect the property rights of Intel, including our e-mail system.

Cases like those above can be avoided by defining ownership and status of e-mail in the company's policy. Corporate America seems to be gaining awareness of this need: in a study for *Information Week* magazine in February 2000, Thomas York found that across America,

companies are making clear that e-mail is company property [62]. I only hope this clarification is first codified in policy documents so that disputes cannot arise later.

Suggestions

In the words of Gary Webb, a policy developer at Los Alamos National Laboratories, "[P]olicy needs to be written and current in order to be effective" [63]. It is not sufficient to write policy and expect employee understanding and compliance -- employees should be educated on policy and tested regularly on it. In addition, policy itself needs employee involvement during development, and updating as technology, laws and the business environment change. An organization cannot afford for policy to become shelf-ware.

Technical Policy Enforcement Measures

Good Network Administration

Practicing good network administration is a prerequisite to any technical policy enforcement step. Watchful network administration will reduce occurrences of illegal file-sharing or of installing pirated software. Los Alamos National Laboratories has an Electronic Software Distribution (ESD) system that helps reduce usage of illegal software. This ESD has many software packages fully licensed and available to authorized users, and allows users to make requests for new software. In addition, it "tracks licenses and gives software companies a single point of contact for their sales" [64].

Methods to block peer-to-peer software are discussed in the next section.

Usage and Network Monitoring

The Washington Post reported on June 12, 2001 that AltaVista had created new software that would allow businesses to scan network machines, employee e-mail accounts and personal computers [65]. If the privacy issues in scanning employee e-mail can be resolved (through policy, possibly), then such scanning software will help locate suspicious IP on employee machines. The class of such usage monitoring software is called Employee Internet Management (EIM). EIM recently became a half-a-billion dollar industry [66].

Some efforts to block peer-to-peer software at universities have been successful. The University of Florida enforces its computing policy using a tool called ICARUS [67]. Repeat offenders caught by ICARUS face judicial proceedings at the university.

Norwich University employs a tool called Packeteer that analyzes network packets at the application layer and "discovers and tracks P2P applications like KaZaA, Morpheus, Gnutella, iMesh, and AudioGalaxy" [68, 69.] Punishments for offenders caught through Packeteer will be worked into Norwich University's computing policy during the summer of 2004 [70].

Non-Technical Policy Enforcement Measures

In "Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks", the researchers make the point that colleges are not obliged to protect students if they break the law [71]. This observation can be extended to businesses and employees. Nevertheless, it makes sense for an organization to educate its users of computing policy and test them for awareness.

User Involvement in Policy Development

In "Intellectual Property Ownership in Distributed Learning", Sara Ulnius, the Online Learning Coordinator for Michigan's Center for Professional Development recommends for a university to work with faculty to define ownership of IP produced [72]. In "The Use of Case Law in Negotiating the Acceptance of Post Secondary Computer Policies", George B. Koszegi's methodology for the development of acceptable use policies -- working with employees all through policy development -- echoes Sara Ulnius's recommendations.

User Education and Testing

The University of Virginia activates network accounts only after students pass a quiz about responsible computing [73]. Their video in which innocent-looking children boast violations of computing policies is both funny and piquant. This would be great educational video to educate employees with [74].

The University of Wisconsin-Madison's poster on copyright infringement is an example of a good policy dissemination tool [75].

Perhaps one of the best times to educate students about computing policies is when they first arrive on campus. Norwich University, University of Maryland and West Virginia Wesleyan College all have a segment on IP property rights issues during their freshman orientation [76,77]. Similarly, employee policy education should begin immediately after hiring.

Peer-to-Peer Software Deactivation Procedure

The University of Chicago outlines steps to deactivate the most popular peer-to-peer software programs on its computing policy website [78]. These instructions can form the beginnings of your IP rights protection procedure document.

Summary

- * The Internet has made information exchange easier.
- * Laws in cyberspace are still taking shape, but traditional laws such as copyright are relevant in the electronic world.
- * Intellectual property, which includes copyright and industrial property, is any "original creative work manifested in a tangible form that can be legally protected".
- * The classic argument to preserve IP rights is to let the creator benefit financially and to promote creativity.
- * The DMCA and TEACH are extensions of IP law in cyberspace.
- * Policy reflects your organization's beliefs.
- * Computer security policy must seek to preserve the six security fundamentals of your organization's information.
- * As institutions of learning, colleges and universities should seek to preserve IP rights.
- * Refer to policy documents available online already.
- * Publish your policies and explain them.
- * Using peer-to-peer software threatens your organization's computer security.
- * In policy, seek compliance with IP (and other) laws.
- * Prevent software piracy through policy.
- * Preserve the rights of in-house IP through policy.
- * Define ownership of e-mail in policy.
- * Review IP rights protection policies and keep them current.

- * Use policy to dictate good network administration and using usage monitoring and network analysis software to preserve IP rights.
- * Involve users in policy development.
- * Constantly educate and test users on policy knowledge.
- * Create a procedures document to define user behavior to protect IP rights. Start it by mandating peer-to-peer software deactivation by users.

References

- 1 Defined in <<http://www.wipo.org/about-ip/en/iprm/pdf/ch1.pdf>>
- 2 See: <<http://www.wipo.org/about-ip/en/>>. (Article 2 (viii)).
- 3 See: <<http://www.wipo.org/about-ip/en/iprm/pdf/ch1.pdf>>
- 4 See: <<http://www.copyright.gov/>>
- 5 See: <<http://www.wipo.org/about-ip/en/>>
- 6 Ibid.
- 7 See: <http://www.lanl.gov/partnerships/pdf/ip_flyer.pdf>
- 8 See: <<http://www.wipo.org/about-ip/en/ipworldwide/index.html>>
- 9 See: <<http://www.wipo.org/about-ip/en/ipworldwide/pdf/us.pdf>>
- 10 See: < <http://www4.law.cornell.edu/uscode/17/>>
- 11 Larry Lessig, David Post and Eugene Volokh, "Cyberspace Law for Non-Lawyers". Available in the Electronic Frontier Foundation's archives at
<http://www.eff.org/Legal/CyberLaw_Course/cyberlaw.004>
- 12 See: <http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html>
- 13 See: < <http://www.arl.org/info/frn/copy/TEACH.html>>
- 14 See: < <http://www.m-w.com/cgi-bin/dictionary?va=policy>>
- 15 M. E. Kabay, Security Policy Guidelines, Computer Security Handbook, 4th ed. (New York: John Wiley & Sons, Inc., 2002).
- 16 See: < <http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&safe=off&q=computing+policy&btnG=Search>>
- 17 See: <<http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&safe=off&q=acceptable+usage+policy&btnG=Search>>
- 18 M. E. Kabay and Stephen Cobb, "Why We Cite Sources". Available at
<<http://www2.norwich.edu/mkabay/opinion/writing.htm>>
- 19 See: <<http://www.educause.edu/about/membership.asp#WHAT>>
- 20 See: < <http://www.educause.edu/ir/library/html/code.html>>

21 See: <<http://www.security.gatech.edu/policy/usage/policy.html>>

22 See: <<http://www.sjmercury.com/svtech/news/breaking/ap/docs/465588l.htm>>

23 See: <<http://www.cmu.edu/policies/documents/Computing.htm>>

24 See: <http://www.jhu.edu/news_info/policy/copyright.html>

25 See: <http://www.isr.bucknell.edu/Rights_and_Responsibilities/aup.asp>

26 See:
<http://www.isr.bucknell.edu/Rights_and_Responsibilities/Copyright_Responsibilities/Copyright_Ad.pdf>

27 See: <http://security.uchicago.edu/peer-to-peer/sharing_letter.shtml>

28 See: <<http://www.univco.cornell.edu/policy/RU.html>>

29 See: <<http://www.luc.edu/infotech/cease/docs/p2p-file-transfer.html>>

30 See: <<http://www.brown.edu/Facilities/CIS/policy/copyright.html>>

31 See Pg. 34 of <<http://www3.baylor.edu/its/pdfs/techguide.pdf>>

32 See: <http://www.yale.edu/policy/policy_doc.html>

33 See:
<http://www.isr.bucknell.edu/Rights_and_Responsibilities/Copyright_Responsibilities/>

34 See: <<http://www.csuchico.edu/stcp/about/aup.shtml>>

35 See: <<http://www.dartmouth.edu/copyright/>>

36 See: <<http://www.dartmouth.edu/comp/about/policies/general/itpolicy/intellectual.html>>

37 See: <<http://www.siliconvalley.com/mld/siliconvalley/3392998.htm>>

38 See: <<http://www.latimes.com/business/20000725/t000069563.html>>

39 "Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks". Available at
<<http://www.acenet.edu/washington/legalupdate/2003/P2P.pdf>>

40 William Couch, "Peer-to-Peer File-Sharing Networks: Security Risks" Available at
<<http://www.sans.org/rr/papers/50/510.pdf>>

41 See Page 2 of *ibid.*

42 See: <<http://www.kazaa.com/us/help/virus.htm>>

43 See page 4 of <<http://www.sans.org/rr/papers/50/510.pdf>>

44 Reported in the USA Today on September 25, 2002. See:
<<http://www.usatoday.com/tech/news/techpolicy/2002-09-25>>

45 See: <<http://www.acenet.edu/washington/legalupdate/2003/P2P.pdf>>

46 *Ibid.*

47 See: < <http://www.copyright.gov/>>

48 See: <<http://www.ecommercetimes.com/perl/story/8826.html>>

49 See: <<http://www.bsa.org/usa/about/>>

50 See: <<http://www.bsa.org/usa/press/newsreleases/Four-Out-Of-Every-Ten-Software-Programs-Are-Pirated-Worldwide.cfm>>

51 Available from <<http://www.bsa.org/usa/antipiracy/Piracy-and-the-Law.cfm>>

52 See: <<http://www.educause.edu/pub/edupage/archives/98/edupage-0813.html#anchor1>>

53 Philip J. Kaleewoun II, "An Overview of Corporate Computer User Policy". Available at <<http://www.sans.org/rr/papers/50/535.pdf>>

54 See: <http://www.lanl.gov/partnerships/pdf/ip_flyer.pdf>

55 See: <<http://www.ee.surrey.ac.uk/Contrib/Edupage/1997/05/06-05-1997.html#1>>

56 See: <http://www.theregister.co.uk/2000/09/27/greasing_the_free_software_skids/>

57 See: <<http://www.educause.edu/pub/edupage/archives/97/edupage-0722.html>>

58 See: <<http://www.unixguru.com/>>

59 See: <<http://www.washingtonpost.com/wp-dyn/articles/A46353-2000Aug6.html>>

60 See: <<http://www.educause.edu/pub/edupage/archives/98/edupage-0802.html>>

61 See: <<http://www.siliconvalley.com/mld/siliconvalley/5517523.htm>>

62 See: <<http://www.informationweek.com/774/email.htm>>

63 Personal e-mail communication with Mr. Gary Webb, April 19, 2004.

64 Ibid.

65 See: <<http://washingtonpost.com/wp-dyn/business/latestap/A54075-2001Jun12.html>>

66 See: <<http://www.msnbc.com/news/380471.asp>>

67 See: <<http://www.wired.com/news/digiwood/0,1412,60613,00.html>>

68 Col. Phil Susmann, Norwich University CIO. Personal interview, March 17, 2004.

69 See: <<http://www.packeteer.com/prod-sol/solutions/p2p.cfm>>

70 Col. Phil Susmann, Norwich University CIO. Personal interview, March 17, 2004.

71 See: <<http://www.acenet.edu/washington/legalupdate/2003/P2P.pdf>>

72 See: <<http://www.educause.edu/ir/library/pdf/erm0346.pdf>>

73 See: <<https://www.people.virginia.edu/cgi-ruby/pwdist>>

74 See: <<http://www.itc.virginia.edu/pubs/docs/RespComp/videos/home.html>>

75 See: <<http://www.doit.wisc.edu/security/policies/ror/copyright.gif>>

76 Col. Phil Susmann, Norwich University CIO. Personal interview, March 17, 2004.

77 See: <<http://www.educause.edu/ir/library/powerpoint/MAC0402.pps>>

78 See: <http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml>

Karthik Raman (<mailto:ramank@norwich.edu>) is a Computer Science and Information Assurance major at Norwich University in Northfield, Vermont. This work was submitted in partial fulfillment of the requirements for the IS342 Management of Information Assurance course taught by M. E. Kabay, PhD, CISSP in the Spring 2004 semester.

Source: Ubiquity, Volume 5, Issue 15, June 9 - 15, 2004