Journal of Law and Policy

Volume 14
Issue 1
SCIENCE FOR JUDGES V:
Risk Assessment Data: Disclosure and Protection

Article 13

2005

Copyright Infringement v. Academic Freedom on the Internet: Dealing With Infringing Use of Peer-to-Peer Technology on Campus Networks

Jason Putter

COPYRIGHT INFRINGEMENT V. ACADEMIC FREEDOM ON THE INTERNET: DEALING WITH INFRINGING USE OF PEER-TO-PEER TECHNOLOGY ON CAMPUS NETWORKS

Jason Putter[*]

"When the danger of abuse is great, however, so also is the danger of unwarranted repression."[1]

INTRODUCTION

In response to the widespread use of peer-to-peer (P2P)[2] file sharing applications to share unlicensed copyrighted movies, music, and software over the internet (P2P piracy), colleges and universities across the country are installing technological impediments on their campus networks to curb the use of all P2P technology.[3] The impact of these impediments is troubling. Some

---

[*] Brooklyn Law School Class of 2006; B.A. Vassar College, 1994. The author would like to thank his wife, Felicia, and his two children, Arielle and Austin, whose love makes it all worthwhile. He would also like to thank his parents for their constant support and encouragement in pursuing a second career. Special thanks to the *Journal of Law and Policy* staff for their hard work.

[1] Urofsky v. Gilmore, 216 F.3d 401, 433 (4th Cir. 2000) (Wilkinson, J., concurring).

[2] For purposes of this note, the term "P2P" is limited to technology that allows internet users—or peers—to "directly interact and share information with each other's computer without the intervention of a server." U. S. GEN. ACCOUNTING OFFICE, FILE SHARING: SELECTED UNIVERSITIES REPORT TAKING ACTION TO REDUCE COPYRIGHT INFRINGEMENT 24 (May 2004) [hereinafter U.S. GEN. ACCOUNTING OFFICE], *available at* http://purl.access.gpo.gov/GPO/LPS53000. For a broader definition, see discussion *infra* Part III.B.1.

[3] *See* Andrea L. Foster, *Lawmakers Demand that Colleges Crack Down on*

not only block the infringing uses[4] of P2P technology, but also the non-infringing uses.[5] Others only block infringing uses, but do so by "actively" monitoring and logging the content of all P2P network traffic, including files that are not remotely suspect.[6]

These types of "blocking" technologies are problematic in the university setting because they place unnecessary restrictions or surveillance upon communication, critical inquiry and research, and significantly devalue core academic values of privacy[7] and

---

Illegal File Sharing, THE CHRONICLE OF HIGHER EDUCATION (Feb. 27, 2003), *available at* http://chronicle.com/free/2003/02/ 2003022701t.htm.

[4] Using P2P file sharing applications to distribute unlicensed copyrighted movies, music, and software is a violation of U.S. Copyright law. *See* 17 U.S.C. §§ 501, 506 (2002). *See* discussion, *supra* Part I.C-E.

[5] For example, many universities use P2P file sharing applications to facilitate the sharing of class notes, class assignments, and countless other forms of non-copyrighted content. *See* discussion *infra,* Part I.B-F; *Intellectual Property Piracy at U.S. Colleges: Hearing before the Subcomm. on Courts, the Internet, and Intellectual Property Comm. on the Judiciary*, 108th Cong. 19 (2003) [hereinafter Spanier Statement] (statement of Graham B. Spanier, President, Penn. State University).

[6] *See* discussion *infra,* Part I.F; AUDIBLE MAGIC CORP., WHITE PAPER: MANAGING PEER-TO-PEER TRAFFIC WITH THE COPYSENSE NETWORK APPLIANCE [hereinafter AUDIBLE MAGIC: COPYSENSE], *available at* http://www.audiblemagic.com/documents/P2P_Managing.pdf (last visited Nov. 1, 2004).

[7] Employing technological measures to defeat P2P piracy has profound implications to the privacy rights of both faculty and staff, but it is beyond scope of this note. *See* VIRGINIA E. REZMIERSKI & NATHANIEL ST. CLAIR, II, LAMP PROJECT, IDENTIFYING WHERE TECHNOLOGY LOGGING AND MONITORING FOR INCREASED SECURITY END AND VIOLATIONS OF PERSONAL PRIVACY AND RECORD BEGINS (2001), *available at* http://www.aacrao.org/ publications/NSFLAMP.pdf; Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2003). However, this note is concerned with privacy as an element of academic freedom. Jonathan Alger, *Prying Eyes In Cyberspace*, ACADAME, Sep./Oct. 1999, *available at* http://www.aaup.org/ publications/Academe/1999/99so/SO99LGWA.HTM. Algers notes, "In an era in which colleges are encouraging faculty members to teach, conduct research, and communicate with students and colleagues on-line, they can best protect academic freedom and the integrity of their educational mission by respecting the privacy of these communications." *Id. See also* Julie E. Cohen, *Information Rights and Intellectual Freedom, in* ETHICS AND INTERNET 7 (Anton Vedder, ed. Antwerp: Intersentia, 2001). Cohen postulates that intellectual freedom requires

academic freedom.[8] This note examines how technological impediments to P2P piracy on campus networks have a significant chilling effect on academic freedom and recommends how to craft a network use policy that fully preserves academic freedom.

Part I of this note introduces P2P technology and details both its beneficial and infringing uses, particularly in the university setting. It also includes a brief background of the copyright issues that universities face regarding P2P piracy. This part concludes with a discussion of campus network use policies, examining both the educational and technical initiatives that universities have undertaken to combat P2P piracy. Part II provides an overview of academic freedom in the United States, including a discussion of its origins in both policy and law. Part III analyzes how poorly-crafted technological solutions unnecessarily erode academic freedom. Part IV offers several recommendations on how universities should approach the P2P piracy problem, including a discussion of an ideal network use policy designed to protect academic freedom to the fullest extent possible under current copyright law.

I. OVERVIEW OF P2P TECHNOLOGY AND THE COPYRIGHT PROBLEM

Though peer-to-peer technology could describe most of the computing done on the internet, P2P technology is commonly understood as a reference to computer applications which share information without using a central computer server.[9] P2P technology has enhanced the educational and research capabilities of universities nationwide.[10] Providing students with access to P2P networks, however, has also included providing the means for copyright infringement.[11] Universities and colleges have thus been targeted by copyright holders looking to enforce their rights

---

sufficient autonomy with respect to the information that Internet users send and receive. In other words, intellectual freedom will depend upon the level of "information privacy" Internet users enjoy. *Id* at 11-32.

[8] *See* discussion, *infra* Parts II-III.

[9] U. S. GEN. ACCOUNTING OFFICE, *supra* note 2 at 24.

[10] *See* discussion, *infra* Part I.B.

[11] *See* discussion, *infra* Part I.C.

against concentrations of file sharers.[12] In response, universities have instituted a combination of educational and technical initiatives to combat P2P piracy.

A. P2P Technology Defined

Peer-to-peer technology allows internet users, or peers, to directly interact and share information with each other's computers.[13] The use of P2P technology is widespread and its growth potential is unimaginable.[14] From academia to industry,[15] P2P technology is being used to share resources such as applications, storage, processing power, human collaboration, information and ideas.[16] Despite the enormous publicity surrounding P2P piracy, P2P technology enables users to do more than share unlicensed copyrighted content.[17] In fact, the architecture of the internet itself is peer-to-peer; e-mail and web

---

[12] *Id*.

[13] U.S. GEN. ACCOUNTING OFFICE, *supra* note 2, at 24. For a broader definition, see discussion *infra* Part I.A.

[14] Telephone Interview by Tim O'Reilly and Richard Koman with Lawrence Lessig, Professor of Law, Stanford Law School (Jan. 9, 2001) (Professor Lessig states that peer-to-peer technologies are "the next great thing on the Internet. We haven't begun to understand or imagine the possibilities"). Spanier Statement, *supra* note 5 (stating that "P2P technology has the potential to expand dramatically the ease, speed, and breadth of information exchange. Such capacity will clearly benefit a wide range of educational and research activities"). *Id.*

[15] For a comprehensive list of companies, projects, and initiatives related to peer-to-peer technologies, see *O'Reilly P2P Directory*, *available at* http://www.openp2p.com/pub/q/p2p_directory (last visited Oct, 24, 2005).

[16] Ashton Applewhite, *From T-Shirts to Pinstripes–Peer-to-Peer Gets Some Respect*, Vol. 4, No. 1, IEEE DISTRIBUTED SYSTEMS ONLINE (Jan. 2003), *available at* http://dsonline.computer.org/portal/site/dsonline/menuitem.9ed3d9924aeb0dcd82ccc6716bbe36ec/index.jsp?&pName=dso_level1&path=dsonline/2003_Archives/0301/f&file=news_print.xml&xsl=article.xsl&.

[17] *See* discussion, *infra* Part I.B; *Overexposed: The Threats to Privacy and Security on File Sharing Networks: Hearing before the House Comm. on Gov. Reform*, 25-30, 108th Cong. (2003) [hereinafter Schiller Statement I] (statement of Jeffrey I. Schiller, Network Manager/Security Architect, Mass. Institute of Technology).

browsing are basic peer-to-peer functions.[18] Yet, the commonly understood use of the term is more refined.

P2P technology refers to systems and applications that allow the sharing of any type of resource directly between two or more computers, including, but not limited to content, storage, computing cycles, processing power, bandwidth, information, and human collaboration.[19] Whatever the shared resource, the key feature of most P2P applications is that they do not rely on the traditional client/server model, which uses a centralized server to facilitate the interaction between users.[20] Rather, P2P technology enables users to share information directly.[21] As such, all of the shared information resides with the users and the producers, and they relate to each other side by side as peers.

P2P systems encompass a wide array of technologies making it difficult to precisely define or categorize them. Three common uses for P2P technology include file sharing, distributed computing, and collaborative applications.[22] File sharing, as the name implies, allows for the transferring of files between computers without the intervention of a server.[23] These files may

---

[18] Schiller Statement I*, supra* note 17, at 27.

[19] *The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of P2P File-Sharing Networks?: Hearing before the Senate Comm. on the Judiciary*, 108th Cong. (Jun. 17, 2003) (statement of Chris Murray, Legislative Counsel, Consumers Union) [hereinafter Murray Statement]; Applewhite, *supra* note 16.

[20] In the client/server architecture, there are two distinct software modules: the server module and the client module. Dinesh C. Verma, LEGITIMATE APPLICATIONS OF PEER-TO-PEER NETWORKS 5 (2004). "[T]he key characteristic of the client-server module is that there is a server module that is the central point for communication. Clients do not communicate with each other, only with the server module." *Id*. However, P2P systems are technically classified into three main categories: centrally coordinated, hierarchical, and decentralized. Theidore Hong, *Performance*, *in* PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 203 (Andy Oram ed., 2001).

[21] U. S. GEN. ACCOUNTING OFFICE, *supra* note 2, at 24.

[22] *Id.* at 24-25.

[23] *The Future of Peer-to-Peer (P2P) Technology: Hearing Before the Subcomm. on Competition, Foreign Commerce, and Infrastructure of the S. Comm. on Commerce, Science and Transportation,* 108th Cong. (2004) [hereinafter Ottolenghi Testimony] (written testimony of Les Ottolenghi,

include data, audio, and video, as well as multimedia and software applications.[24] Distributed computing, or highly parallel computing, harnesses the idle processing power of many separate computers to accomplish a single task like processing data.[25] Collaborative applications allow users in different geographical locations to communicate and work with each other, often in real-time, in order to increase productivity.[26] Regardless of its categorization, the underlying premise of any P2P technology is that users have something valuable to share and P2P provides an efficient way of sharing it.[27]

B. Beneficial Uses

The overall design of any P2P technology overcomes many of the limitations of the client/server model in creating, reproducing, and distributing information. The lack of a central server makes building and maintaining these systems inexpensive.[28] A P2P network can make use of the computation and storage resources of computers across the entire internet.[29] Additionally, P2P technology decentralizes and distributes content in a system,

President, INTENT MediaWorks, LLC).

[24] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1032 (C.D. Cal. 2003); Ottolenghi Testimony*, supra* note 23.

[25] Verma, *supra* note 20, at 1-5 (2004).

[26] U. S. GEN. ACCOUNTING OFFICE, *supra* note 2, at 25. *See* Verma, *supra* note 20, at 135-36.

[27] Gene Kan, *Gnutella, in* 94 PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 122 (Andy Oram ed., 2001) ("The basic premise underlying all peer-to-peer technologies is that individuals have something valuable to share.").

[28] *Piracy of Intellectual Property on Peer-to-Peer Networks: Hearing Before the Subcomm. on Courts, the Internet and Intellectual Property of the H. Judiciary Comm.,* 106th Cong. (2002) [hereinafter Sohn Statement] (statement of Gigi B. Sohn, President, Public Knowledge) (noting that through "linking together individual computers and distributing their power, P2P technology is superior to the centralized server [model] . . . because it is more cost effective"). *Id.*

[29] *Id*. (noting that the P2P model is superior to the centralized sever model because it harnesses bandwidth and storage resources that would otherwise go unused).

making it much less prone to failure.[30] In most P2P file sharing applications, for example, all files on an individual user's machine are available to all the other users so there is no need to maintain and update a central server.[31] The lack of central coordination and management enables information exchange without the added costs of maintaining a server or sites that store the information.[32]

The use of P2P technology in academia is diverse and widespread and its importance to the future of education and research is immeasurable.[33] The most common academic use of P2P technology is for file sharing applications that allow students and faculty to share class notes, class assignments, and other forms of non-copyrighted content.[34] For example, university music departments are sharing, on campus and between campuses, their non-copyrighted music through P2P file sharing applications.[35] Similarly, literary projects, such as Project Gutenberg, make available electronic copies of books whose authors have given permission to do so or are non-copyrighted.[36] The Project

---

[30] Hari Balakrishnan et al., *Looking Up Data in P2P Systems*, COMMUNICATIONS OF THE ACM 43 (2003). *See also* Sohn Statement, *supra* note 28 (noting P2P technology is superior to the centralized sever model because it is more robust and resilient; faster and more reliable; harnesses bandwidth and storage resources that would otherwise go unused; and enables real-time collaborative work).

[31] Verma, *supra* note 20, at 63.

[32] *Id*.

[33] *Peer-to-Peer Networks: Hearing before the Subcomm. in Competition, Foreign Commerce and Infrastructure*, 108th Cong. (2004) [hereinafter Pederson Statement] (statement of Curt Pederson, Vice President for Information Services, Oregon State University) (stating that P2P technology will "change the way educational and research materials are shared, explored, dissected, or manipulated"); Spanier Statement, *supra* note 5 (stating P2P technology has the "potential to expand dramatically the ease, speed, and breath of information exchange" which will benefit a "wide range of educational and research activities"); Lawrence Lessig, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 79 (2004) (arguing that "P2P technology can be ideally efficient in moving content across a widely diverse network").

[34] *See* Pederson Statement, *supra* note 33.

[35] *Id.*

[36] PROJECT GUTENBERG: HISTORY AND PHILOSOPHY OF PROJECT

Gutenberg repository alone currently has over 9,500 books available;[37] however, this is only a small fraction of the amount of digital material that libraries, including university libraries, wish to distribute via P2P file sharing.[38]

Universities are also making use of commercial P2P applications like Groove Network's Groove Workspace "virtual classroom" solution.[39] Through P2P collaboration and file sharing applications, "virtual classroom" allows students and teachers to store and share an impressive array of information. They can post and access drafts, annotate revisions, review documents, and collaborate and chat with each other in real time.[40] One professor described this interactive shared space as "com[ing] very close to being, for me, the ideal academic tool."[41]

Universities, especially research universities, are creating similarly robust P2P applications. For example, Lionshare, a project started by Penn State University, is using P2P file sharing technology to create a series of networks across the country for sharing knowledge among instructors, scholars, researchers,

---

GUTENBERG (1992), *available at* http://promo.net/pg/history.html#the selection. Project Gutenberg makes available a wide range of fiction and non-fiction, examples include: Alice in Wonderland, Aesop's Fables, the Bible and other religious documents, Shakespeare, and references, such as Roget's Thesaurus, almanacs, and a set of encyclopedia. *Id. See also*, LIONSHARE, CONNECTING AND EXTENDING PEER TO PEER NETWORKS (October 2004), *available at* http://lionshare.its.psu.edu/main/info/docspresentation/LSFinal WhitePaper. pdf.

[37] Brief of Amici Curiae American Civil Liberties Union et al. at 10, MGM v. Grokster, 380 F.3d 1154 (9th Cir. 2004).

[38] *Id*. (noting that libraries have a strong interest in using P2P file sharing technology to "share information in such areas as medicine, law, and science; to archive historical documents; and to provide electronic access to a broad range of public domain information, including government documents").

[39] *See*, *e.g.*, GROOVE NETWORKS, CASE STUDIES, THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL, [hereinafter GROOVE NETWORKS, UNC STUDY], http://www.groove.net/index.cfm?pagename=CaseStudy_UNC (last visited Nov. 20, 2004). A partial list of Groove Networks education clients include Harvard Medical School, MIT, and Yale University. *See id.,* at http://www.groove.net/index. cfm/pagename/CustomerList/.

[40] GROOVE NETWORKS, UNC STUDY, *supra* note 39.

[41] *Id*.

librarians, and students.[42] This system will take each local user's repository of digital content—including data, photographs, sounds, instructional videos, as well as other content used for teaching, and research purposes—and will compile it into a federated search system that will allow all of the users on the network to search and share.[43] Equally impressive is the P2P technology on which this application runs. Internet2, a consortium of schools, industry, and government, is a P2P platform designed for advanced network applications and technologies, such as Lionshare.[44] Using the advantages inherent to P2P technology, the speed of this network is up to a thousand times faster than ordinary internet networks, allowing researchers to handle data in ways never before possible.[45]

Another university-created P2P application is NYU's Coral project, which is a P2P content distribution network that allows web site operators to handle high volumes of internet traffic by sharing the load with all participating peers.[46] Using the Coral software, a web site's capacity to handle a large volume of traffic grows automatically with the site's popularity.[47] Such a system has a "democratizing effect" on content distribution, as many publishers are limited "in the size of the audience and the type of content that they can serve" by the high costs associated with the client/server model.[48] However, the underlying purpose of the project is more ambitious. The Coral project is part of project

---

[42] LIONSHARE, *supra* note 36.

[43] *Id.*

[44] *See generally* INTERNET2, *available at* http://www.internet2.org. *See also* Penn State University's Internet2 page, http://aset.its.psu.edu/i2/.

[45] *Id.*

[46] Michael J. Freedman et al., *Democratizing Content Publication with Coral,* NYU DISTRIBUTION NETWORK*, available at* http://www.coralcdn.org/docs/coral-nsdi04.pdf (last visited Oct. 24, 2005). According to the authors, Coral "leverages the aggregate bandwidth of volunteers running the software to absorb and dissipate most of the traffic for web sites using the system. In so doing, CoralCDN replicates content in proportion to the content's popularity, regardless of the publishers resources—in effect democratizing content publication." *Id*.

[47] *Id.*

[48] *Id.*

Infrastructure for Resilient Internet Systems (IRIS), which is a government sponsored P2P network designed to foil "Denial of Service" attacks, a hacking technique used to swamp a web server with requests until it crashes.[49] Denial of Service attacks cost the U.S. economy billions of dollars a year in lost revenue[50] and are of growing interest to terrorists seeking to damage U.S. technology infrastructure.[51]

P2P technology has also long been of interest to the educational arm of the Department of Defense.[52] At the Naval Post Graduate School, researchers use P2P file sharing and collaboration technology to support, among other things, complex humanitarian emergency aid operations, wearable computing systems, and airborne en-route mission planning.[53] Similarly, the Department of Homeland Security is using P2P technology as a core component of its counterterrorism communications network, which is a nationwide system designed to deter, detect, and respond to terrorist actions.[54] This system utilizes P2P technology because its decentralized architecture provides a more agile and secure collaboration infrastructure, and is thus more reliable and

---

[49] David Cohen, *New P2P Network Funded by the US Government*, NEWSCIENTIST.COM (Oct. 2002), http://www.newscientist.com/news/print.jsp?id=ns99992861.

[50] James Pearce, *Netsky Causing Billions in Damages*, ZD NET (Feb. 26, 2004), http://news.zdnet. com/2100-1009_22-5165642.html.

[51] Sam Costello, *Terrorists May Launch Denial of Service Attacks*, IDG NEWS SERVICE (Sept. 18, 2001), *available at* http://www.pcworld.com/news/article/0,aid,62505,00.asp.

[52] The Naval Post Graduate School studies and researches programs relevant to the Navy as well as other arms of the Defense Department. GROOVE NETWORKS: CASE STUDIES, NAVAL POST GRADUATE SCHOOL (2003), *available at* http://www.groove.net/index.cfm?pagename=CaseStudy_Naval.

[53] *Id.*

[54] Press Release, Department of Homeland Security, Homeland Security Information Network to Expand Collaboration, Connectivity for States and Major Cities (Feb. 24, 2004), *available at* http://www.dhs.gov/dhspublic/display?content=3350; Press Release, Groove Networks, Groove Networks Announces Role In Newly Announced Homeland Security Information Network (Feb. 26, 2004), *available at* http://www.groove.net/release.cfm?pagename=press_feb26_2004.

less vulnerable to terrorist attack.[55] In fact, a task force formed in the wake of the 9/11 tragedy to study national security and information technology recently reported that the centralized information processing systems in the U.S. government are ineffective in the war on terror.[56] The report recommends a shift to a distributed, decentralized P2P network as "peer-to-peer collaboration allows federal, state, and local participants to draw upon the collective expertise of the community."[57]

In short, P2P technology has many beneficial uses, especially in academia. Most importantly, the decentralized nature of P2P applications allows users to create and distribute virtually limitless types of resources, in ways that were never before possible. Despite these enormous benefits, however, the focus on P2P technology has been its widespread use to share unlicensed, copyrighted content.

C. Infringing Uses

The most widely publicized use of P2P technology is the sharing of unlicensed copyrighted movies, music, and software through applications like BitTorrent, Kazaa, LimeWire, and Morpheus.[58] P2P piracy has become particularly rampant on university campuses as the average campus has a high-bandwidth internet connection on its network and a large concentration of young, computer-literate users.[59]

The amount of piracy occurring on these applications is

---

[55] Press Release, Department of Homeland Security, *supra* note 54; Press Release, Groove Networks, *supra* note 54.

[56] This 34-member task force consists of leaders from across academia and industry. THE MARKLE FOUND., TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (Oct. 2002), *available at* http://www.911investigations. net/IMG/pdf/doc-963.pdf.

[57] *Id*. at 13.

[58] For a list of the most popular P2P file sharing applications and how they work, see http://www.filesharingwatch.com.

[59] U.S. GEN. ACCOUNTING OFFICE, *supra* note 2, at 5.

massive.[60] The most popular P2P file-trading software programs have been downloaded by computer users over two hundred million times.[61] At any one time there are over three million users simultaneously using just one of these services.[62] Each month, on average, over 2.3 billion digital-media files are transferred among users of P2P systems.[63] Experts estimate that anywhere from 70 to 90 percent of the files shared on these networks are unlicensed copyrighted files.[64] While there are no definitive statistics, it is believed that a fair amount of the infringing files downloaded each month are downloaded from university campuses.[65]

Additionally, the infringing use of these file sharing applications has created a bandwidth problem on many university campuses, as the large number and size of files being shared overtaxes the schools' networks.[66] In many cases, this affects the availability of network resources for legitimate uses.[67] As a result, most universities "passively" monitor the traffic flow on their networks by measuring the amount of data that is transmitted over a network.[68] Under notions of academic freedom and privacy, however, many universities decline to monitor the actual content of

---

[60] *See* Piracy Deterrence and Education Act of 2004, H.R. 4077.IH, 108th Cong. § 2(3) (2004).

[61] *Id.*

[62] *Id.*

[63] *Id*.

[64] Brief of Amici Curiae American Civil Liberties Union et al., *supra* note 37, at 10.

[65] Roy Mark, *College File Swapping: Making the Illegal Legal?*, INTERNETNEWS.COM (Sept. 2, 2003), http://dc.internet.com/news/article.php/3071331 (noting that it is a "widely-held belief that college students, using university-supplied networks and bandwidth, are at the forefront" of the P2P piracy problem).

[66] ELECTRONIC COMMERCE NEWS: HOUSE SUBCOMM. HEARINGS TARGETS P2P PIRACY ON UNIVERSITY CAMPUSES (Mar. 3, 2003).

[67] *Id.*

[68] *See Pornography, Technology, and Process: Hearing before Comm. on the Judiciary*, 108th Cong. (2003) [hereinafter Hess Statement] (statement of Stephen Hess, Associate Academic Vice President for Information Technology, University of Utah).

the information contained within the data flow.[69]

D. The Copyright Problem

Due to the high volume of P2P piracy on university campuses, both Congress and the creative content providers that own copyrights[70] have exerted a great deal of pressure on universities to take a more proactive role in curbing P2P piracy.[71] In October 2002, representatives of the creative content industries sent letters to two thousand three hundred colleges and universities, requesting that they take immediate action to curb P2P piracy on campus networks.[72] The letters stated that students and other users of campus networks who operate P2P applications to share copyrighted materials were violating federal copyright law and faced legal action.[73]

In order to implement stronger anti-piracy measures, universities across the country are reviewing and amending their network use policies, which define acceptable internet use on campus.[74] Many universities have already amended their network use policies to include explicit language that unauthorized downloading of copyrighted material is illegal and will not be tolerated. Some universities have also instituted various campaigns to educate students about unauthorized file-sharing.[75] Others are

---

[69] *Id.*

[70] The creative content industries are represented collectively by the Motion Picture Association of America (MPAA), the National Music Publishers' Association (NMPA), the Recording Industry Association of America (RIAA), and the Songwriters Guild of America (SGA).

[71] Foster, *supra* note 3.

[72] Letter from Rick Carnes, President, The Songwriters Guild of America et. al., to University/College President (Oct. 3, 2002), http://www.aau.edu/intellect/UniversityLetter.pdf.

[73] *Id*.

[74] *See* JOINT COMM. OF THE HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES, PROGRESS DURING THE PAST ACADEMIC YEAR ADDRESSING ILLEGAL FILE SHARING ON COLLEGE CAMPUSES 3 (2004).

[75] *Id*. AMERICAN COUNCIL ON EDUCATION: UNIVERSITY POLICIES AND PRACTICES ADDRESSING IMPROPER PEER-TO-PEER FILE SHARING 3 (Mar. 19, 2004), *available at* http://www.acenet.edu/AM/Template.cfm?Section=

employing technological impediments to curb P2P piracy.[76]

The media industry, however, is not waiting for universities to solve the problem themselves.[77] Since issuing the warning letter in October 2002, the Recording Industry Association of America (RIAA) has sent over 30,000 notices to universities detailing specific instances of illegal sharing of files on their networks.[78] By March 2003, the RIAA had brought legal action against alleged illegal file sharers at 21 separate colleges and universities,[79] and by 2004 those numbers increased to 190 students at 61 universities.[80] The wave of litigation continues, as the RIAA has already brought 560 lawsuits at 39 campuses in the first nine months of 2005.[81] Additionally, despite a significant study showing that the RIAA's legal threats have had absolutely no impact on P2P file-sharing traffic,[82] the Motion Picture Association of America (MPAA) recently announced that it had filed 200 separate copyright infringement suits, although it is not clear how many of these suits targeted college students.[83]

The media industry also recently scored a key victory against

---

Search&section=Legal_Issues_and_Policy_Briefs1&template=/CM/ContentDisplay.cfm&ContentFileID=721.

[76] *See* discussion, *supra* Part I.F.2.

[77] *See* discussion, *supra* Part I.F.

[78] U.S. GEN. ACCOUNTING OFFICE, *supra* note 2, at 5.

[79] Press Release, RIAA Brings New Round of Cases Against Illegal File Sharers, (Mar. 23, 2003), *available at* http://www.riaa.com/news/newsletter/032304.asp.

[80] *Intellectual Property Piracy at U.S. Colleges: Hearing before the Subcomm. on Courts, the Internet, and Intellectual Property Comm. on the Judiciary*, 108th Cong. (2003) [hereinafter Sherman Statement] (statement of Cary Sherman, President, RIAA).

[81] Press Release, Latest Round Of Music Industry Lawsuits Targets Internet Theft At 17 College Campuses (Sept. 29, 2005), *available at* http://www.riaa.com/news/newsletter/092905.asp.

[82] Thomas Karagiannis et al., *Is P2P Dying or Just Hiding*, CAIDA (Nov. 2004), *available at* http://www.caida.org/outreach/papers/2004/p2p-dying/ (finding that "P2P traffic represents a significant amount of Internet traffic and is likely to continue to grow in the future, RIAA behavior notwithstanding").

[83] Cynthia L. Webb, *Hollywood's One Strike Policy*, WASHINGTON POST.COM (Nov. 17, 2004), *available at* http://www.washingtonpost.com/ac2/wp-dyn/A56746-2004Nov17?language=printer.

the creators of Grokster, one of the most popular P2P file sharing applications.[84] In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster*, the Supreme Court held that creators of P2P file sharing applications can be held liable for copyright infringement where they specifically promote the applications' use to infringe copyright and design them primarily to infringe copyright.[85]

While the content industries have only taken legal action against the people who actually engaged in the illegal sharing or created the file sharing application itself, it is widely understood that universities may face legal action as well, under the theory that their knowledge of or contribution to the conduct of their students exposes them to claims of vicarious or contributory copyright infringement.[86] Under U.S. copyright law, damage awards for such infringement can range from $750 to $30,000 per infringed copyrighted work.[87] Fear of such liability, however, is greatly diminished by the Digital Millennium Copyright Act.[88]

E. The Digital Millennium Copyright Act (DMCA)

Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act, is the controlling statute regarding university liability for the infringing use of P2P file sharing applications on their networks.[89] Universities' liability for copyright infringement is limited by the "safe harbor" provisions of this Title.[90] These provisions shield Internet Service Providers

---

[84] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 125 S. Ct. 2764 (2005).

[85] *Id.*

[86] *See* Michael J. Remington, *Background Discussion of Copyright Law and Potential Liability for Students Engaged in P2P File Sharing on University Networks*, AMERICAN COUNCIL OF EDUCATION 8 (Aug. 7, 2003), *available at* http://www.acenet.edu.

[87] 17 U.S.C. § 504(c)(1) (2004).

[88] 35 U.S.C. §§ 5, 17, 28 (2000).

[89] *Id.* Title II is now codified in Section 512 of the Copyright Act.

[90] *See* 17 U.S.C. 512(a)-(d) (2003). Specifically, if it satisfies all of the requisites of section 512, an ISP enjoys a "safe harbor" by providing any of four following services: (1) transitory digital network communications, i.e. providing internet service as a "mere conduit" (512(a)); (2) system caching (512(b)); (3)

(ISP), including university internet networks,[91] from charges of vicarious and contributory copyright infringement, provided that they conform to certain requirements.[92]

In terms of P2P file sharing, the critical requirement is that a university ISP must act as a "mere conduit" of material transmitted over its network. In other words, when a university simply enables the transfer of files between two or more of its users, and that information only resides on the users' computers, there is no liability. Additionally, a university must adopt and reasonably implement use policies that describe and promote compliance with copyright laws and provide for the termination of accounts belonging to users who repeatedly infringe the copyrights of others.[93] Universities that allow users to store files on the network face additional requirements. They must remove any infringing material residing on the network once it has actual or constructive knowledge of such material and must take reasonable steps to inform the infringing user of the removal.[94]

The requirements of the DMCA provide strong incentive for universities to not police their networks for infringing materials, because doing so may lead to "knowledge" of infringement, whereby the failure to take action could result in liability.[95]

While it appears that universities are in a relatively safe position regarding current copyright law, Congress has taken an active role in addressing P2P piracy, proposing a variety of new

---

storing materials on its servers at the direction of its users, i.e. hosting (512(c)); and (4) information location tools, i.e. links to infringing materials (512(d)).

[91] A university, in providing computers, storage, or network connection, is considered an ISP. *See* 17 U.S.C. § 512(e) (2000).

[92] 17 U.S.C. § 512(a)-(h) (2003).

[93] *Id*. Additionally, universities may also have to disclose the identity of an alleged infringer provided that it is requested by a lawfully issued subpoena, but the law is unsettled. *See* RIAA v. Verizon, 351 F.3d 1229 (D.C. Cir. 2003) (holding that under the DMCA, subpoenas served to identify the names of infringing users can only be issued to an ISP that stores infringing material on its servers, and not to an ISP acting as a "mere conduit" for P2P file sharing).

[94] 17 U.S.C. § 512(a)-(h) (2003); Constance S. Hawke, *The P2P File Sharing Controversy: Should Colleges be Involved?*, 184 ED. LAW REP. 681, 689 (2004).

[95] *See* Hawke, *supra* note 94, at 690.

legislative measures if universities, as well as other P2P distributors, cannot curb infringing use.[96] These laws would create new areas of copyright liability and increase the penalties under current copyright law.[97]

F. University Network Use Policy

As noted, most universities counterbalance the liability that they might have for copyright infringement with educational initiatives to discourage unlicensed file-sharing on their networks. Technological options have also emerged.

1. Educational Initiatives

As institutions of learning, it is not surprising that universities' first line of defense in dealing with claims of copyright infringement is the implementation of educational initiatives.[98] While educational approaches vary from university to university, their fundamental components are quite similar.[99] Generally, universities are attempting to educate students, as well as teachers and staff, about the unauthorized use of file-sharing and to "provide a legal and ethical framework for the use of copyrighted

---

[96] A variety of legislative solutions have been proposed in Congress, aimed at addressing new internet technologies, including P2P networks. *See* H.R. 2885, 108th Cong. (2003) (bill to regulate P2P software); H.R. 2752, 108th Cong. (2003) (bill to enhance criminal copyright penalties for P2P file sharing and regulate software); H.R. 2517, 108th Cong. (2003) (bill to enhance criminal copyright enforcement and create Internet education programs); H.R. 5211, 107th Cong. (2002) (bill to authorize copyright owners to take technical measures to halt unauthorized P2P file-sharing); S. 2048, 107th Cong. (2002) (bill to impose federally mandated content-protection technologies on software and devices).

[97] *See supra* note 96.

[98] *Intellectual Property Piracy at U.S. Colleges: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property Comm. on the House Judiciary*, 108th Cong. (Feb. 26, 2003) (statement of Molly Corbett Broad, President, Univ. of North Carolina); Spanier Statement, *supra* note 5.

[99] *See* AMERICAN COUNCIL ON EDUCATION *supra* note 75, at 3-4.

works."[100] Some universities require students to sign a network use policy before they can access the school's network.[101] Others hold lectures regarding copyright infringement, or otherwise distribute notices, fliers, and posters on the subject.[102] Aside from these pre-emptive educational actions, many universities also have some form of educational program for users who are caught engaging in unauthorized file sharing.[103]

In order to comply with the safe harbor provisions of the DMCA, many universities have updated their network use policies to educate entire campuses about policies terminating the access of users who repeatedly infringe copyrights.[104] Normally included in these use policies are also the penalties that users may face for engaging in unlawful file sharing.[105]

2. Technological Impediments

Universities employ two main types of technological impediments to P2P piracy: software that blocks all use of P2P applications and software that attempts to block only the infringing use of P2P applications. An example of each type of technological impediment is discussed below.

The University of Florida's ICARUS program is a well-publicized technological solution to P2P piracy.[106] ICARUS, short

---

[100] JOINT COMM. ON HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES: A REPORT TO THE SUBCOMM. ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY 4 (2004).

[101] AMERICAN COUNCIL ON EDUCATION *supra* note 75, at 3-4; JOINT COMM. ON HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES *supra* note 100, at 4.

[102] AMERICAN COUNCIL ON EDUCATION, *supra* note 75, at 3-4; JOINT COMM. ON HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES *supra* note 100, at 4.

[103] AMERICAN COUNCIL ON EDUCATION, *supra* note 75, at 3.

[104] *See* discussion, *supra* Part I.E.

[105] *Id*.

[106] *See*, *e.g.,* David Joachim*, The University of Florida's ICARUS P2P Blocking Software has Clipped Students' File Sharing Wings*, NETWORK COMPUTING (Feb. 19, 2004), *available at* http://cyber.law.harvard.edu/digitalmedia/Icarus%20at%20UF.htm.

for Integrated Computer Application for Recognizing User Services, effectively blocks the use of all P2P file sharing applications on the university's dormitory network.[107] However, ICARUS has a waiver provision whereby students and researchers may request permission to use P2P applications if they can prove it is for legitimate academic purposes.[108]

In terms of reducing instances of copyright infringement, ICARUS has been a complete success. Prior to the school's use of ICARUS, there were as many as three thousand five hundred infringing users at any given time at just one of the University of Florida's campuses. The moment the application was turned on, fifteen hundred infringers were caught.[109] Over time, the campus network experienced an eighty-five percent drop in uplink data volume.[110] In fact, the program is so successful that it is being marketed to universities across the country[111] and over one hundred schools have already expressed their interest.[112]

Another technological solution is Audible Magic's CopySense Network Appliance (CopySense).[113] CopySense is an application designed to block copyrighted songs from being traded via P2P applications, while allowing all other P2P traffic to flow through.[114] Currently, CopySense is being heavily promoted by the RIAA as a "filtering" solution to the P2P piracy problem, and the RIAA has specifically encouraged universities to adopt it.[115]

---

[107] *Id*.

[108] *Id. See* discussion, *supra* Part I.F.2.

[109] Joachim, *supra* note 106.

[110] Such a significant decrease in uplink data volume indicates less file-sharing because media files are large and thus consume a great deal of bandwidth. *Id*. *See* discussion, *supra* Part I.C.

[111] *See* Joachim*, supra* note 106.

[112] P2PNET.NET: U OF A ASKS U OF F FOR HELP (Nov. 21, 2003), http://p2pnet.net/story/193.

[113] AUDIBLE MAGIC: COPYSENSE, *supra* note 6.

[114] *Id.* at 3.

[115] Press Release, Recording Industry Association of America, Newsletter (Apr. 15, 2004), *available at* http://www.riaa.com/news/newsletter/ 041504.asp (noting that the RIAA has "hosted a series of demonstrations of Audible Magic's filtering product for key Congressional staff, higher education leaders and other policymakers").

CopySense works by examining, or "fingerprinting," all P2P network traffic at the content layer—"that is, it analyzes the actual file transferred in the application layer."[116] CopySense decodes this content to identify the application in use and then determines if it contains copyrighted material by cross referencing it with Audible Magic's database of copyrighted music.[117] Once copyrighted audio files are discovered, the system can actively block the transmission.[118] Like ICARUS, CopySense can also be configured to block all P2P traffic.[119] With CopySense installed, universities have been able to greatly reduce instances of P2P piracy as well as reclaim half of their network's bandwidth.[120] The result at one university campus was going from a rate of one notice of copyright infringement per week to none.[121] Before the Fall semester of 2004, CopySense was only running on two University networks; now it is running on about 30 to 40.[122]

Regardless of the kind of network use policy a university chooses to implement, use policy must be molded within the boundaries of academic freedom. Unlike the corporate world, universities face this additional restriction due to the unique role that they play in American society.

II. NOTIONS OF ACADEMIC FREEDOM IN LAW & POLICY

Academic freedom finds its roots in functional policy

---

[116] Chris Palmer, *Audible Magic – No Silver Bullet for P2P Infringement*, ELECTRONIC FRONTIER FOUNDATION, *available at* http://www.eff.org/share/audible_magic.php (last visited Nov. 30, 2004).

[117] AUDIBLE MAGIC: COPYSENSE, *supra* note 6, at 3. This database is updated regularly via the Internet and contains over 3.7 million registered works. *Id.*

[118] *Id.*

[119] AUDIBLE MAGIC CORP., COPYSENSE NETWORK APPLIANCE CASE STUDY [hereinafter AUDIBLE MAGIC CASE STUDY], *available at* http://www.audiblemagic.com/pdf/AudibleMagic-CaseStudyFresnoPacific.pdf.

[120] JOINT COMM. ON HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES, *supra* note 100.

[121] *Id.*

[122] Charlotte Hsu, *UCLA Uses Its Own Creation to Fight Illegal File-sharing*, DAILY BRUIN, Oct. 5, 2004, at 1.

considerations about the purpose of the university itself: its mission in promoting understanding through freedom in research and teaching, and, ultimately, in serving the public good. There is also a legal concept of academic freedom, which is sourced in both constitutional and contract law.

A. The American Association of University Professors' Policy on Academic Freedom

In 1915, the American Association of University Professors (AAUP), in conjunction with its administrative counterpart, the Association of American Colleges (AAC), issued the Declaration of Principles (1915 Declaration), which provides a comprehensive analysis of academic freedom in the United States.[123] According to the 1915 Declaration, the principle mission of the university is "discovering and disseminating knowledge to our students and to the public."[124] This report was later codified in the 1940 Statement on Principles on Academic Freedom and Tenure (1940 Statement).[125]

Both the 1915 Declaration and the 1940 Statement stress the importance of academic freedom, identifying three central principles: (1) freedom in research and publication; (2) freedom in the classroom; and (3) freedom from institutional censorship or discipline when speaking as a private citizen.[126] Speaking in

---

[123] AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS, GENERAL DECLARATION OF PRINCIPLES (1915) [hereinafter AAUP DECLARATION OF PRINCIPLES], *available at* http://www.campus-watch.org/article/id/566; David M. Rabban, *Functional Analysis of "Individual" and "Institutional" Academic Freedom Under the First Amendment*, 53 LAW & CONTEMP. PROBS. 227, 232 (1990); Walter P. Metzger, *Profession and Constitution: Two Definitions of Academic Freedom in America*, 66 TEX. L. REV. 1265, 1266 (1998).

[124] Letter from Robert Post to Richard C. Atkinson, President, University of California (March 12, 2003), at 2, *available at* http://www.universityof california.edu/senate/committees/ucaf/afforum/post_apm 010.pdf.

[125] AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS, 1940 STATEMENT OF PRINCIPLES ON ACADEMIC FREEDOM AND TENURE (1940) [hereinafter AAUP ON FREEDOM AND TENURE], *available at* http://www. aaup.org/statements/Redbook/1940stat.htm#[1].

[126] AAUP DECLARATION OF PRINCIPLES, *supra* note 123; AAUP ON

functional terms about academic freedom in research and teaching, the 1940 Statement noted that freedom in research "is fundamental to the advancement of truth" and that freedom in teaching is "fundamental for the protection of the rights of the teacher in teaching and of the student to freedom in learning."[127]

The 1915 Declaration "remains the foundation for the nonlegal understanding of academic freedom within the academic world."[128] It is so widely accepted and endorsed,[129] that the 1915 Declaration has become the standard creed of the American academic profession.[130] The AAUP recently released a report, entitled "Academic Freedom and Electronic Communications" (AFEC), which confirms that its original precepts of academic freedom extend to the unforeseen advances in electronic and digital communications that have since become "an integral part of academic discourse."[131]

In addressing the advent of Internet-based technologies, the AFEC report stresses that the "basic principles of academic freedom transcend even the most fundamental changes in media" and that "[a]cademic freedom, free inquiry and freedom of expression within the academic community may be limited to no greater extent in electronic format than they are in print."[132] Of

---

FREEDOM AND TENURE, *supra* note 125.

[127] AAUP ON FREEDOM AND TENURE, *supra* note 125.

[128] Rabban, *supra* note 123, at 231.

[129] AAUP DECLARATION OF PRINCIPLES, *supra* note 123. To date, 175 professional and academic organizations have endorsed the Declaration of Principles as codified in the 1940 Statement on Principles on Academic Freedom and Tenure. J. Peter Byrne, *Academic Freedom: A "Special Concern of the First Amendment,"* 99 YALE L.J. 251, 279 (1989) (noting that the 1940 Declaration "has been endorsed by every major higher education organization in the nation").

[130] Metzger, *supra* note 123, at 1266.

[131] AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS, ACADEMIC FREEDOM AND ELECTRONIC COMMUNICATIONS (Nov. 2004) [hereinafter AAUP ACADEMIC FREEDOM REPORT], *available at* http://www.aaup.org/statements/REPORTS/04AFelec.htm. While this report was initially published in 1997, it was recently amended to address the rapid advances in technology.

[132] *Id*. To be fair, the report also stresses that these core academic values may be limited in "the most unusual situation where the very nature of the

particular relevance to the P2P debate, the report also notes that changes in the methods by which information is obtained and disseminated, as well as the means for storing and retrieving such information, do not transcend the basic principles of academic freedom.[133] This is an important statement on academic freedom, as both the AAUP and the courts agree that academic freedom concerns both the method and the content of digital and electronic transmissions.[134]

B. Contractual Rights to Academic Freedom

Despite the proclivity of the courts[135] and proponents of open P2P access to couch academic freedom in terms of constitutional law, the legal boundaries of academic freedom are initially defined by contract law.[136] This is an important aspect of academic freedom as contract law applies to all institutions of higher learning, while constitutional law, with limited exceptions, only applies to public universities.[137] Every academic is in an employment relationship, and if it is not an at will relationship, there will be an employment contract that provides, either expressly or impliedly, for a form of academic freedom.[138] This, in turn, creates an enforceable legal right from which violations of academic freedom may be remedied.[139]

---

medium itself might warrant unusual restrictions." *Id*. At first blush, this would appear to apply to technology like P2P, but P2P technology cannot be separated from the technology of the internet itself, and as a result this exception would not apply. *See* discussion, *infra* Part III.

[133] *See* AAUP ACADEMIC FREEDOM REPORT, *supra* note 131.

[134] *See* discussion, *infra* Part II.C.

[135] *Id.*

[136] CONSTANCE S. HAWKE, COMPUTER AND INTERNET USE ON CAMPUS 72 (2001); Jim Jackson, *Express and Implied Contractual Rights to Academic Freedom in the United States*, 22 HAMLINE L. REV. 467, 473 (1999).

[137] HAWKE, *supra* note 136, at 72.

[138] Jackson, *supra* note 136, at 473.

[139] *See*, *e.g.*, Taggart v. Drake Univ., 549 N.W.2d 796 (Iowa 1996) (finding that there is "ample authority for the proposition that university rules, regulations, policies and bylaws can become implied terms of a faculty employment contract").

The reach of academic freedom in contract law is broad. In establishing a contractual right to academic freedom, a faculty member may be able to point to a variety of arguments, including: (1) "an express written clause guaranteeing academic freedom;"[140] (2) "a clause from another source incorporated by reference," such as the AAUP statement on academic freedom or faculty handbooks;[141] or (3) "a custom or tradition that academic freedom exists" at their university or universities generally.[142] Of particular importance are the AAUP guidelines on academic freedom because they are widely accepted and endorsed not merely as an ideal or aspiration, but the language is actually incorporated into the handbooks and bylaws of most universities.[143] As such, the courts may include the broad language of the AAUP statement on academic freedom as an express or implied term of a faculty employment contract.[144] For example, in the seminal case on faculty employment in higher education, *Green v. Howard University*, the D.C. Circuit noted that a university which accepts the policies of the AAUP "as guiding principles" in its faculty handbook will be contractually bound to those guidelines.[145]

Regardless, in the rare instance that academic freedom is not defined, or even mentioned, in an employment contract or a faculty handbook, the courts may apply a common law definition of academic freedom as "it is so entrenched in the very concept of an American university that it will be implied generally into employment contracts."[146] This common law definition will most

---

[140] Jackson, *supra* note 136, at 473.

[141] *Id.*

[142] *Id.*

[143] Metzger, *supra* note 123, at 1267.

[144] Jackson, *supra* note 136, at 490-93.

[145] 412 F.2d 1133, 1134 n.7 (D.C. Cir. 1969).

[146] Jackson, *supra* note 136, at 494.

> The notion of academic freedom is so entrenched in the definition of an organization that styles and describes itself as a university that the institution itself will be very hard pressed to deny the legal existence of such freedom rights in its faculty – freedoms most likely acquired as a contractual custom or tradition in the faculty's employment relationship with the university. It certainly places the onus on the "universities" that would seek to narrow the academic freedom rights of faculty

likely include the AAUP's 1940 Statement.[147]

C. Constitutional Rights to Academic Freedom

While contract law applies to all institutions of higher learning, public universities enjoy additional academic freedom protections under the First Amendment.[148] However, while academic freedom is clearly recognized as a legal right under the First Amendment, its precise legal definition and application are elusive and inconsistent.[149] Given this ambiguity, it is not clear whether there is a constitutional academic freedom to unrestricted access to the internet in general, or to P2P technologies specifically.[150] A cursory review of the major case law surrounding constitutional academic freedom is necessary to analyze the larger policy rationales supporting an academic freedom to unrestricted P2P access, as these policy arguments underlie the language of these cases. Moreover, while a constitutional academic freedom may be vague as a general proposition, at least two cases provide strong support for the contention that overly restrictive network use policies will be found unconstitutional on academic freedom and prior restraint grounds.[151]

---

members to do so clearly and openly.

Id. at 469.

[147] *Id*.

[148] HAWKE, *supra* note 136, at 72.

[149] *See* Hillis v. Stephen F. Austin State Univ., 665 F.2d 547, 553 (5th Cir. 1982), *cert. denied*, 457 U.S. 1106 (1982) (noting that academic freedom is well recognized, but its perimeters ill-defined and the case law defining it is inconsistent); Mahoney v. Hankin, 593 F. Supp. 1171, 1174 (S.D.N.Y. 1984) (noting parameters of academic freedom are ill-defined). *See also* Rabban, *supra* note 123, at 230 (noting that the Supreme Court's analysis of academic freedom has produced "scant, and often ambiguous, analytic content"); Byrne, *supra* note 129 ("Lacking definition or guiding principle, the doctrine [of academic freedom] floats in the law, picking up decisions as a hull does barnacles.").

[150] A comprehensive analysis of this question is well beyond the scope of this note.

[151] *See generally*, Urofsky v. Gilmore, 216 F.3d 401, 441 (4th Cir. 2000), *cert. denied*, 531 U.S. 1070 (2001); Loving v. Boren, 133 F.3d 771 (10th Cir. 1998).

While the right of academic freedom is "not a specifically enumerated constitutional right,"[152] the Supreme Court imputed a constitutional right in a series of cases in the 1950's and 1960's, recognizing a right to academic freedom under the First Amendment freedoms of speech and association.[153] In 1957, the Supreme Court first recognized a First Amendment academic freedom right in *Sweezy v. New Hampshire*.[154] *Sweezy* upheld a Professor's right to refuse to testify in a state investigation regarding the content of his lectures and other related matters, on First Amendment grounds.[155] While this case is far removed from the current P2P controversy, Chief Justice Warren's plurality opinion contains the Court's most comprehensive discussion of academic freedom:[156]

> The essentiality of freedom in the community of American universities is almost self-evident. No one should underestimate the vital role in a democracy that is played by those who guide and train our youth. To impose any strait jacket upon the intellectual leaders in our colleges and universities would imperil the future of our Nation. No field of education is so thoroughly comprehended by man that new discoveries cannot yet be made . . . . Teachers and students must always remain free to inquire, to study and to evaluate, to gain new maturity and understanding; otherwise our civilization will stagnate and die.[157]

This famous paragraph highlights the foundational concepts of constitutional academic freedom; notably, the critical role universities play in the preservation of democracy and the promotion of discovery and understanding.[158]

---

[152] Regents of the Univ. of Cal. v. Bakke, 438 U.S. 265, 312 (1978).

[153] HAWKE, *supra* note 136, at 72; Sweezy v. N.H., 354 U.S. 234 (1957).

[154] 354 U.S. 234 (1957).

[155] *Id*. at 238-41.

[156] Rabban, *supra* note 123, at 239.

[157] *Sweezy*, 354 U.S. at 250.

[158] *See* Rabban, *supra* note 123, at 239 (noting that Chief Justice Warren's statement recognized two distinct social benefits of academic freedom: critical inquiry as an essential tool to promote democracy and the promotion of "discoveries and understanding necessary for civilization").

A decade later, in *Keyishian v. Board of Regents*,[159] the Supreme Court used similarly expansive language to discuss the First Amendment right to academic freedom when it invalided political tests for public university employment.[160] Writing for the majority, Justice Brennan reasoned that "[o]ur Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers," and as a result academic freedom is "a special concern of the First Amendment."[161]

In *Keyishian*, the Court again presented a sweeping view of the role academic freedom plays in protecting the future of the country, noting that the classroom is a "market place of ideas"[162] and that "[t]he Nation's future depends upon leaders trained through wide exposure to that robust exchange of ideas which discovers truth out of a multitude of tongues, [rather] than through any kind of authoritative selection."[163] While the Court again did not give a precise definition of constitutional academic freedom, it is clear from the opinion that academic freedom requires an open minded environment where access to information is not unnecessarily restricted.[164] Without such "breathing space," Justice Brennan warns of the danger of a "chilling effect" upon the exercise of First Amendment academic freedom rights, noting that "when one must guess what conduct or utterance may lose him his position, one necessarily will 'steer far wider of the unlawful zone'"[165] as "[t]he threat of sanctions may deter almost as potently as the actual application of sanctions."[166]

These early cases left some doubt as to whether the Court was conferring First Amendment protection upon members of the faculty as individuals only, or the university as an institution.[167] In

---

[159] 385 U.S. 589 (1967).

[160] *Id.* at 603.

[161] *Id.*

[162] *Id.*

[163] *Id.* (internal quotations omitted).

[164] Keyishian v. Board of Regents, 385 U.S. 589 (1967).

[165] *Id.* at 685 (citing Speiser v. Randall, 357 U.S. 513, 526 (1958)).

[166] *Id.* (citing N.A.A.C.P. v. Button, 371 U.S. 415, 433 (1963)).

[167] Robert M. O'Neil, *Academic Freedom and the Constitution*, 11 J.C. &

later cases, however, the Court made clear that a First Amendment academic freedom is conferred upon both.[168] Moreover, while the vast majority of Supreme Court jurisprudence on academic freedom concerns the rights of teachers and of the university, it has implied that similar constitutional academic freedom protections also extend to students, under First Amendment freedoms of speech and association.[169] Lower courts have imputed this right as well.[170] Regardless, students enjoy the First Amendment's protection of academic freedom because if a professor's right to research and to teach is protected, it follows that a student has the right to receive this information.[171]

D. Academic Freedom and Internet Access

The holdings of the Supreme Court in both *Sweezy* and *Keyishian* are authoritative, leaving little doubt that academic freedom is a constitutionally-protected right. However, courts have also held that schools, as well as the state, may nonetheless balance First Amendment rights against other legal and societal interests.[172]

U.L. 275, 281 (1984).

[168] Regents of the Univ. of Mich. v. Ewing, 474 U.S. 214, 226 n.12 (1985).

[169] *See* Healy v. James, 408 U.S. 169 (1972); Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503 (1968). *See also* Rosenberger v. Rector and Visitors of Univ. of Va., 515 U.S. 819, 836 (1995).

> The quality and creative power of student intellectual life to this day remains a vital measure of a school's influence and attainment. For the University, by regulation, to cast disapproval on particular viewpoints of its students risks the suppression of free speech and creative inquiry in one of the vital centers for the Nation's intellectual life, its college and university campuses.

Id.

[170] Piarowski v. Ill. Cmty Coll. Dist., 759 F.2d 625, 629 (7th Cir. 1985) (noting that academic freedom is used to denote the freedom "of the individual teacher (or in some versions–indeed in most cases–the student) to pursue his ends without interference from the academy").

[171] *See* Minarcini v. Strongsville City Sch. Dist., 541 F.2d 577, 582 (6th Cir. 1976) (noting that the First Amendment's protection of academic freedom protects both the right of the teacher to speak and the students' right to listen).

[172] Widmar v. Vincent, 454 U.S. 263, 268 n.5 (1981) (reasoning that a "university's mission is education, and decisions of this Court have never denied

Both the state and universities themselves may restrict the speech and other conduct of the faculty, student, and staff in order to protect an educational mission and maintain an efficient educational system.[173] In essence, universities have the legal right to somewhat limit where information can be emitted and where it can be obtained.[174] While the Supreme Court has never considered in what manner a public university may restrict access to the internet in general, or P2P technology specifically, lower courts have examined the extent to which both the state and university officials may restrict internet use.[175]

In *Loving v. Boren*,[176] the United States District Court for the Western District of Oklahoma evaluated a decision by the University of Oklahoma to block access to a large number of sexually related internet newsgroups[177] because it violated state law banning the distribution of obscene material.[178] A professor sued on grounds that restricting access to the internet violated his academic freedom under the First Amendment.[179] The court examined the university's internet use policy to determine if it indeed met constitutional requirements.[180] In its examination, the court noted that before trial the university had set up an alternative "B" server to provide access to all newsgroups, including those

---

a university's authority to impose reasonable regulations compatible with that mission upon the use of its campus and facilities"); Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503, 507 (1969) (noting the "comprehensive authority of the states and of school officials, consistent with fundamental constitutional safeguards, to prescribe and control the conduct in the schools").

[173] *Widmar*, 454 U.S. 263, 268 n.5 (1981).

[174] Philip T.K. Daniel & Vesta A.H. Daniel, *A Legal Portrait of the Artist and Art Educator in Free Expression and Cyberspace*, 140 ED. LAW REP. 431, 447 (2000).

[175] *See, e.g.*, Urofsky v. Gilmore, 216 F.3d 401 (4th Cir. 2000); Loving v. Boren, 133 F. 3d 771 (10th Cir. 1998).

[176] 956 F. Supp. 953, 954 (W.D. Okl. 1997).

[177] "News groups are interactive 'places' on the Internet into which anyone with access, anywhere in the world, may place graphic or text messages." *Id.*

[178] *Id*.

[179] *Id.*

[180] *Id.* at 955.

that had been previously blocked.[181] According to the terms of use, users of the "B" server had to be over 18 years old and were restricted to accessing the newsgroups for academic and research purposes.[182] The court found that since newsgroup access by an adult was plenary on at least the "B" server, the new policy did not run afoul of First Amendment academic freedom rights.[183]

While the court held against the professor, its internet access test is very useful in examining the legality of restricting P2P use. According to the court in *Loving*, where there is a question of an unconstitutional violation of academic freedom on the internet, there will be an inquiry into whether users have unfettered access to the internet for academic and research purposes.[184] If there is not, it is likely the law or policy will be struck down.[185] The Fourth Circuit applied this same reasoning in *Urofsky v. Gilmore*.[186]

In *Urofsky*, the Fourth Circuit considered *en banc* whether a Virginia state law that restricted state employees from accessing sexually explicit material on computers that are owned or leased by the state was inconsistent with academic employees' right to academic freedom.[187] In a widely criticized opinion,[188] the majority

---

[181] *Id.*

[182] *Loving*, 956 F. Supp. at 955.

[183] *Id*. Moreover the court noted that: "Whatever the constitutional state of affairs may have been before the new policy was enacted, the current situation meets constitutional requirements." *Id.* On appeal, the Tenth Circuit held for the university on grounds that the professor lacked standing as he never attempted to access any of the newsgroups. Loving v. Boren, 133 F. 3d 771, 773 (10th Cir. 1998).

[184] *Loving*, 956 F. Supp. at 955.

[185] *Id.* (noting that a university may lawfully restrict internet use to academic and research uses only when access by an adult is plenary).

[186] 216 F.3d 401, 404 (4th Cir. 2000).

[187] *Id.* at 405-06.

[188] J. Peter Byrne, *Constitutional Academic Freedom in Scholarship and in Court*, THE CHRONICLE OF HIGHER EDUCATION (Jan. 5, 2001) (noting that "[b]ecause the [*en banc Urofsky*] court relied in no small part on a scholarly article by me to support its conclusion, I feel a duty to express my professional view that the opinion is profoundly wrong as a matter of law, and threatens the freedom of higher education"). *See also* Michael D. Hancock, *The Fourth Circuit's Narrow Definition of 'Matters of Public Concern' Denies State-Employed Academics Their Say:* Urofsky v. Gilmore, 6 RICH. J.L. & TECH. 11

held that the Act was constitutional because it did not affect speech by the academic employees in their capacity as private citizens speaking on matters of public concern.[189] Moreover, the court held that any right to academic freedom belongs to the university rather than to individual professors.[190] However, like the *Loving* court, the Fourth Circuit was concerned whether there was a means by which a user may obtain unfettered internet access. Both Justice Wilkin's majority opinion and Chief Justice Wilkinson's concurrence note that the state law was constitutional, in part, because it explicitly provided for a waiver by which academic users could obtain full access to the internet for all *bona fide* research projects.[191]

While agreeing that the Act was facially constitutional partly due to the waiver provision, Chief Judge Wilkinson took the opportunity to write separately because the Act "restricts matters of public concern, especially in the context of academic inquiry."[192] Specifically, Wilkinson, much like Justice Brennan in *Keyishian*, was concerned with the danger of a "chilling effect" on academic freedom, noting that the Act "constitutes a prior restraint because it chills Internet research before it even happens."[193] As such, he reasoned that limiting a professor's ability to use the internet to research and write is a "wholesale deterrent to a broad category of expression by a massive number of potential speakers."[194] This result, Wilkinson argued, is inconsistent with academic freedom because internet research "lies at the core" of our intellectual and philosophic tradition.[195]

In a vigorous dissent, Justice Murnaghan furthered Wilkinson's prior restraint concerns, and also took issue with the Act's prior

---

(Fall 1999); Michael D. Hancock, *Why* Urofsky v. Gilmore *Still Fails to Satisfy*, 6 RICH. J.L. & TECH. 14 (Winter 1999).

[189] *Urofsky*, 216 F.3d at 404.

[190] *Id.* at 420.

[191] *Id.* at 404, 426.

[192] *Urofsky*, 216 F.3d at 426.

[193] *Id*. at 426.

[194] *Id.* (citing United States v. Nat'l Treasury Employees Union, 513 U.S. 545, 467 (1995)).

[195] *Id*. at 428.

approval provision.[196] According to Murnaghan, the Act's prior approval process is unconstitutional because it "has no check on discretionary authority," which invites "arbitrary enforcement."[197] He reasoned that such arbitrary enforcement is unconstitutional because it permits a university official to decide what is and what is not a bona fide research project based upon the content of the project or the viewpoint of the speaker.[198] As Justice Murnaghan pointed out, the Supreme Court found such discretion unconstitutional in a related First Amendment context.[199] Moreover, Murnaghan reasoned that even if there was no arbitrary enforcement, the Act would still be unconstitutional on prior restraint grounds because the "mere existence of the licensor's unfettered discretion, coupled with the power of prior restraint, intimidates parties into censoring their own speech, even if the discretion and power are never actually abused."[200]

III. ANALYSIS

Against this backdrop of the legal justifications for providing open access to P2P technology, universities and colleges have choices as to how to provide access. As noted, some deal with the liability that they might have for copyright infringement through educational initiatives alone. Technological options have also emerged. However, there are implementation problems from the perspective of contractual and constitutional guarantees of academic freedom as well as other legal and policy concerns.

A. The Problem With Technological Solutions

---

[196] *Id*. at 441 (Murnhagan, J. dissenting).

[197] *Id*.

[198] *Urofsky*, 216 F.3d at 441 (4th Cir. 2000).(citing City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750 (1988)).

[199] *Lakewood*, 486 U.S. at 772 (holding that the statute giving the mayor unbridled discretion to deny a newsrack permit application and unbounded authority to condition the permit on any additional terms he deems "necessary and reasonable" is unconstitutional).

[200] Urofsky v. Gilmore, 216 F.3d 401, 441 (4th Cir. 2000) (Murnhagan, J. dissenting) (citing *Lakewood*, 486 U.S. at 757).

Many universities have adopted network use policies that include overly burdensome technological solutions such as ICARUS and CopySense.[201] This has occurred despite efforts by legal experts to persuade universities that employing technological measures to police P2P piracy is not required by law, will increase liability,[202] and will erode the academic freedom of both teachers and students.[203]

Some universities have no choice but to implement some form of bandwidth management technology to control excessive bandwidth.[204] Examples of legitimate technological impediments that universities employ to manage bandwidth include throttling the internet speeds for P2P programs (bandwidth shaping), capping the amount of data each user is allowed to upload and download per week, and reprimanding "top talkers" or "bandwidth hogs."[205] While it is unfortunate that these measures will inevitably curtail the legitimate academic use of P2P technology, it appears likely that rapid advances in bandwidth speed will quickly supersede the need for such measures.[206]

As for the various types of technological impediments that erode academic freedom, two specific examples, ICARUS[207] and

---

[201] *See* discussion, *supra* Part I.F.2.

[202] See discussion, *supra* Part I.E.

[203] *See* ELECTRONIC PRIVACY INFORMATION CENTER: EPIC LETTER ON P2P MONITORING TO COLLEGES AND UNIVERSITIES 1 (Nov 6, 2002), *available at* http://www.epic.org/privacy/student/p2pletter.html; ELECTRONIC FRONTIER FOUNDATION, UNIVERSITIES SHOULD RESIST NETWORK MONITORING DEMANDS, *available at* www.eff.org/IP/P2P/university-monitoring.pdf.

[204] *See* discussion, *supra* Part I.C.

[205] *See* JOINT COMM. ON HIGHER EDUCATION AND ENTERTAINMENT COMMUNITIES, *supra* note 100; Spanier Statement, *supra* note 5; Dawn C. Chmielewski, *Colleges Ambivalent About Anti-Piracy Role*, SILICONVALLEY.COM (Feb. 18, 2003), *available at* http://www.uh.edu/admin/media/topstories/2003/silval/200302/20030221pir.html.

[206] Duncan Martell, *Ultrawideband Heralds Zippier Wireless Connections*, REUTERS (Oct. 9, 2004), *available at* http://www.usatoday.com/tech/wireless/data/2004-10-06-ultrawideband-preview_x.htm.

[207] *See* discussion, *supra* Part.I.F.2.

CopySense Network Appliance (CopySense),[208] highlight how these solutions defile basic principles of academic freedom and exemplify the broader legal and policy problems of technological restrictions on network use.[209]

1. ICARUS

Arguably, ICARUS has been a complete success for universities seeking to avoid infringement liability; it successfully blocks all infringing use of P2P file sharing applications. Seen through the lens of academic freedom, however, ICARUS is a complete failure. In clipping the wings[210] of P2P file sharing applications, ICARUS blocks all file sharing, which includes both infringing and non-infringing use.[211] Such a policy violates core principles of academic freedom.[212] By completely blocking an important method by which academics conduct research and inquiry, by which they study and evaluate, ICARUS defiles the very purpose of academic freedom, which is to promote discovery and understanding.[213] In other words, ICARUS raises barriers to learning although it is part of the university mission to lower them.[214] To shut down technology simply because it is difficult and has infringing use[215] runs counter to 90 years of policy and jurisprudence on academic freedom.[216] Regardless of the unique role academic freedom plays in the university setting, banning technology that is merely capable of infringing use should strike everyone as excessive in any setting considering that the very same concerns may be raised over P2P as with the now ubiquitous

---

[208] *See* discussion, *supra* Part I.F.2.

[209] *See* discussion, *infra* Part III.

[210] Joachim, *supra* note 106.

[211] *Id.*; AMERICAN COUNCIL ON EDUCATION, *supra* note 75, at 4.

[212] *See* discussion, *supra* Part II.

[213] *Id.*

[214] *Id.*

[215] *See* Brief of Amici Curiae American Civil Liberties Union et al., *supra* note 37, at 30.

[216] *See* discussion, *supra* Part II.

technologies of the copy machine and the video recorder.[217]

This is why university administrators at the forefront of P2P piracy debate have stressed that universities should be reluctant to embrace any technology that would block both legitimate and illegitimate uses of P2P technology indiscriminately.[218] As one University President notes, such an approach would "stifle the very creativity and experimentation that has brought us the extraordinary technological capacities that enrich our lives today."[219] Another administrator simply describes technology like ICARUS as "draconian." [220] Even the RIAA is ambivalent about such a drastic approach to P2P piracy.[221] According to the former Chairman and CEO of the RIAA: "It is the misuse of technology that must be stifled, not the technology itself. We believe that P2P technology will offer great benefits for legitimate use."[222]

The courts see similar threats to academic freedom in restricting access to modes of transmission and reception at the university.[223] In his concurrence in *Urofsky*, Chief Justice Wilkinson warns: "The right to academic inquiry . . . cannot be divorced from access to one means (the Internet) by which the inquiry is carried out. By restricting Internet access, a state thus restricts academic inquiry at what may become its single most

---

[217] *See* Lessig, *supra* note 33.

> There is no way to assure that a P2P system is used 100 percent of the time in compliance with the law, any more than there is a way to assure that 100 percent of VCRs or 100 percent of Xerox machines or 100 percent of handguns are used in compliance with the law.

Id.

[218] *See* Spanier Statement, *supra* note 5; Hess Statement, *supra* note 68.

[219] Spanier Statement, *supra* note 5.

[220] David Jaochim, *University Gets Tough on P2P*, SECURITYPIPELINE (Feb. 18, 2004), *available at* http://securitypipeline.com/trends/17701191 (quoting Richard Holeton).

[221] *Intellectual Property Piracy at U.S. Colleges: Before the Subcomm. on Courts, the Internet, and Intellectual Property Comm. on the House Judiciary*, 108th Cong. (2003) (statement of Hilary Rosen, Chairman and CEO, RIAA).

[222] *Id.*

[223] Urofsky v. Gilmore, 216 F.3d 401, 428-33 (4th Cir. 2000) (Wilkinson, C.J., concurring).

fruitful source."[224] Chief Justice Wilkinson has an acute sense of the perils of restricting inquiry on the internet; it is unparalleled in access to information, "holding tremendous promise for virtually all types of research."[225]

While Chief Justice Wilkinson speaks about restricting internet access generally, there should be no doubt that barring legitimate P2P use is to turn away from the internet itself.[226] If it were not for the P2P nature of the internet, the World Wide Web would never have been invented in the first place.[227] As such, P2P file sharing is "part of the fundamental design of the internet and it simply cannot be turned off in any categorical way."[228] Seen in this light, banning legal P2P use is not compatible with any number of a university's core values of academic freedom, such as the promotion of free and open exchange of ideas, and of discovery and understanding.[229]

Of course, at least in a constitutional sense, a university is well within its right to curtail activity that interrupts the efficient operation of its network.[230] However, the solution must be shaped around academic freedom values so it is not overly restrictive, or even illegal.[231] Regardless, there is serious doubt as to whether ICARUS makes the network more efficient, which points to other

---

[224] *Id.* at 428.

[225] *Id*. at 433.

[226] *See* Murray Statement, *supra* note 19 (noting that "[p]eer-to-peer sharing of resources is part of the fundamental design of the Internet and it simply cannot be turned off in any categorical way").

[227] *Dangers of File Sharing: Before the Comm. on House Gov. Reform*, 108th Cong. (2003) [Schiller Statement II] (statement of Jeffrey I. Schiller, Network Manager/Security Architect, Mass. Institute of Technology). Schiller relates the story of a programmer working for CERN in Switzerland who would not be able to modernize the telephone directory without P2P technology, and as a result invented the World Wide Web. *Id*.

[228] Murray Statement, *supra* note 19.

[229] *See* discussion, *supra* Part II.

[230] *Id.*

[231] *See* AMERICAN COUNCIL ON EDUCATION, *supra* note 75, at 4 (finding that "some observers have expressed serious concerns" that ICARUS is restricting resources too strictly).

problems with using a technological impediment.[232] One University of Florida student complains that "you can't go a day without someone in a dorm saying that their internet connection has stopped working [and that] can be really frustrating when you are taking a timed on-line quiz or trying to accomplish other schoolwork."[233]

ICARUS would likely survive constitutional scrutiny in at least two Circuits because of its waiver provision which allows unfettered use of P2P applications for bona fide research projects.[234] Yet, this does not absolve the University of Florida, or any other university, of their obligations under contract law and other policy issues surrounding academic freedom.[235] First, it may be difficult to determine what qualifies as an official academic project under a waiver provision.[236] As P2P technology so aptly demonstrates, new areas of learning often begin at the fringes; what may be seen as a non-academic endeavor today may be recognized as important academic research tomorrow.[237] Thus, a waiver provision may stymie legitimate academic inquiry and research so it "should strike virtually everyone as a violation of academic freedom."[238]

Second, there is no guarantee that approvals will not be

---

[232] P2PNET.NET, U OF FLORIDA AS RIAA ENFORCEMENT AGENCY, http://www.p2pnet.net/8281.html (last visited Nov. 15, 2004). *See* discussion, *supra* Part III.B.

[233] P2PNET.NET, *supra* note 232.

[234] *See* discussion, *supra* Part II.C.

[235] *See* discussion, *supra* Part II.B.

[236] Schiller Statement II, *supra* note 227.

[237] *Id.*

[238] *See* David M. Rabban, *Does Academic Freedom Limit Faculty Autonomy?*, 66 TEX. L. REV. 1405, 1419 (1988). While Rabban is referring to the prior approval process as a violation of academic freedom in regards to faculty, it is not a far leap to see how this would be a violation of student academic freedom. Also, the AAUP explicitly grants graduate students, who may reside in campus dormitories, the same rights of academic freedom as faculty members. AMERICAN ASSOC. OF UNIV. PROFESSORS: STATEMENT ON GRADUATE STUDENTS, *available at* http://www.aaup.org/statements/Redbook/Gradst.htm ("Free inquiry and free expression are indispensable.").

withheld arbitrarily[239] and a "refusal to approve a particular research project might raise genuine questions—perhaps even constitutional ones—concerning the extent of the authority of a university to control the work of its faculty."[240] Who is to say that a faculty research project, or simply a class assignment, will not entail the use of a P2P file sharing application, whose basic purpose is to allow students to access the program anywhere there is a network connection?[241] Lastly, as the courts have noted, the waiver provision may constitute an impermissible prior restraint on academic freedom as it may chill research before it happens.[242]

2. CopySense Network Appliance

While proponents of CopySense endorse it as an innocuous "filter," it is at best an invasive content-monitoring tool and at worst an illicit wiretap.[243] Technology like CopySense presents multiple problems to academic freedom. First and foremost, CopySense does not simply monitor network traffic, but delves

---

[239] Urofsky v. Gilmore, 216 F.3d 401, 451 (4th Cir. 2000) (C.J. Murnhagan dissenting).

[240] *Id*. at 415 n.17.

[241] *See* discussion, *supra* Part I.B.

[242] *Urofsky*, 216 F.3d at 425 (C.J. Hamilton concurring). *See* discussion, *supra* Part III.B.2.

[243] Letter from Adam M. Eisgrau, Executive Director, P2P United, to Mitch Bainwol, Chairman, Recording Industries of America (Nov. 22, 2004) (on file with the *Journal of Law and Policy*) (describing CopySense as "a warrantless wiretap designed to divert and privately inspect potentially every file requested by a P2P user"). Eisgrau further notes that since the Federal courts have concluded that P2P software is used for substantial non-infringing uses, the public is owed a "clear explanation as to why the public should be required to subject their electronic communications to ungoverned surveillance by an understandably parochial industry collective." *See also* Ernest Miller, *Does Audible Magic Violate Wiretap Laws?,* CORANTE TECH NEWS (Jul. 14, 2004), *available at* http://www.corante.com/importance/archives/004986. html. Miller argues that CopySense's monitoring and logging of P2P streams in order to analyze their contents appear to be a violation of Federal wire tapping law under 18 U.S.C. § 2511. *Id*. According to Miller, the elements of an illicit wiretapping are satisfied as CopySense acquires the contents of electronic communications without the consent of the communicating parties. *Id.*

into the actual content of the data flowing through the network.[244] This data may consist not only of infringing sound files, but all other non-infringing data, including personal e-mails, documents exchanged, even confidential counseling and grade reports.[245] In other words, CopySense is more accurately described as a surveillance tool for ubiquitous content monitoring, than as a "filter."

Content monitoring significantly infringes upon academic freedom as it chills "the climate for inquiry and research."[246] As one professor notes, content monitoring is "absolutely destructive to the university, because it creates a chilling environment when we want to have an environment of openness and creativity."[247] Knowing that the information they send and receive is being actively monitored and logged,[248] both students and faculty may restrain their legitimate use of P2P technology,[249] thus chilling research and inquiry before it even happens.[250]

Under this type of surveillance regime the network user will engage in self-censorship,[251] restricting her use of P2P technology

---

[244] AUDIBLE MAGIC: COPYSENSE, *supra* note 6; Palmer, *supra* note 116.

[245] ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 203. *But see* Chris Palmer & Seth Schoen, *Debunking Audible Magic — Again*, ELECTRONIC FRONTIER FOUNDATION, *available at* http://www.eff.org/ share/?f=audible_ magic2.html. In a response to criticism of its application, Audible Magic claims that CopySense "does not report or intercede on email, FTP, or even HTTP traffic." However, there is no technical reason why it cannot be made to do so. *Id.*

[246] ELECTRONIC FRONTIER FOUNDATION, *supra* note 203.

[247] Chmielewski, *supra* note 205.

[248] "Logging" is the "[p]rocess of systematically or automatically collecting information and recording it to a detailed document for later study and analysis." In order to analyze the content for copyrighted songs, CopySense must first log it. AUDIBLE MAGIC: COPYSENSE, *supra* note 6, at 3 (noting that CopySense logs "all P2P transactions or attempts").

[249] ELECTRONIC FRONTIER FOUNDATION, *supra* note 203; ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 203, at 1 (noting that "[m]onitoring chills behavior, and can squelch creativity that must thrive in the in educational settings"). *See* discussion, *supra* Part II.

[250] *See* Urofsky v. Gilmore, 216 F.3d 401, 426 (4th Cir. 2000) (Wilkinson, J., concurring).

[251] *Id.* at 438 (Murnachan, J. dissenting).

whether or not the use is infringing on a copyright.[252] Such restraint inevitably leads to "less variety and diversity of creative output"[253] and hampers "independence of thought in decisions about both the consumption and creation of information."[254] Thus, content monitoring limits the legitimate use of P2P technology as a method for collaboration, inquiry, and research. The impact of this restraint is significant and the violation of academic freedom is severe.[255]

This effect defiles core values of academic freedom such as the freedom to research, the freedom to inquire, and the freedom to exchange information freely and openly.[256] For example, under the AAUP's first basic tenet of academic freedom—the right to research and publication—professors and graduate students enjoy the freedom to pursue research and to transmit "the fruits of inquiry to the wider community"[257] without prior restraint because it is "essential to the advancement of knowledge."[258] As members of the academy, this right is implied to students as well.[259]

Moreover, absent a showing of a compelling countervailing interest, at least one court has expressed its intolerance of prior restraint upon internet research under the First Amendment right to

---

[252] *See* Julie Hilden, *Should Universities Crack Down on File Swapping?*, FINDLAW (Mar. 4, 2003), *available at* http://writ.news.findlaw.com/hilden/20030304.html; ELECTRONIC FRONTIER FOUNDATION, *supra* note 203 (noting that "[s]tudents who fear that their every communication will be monitored and stored will feel less free to engage in . . . experimentation").

[253] Cohen, *supra* note 7, at 7.

[254] *Id.*

[255] Specifically, consider Chief Justice Earl Warren's famous words: "Teachers and students must always remain free to inquire, to study and to evaluate, to gain new maturity and understanding; otherwise our civilization will stagnate and die." Sweezy v. N.H. 352 U.S. 234, 250 (1957). *See also* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 203 (noting that monitoring is incompatible with intellectual freedom).

[256] *See* discussion, *supra* Part II.

[257] AMERICAN ASSOC. OF UNIV. PROFESSORS: ACADEMIC FREEDOM IN THE MEDICAL SCHOOL, ACADEME ¶ 5 (Jul.-Aug., 1999), *available at* http://www.aaup.org/publications/Academe/1999/99ja/JA99RPTS.HTM.

[258] *Id.*

[259] *See* discussion, *supra* Part II.C.

academic freedom.[260] In a related context, the Supreme Court has echoed this sentiment, noting that when the power of prior restraint intimidates parties into self-censorship, it is uniformly unconstitutional.[261] And regardless of these constitutional protections, most professors and other researchers are protected against such violations of academic freedom in their employment contracts.[262]

In defending itself against critics of content monitoring, Audible Magic claims that CopySense stops the transfer of copyrighted files instead of focusing on monitoring content.[263] This claim is undermined by the company's marketing, which touts this technology as "content-aware,"[264] mentions the monitoring of users as one of CopySense's three main functions, and presents "log and report" as the primary policy it can implement.[265] Furthermore, while Audible Magic highlights the fact that it only identifies the specific contents of a packet that contains copyrighted material, it can nonetheless monitor and log all

---

[260] Urofsky v. Gilmore, 216 F.3d 401, 426 (4th Cir. 2000) (C.J. Wilkinson concurring). Wilkinson noted that the state had "a legitimate interest in preventing its employees from accessing on state-owned computers sexually explicit material unrelated to their work" and that the waiver provision for bona fide research made the Act minimally intrusive. *Id*. Regardless, Wilkinson found the Act's restriction "constitutes a prior restraint because it chills Internet research before it happens." *Id*. Arguably, unlike the instant case, students and professors use P2P in relation to their work, i.e. research. Thus it appears likely that Wilkinson might find such a policy unconstitutional, and certainly impermissible under a professor's employment contract.

[261] City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750 (1988). *See also* Thornhill v. Ala., 310 U.S. 88, 97 (1940) (noting that "it is not merely the sporadic abuse of power by the censor but the pervasive threat inherent in its very existence that constitutes the danger").

[262] *See* discussion, *supra* Part II.B.

[263] *See* Palmer & Schoen, *supra* note 245.

[264] Press Release, Audible Magic Corp., Audible Magic Tests "Content – Aware" Network Monitoring System at University of Wyoming for Intelligent Management of P2P (Feb. 18, 2002) [hereinafter Audible Magic Content Aware Press Release], *available at* http://www.audiblemagic.com/news/press-releases/pr-2002-02-18.asp.

[265] "Log and report" appears first on the company web site's list of the policies it can implement. *Id*. *See* Palmer, *supra* note 116.

network content down to the name of the user transferring a file and the title of the file being transferred.[266]

Universities across the country are rejecting network use policies that employ any type of technology that monitors the content of network traffic for that reason.[267] The University of Wyoming, which was the first to test and use Audible Magic[268] discontinued its use in the face of repeated criticism.[269] Another university declined to use CopySense on grounds that "[i]t gets too close to policing, . . . looking into our own networks and looking for our own behavior."[270] At present, no legal action has been brought against a university for using CopySense on grounds that it is a breach of contract[271] or an unlawful invasion of privacy.[272] It is simply too early to determine CopySense's legality; however, the application does seem to invite litigation, based either on breach of contract[273] or an unlawful invasion of privacy theories.[274]

B. All Technological Solutions are Problematic

Aside from the overt threats to academic freedom in using

---

[266] AUDIBLE MAGIC: COPYSENSE, *supra* note 6.

[267] Zachary Goldstein, *College Unlikely to Adopt New File-Sharing Filter*, DARTMOUTH ONLINE (Apr.13, 2004), http://www.thedartmouth.com/article.php?aid=2004041301020; Jane Black, *Music Pirates at the Naval Academy?*, BUSINESSWEEK ONLINE (Nov. 27 2002), http://www.businessweek.com/technology/content/nov2002/tc20021127_2314.htm. Black notes that despite the fact that universities would love to rid their networks of the "file sharing plague," many universities prefer to take the "hands-off" approach to copyright infringement as "[f]ears are rampant that the ubiquitous monitoring required to eliminate file-sharing would chill free speech and squelch the creativity that's an integral part of university life." *Id*.

[268] Audible Magic Content Aware Press Release, *supra* note 264.

[269] Annalee Newitz, *Don't Look Now, but the Dean is Watching*, SALON.COM (Nov.12, 2003), http://www.salon.com/tech/feature/2003/11/campus _surveillance.

[270] Hsu, *supra* note 122, at 2.

[271] *See* discussion, *supra* Part II.B.

[272] *See* discussion, *supra* Part II.B.

[273] *See* discussion, *supra* Part II.B.

[274] *See* discussion, *supra* Part II.

technological impediments like CopySense and ICARUS, there are at least three other significant legal and practical problems that erode academic freedom in ways that further diminish the utility of technological impediments in defeating copyright infringement.

First, the use of any technology to control network user behavior implicates "surveillance creep," which is "the tendency to increase the potential and range of surveillance capabilities."[275] The danger of surveillance creep on the university campus is that technological impediments to P2P, even those that are introduced benignly and for limited purposes, may extend beyond those borders.[276] This has a deleterious impact upon academic freedom as it will raise the specter of ever increasing surveillance which leads to self-censorship, and ultimately restricts the free and open exchange of information.[277]

For example, ICARUS may currently be installed only on the dormitory network, but there is nothing to stop its implementation on the rest of campus, including the libraries and classrooms. Similarly, CopySense—or any technology like it—may currently monitor only the content of P2P traffic and attempt to block only infringing media, but it is easily configurable to monitor and block any type of network traffic, including e-mail, FTP, and even web traffic.[278] In fact, the Logging, Monitoring, and Privacy Project

---

[275] REZMIERSKI & ST. CLAIR, *supra* note 7, at 6.7.

[276] *See* Gary T. Marx, *Now the Techno-Snoopers Want to Get Into Our Genes*, L.A. TIMES, Sep. 15, 1989, at II7. Marx provides numerous historical examples of the surveillance creep effect, noting that "video cameras, once restricted to prisons and high-security areas, are found in offices and shopping malls; the polygraph, once limited to national-security violations, is now routinely applied to government employees and contractors; drug testing, once restricted to those working in nuclear-power facilities, is now required of bank tellers and even junior high students."

[277] *See* discussion, *supra* Parts II-III. Rezmierski & St. Clair also caution that the university campus is particularly susceptible to surveillance creep as there is a greater desire to "extend technologies to their outer limits." This is inevitable, as colleges and universities are inherently teaching, learning, and experimental environments where such exploration is valued and supported. REZMIERSKI & ST. CLAIR, *supra* note 7, at 6.7.

[278] Palmer, *supra* note 116. While touted as a "filtering" tool, a core feature of CopySense is its ability to block completely all P2P traffic. *Id.*

(LAMP), a comprehensive study of university logging and monitoring practices, was critical of even passive network monitoring technology noting that "what may begin as logging activity to protect efficient and effective surveillance of one system can become targeted data collection and surveillance of a specific individual."[279]

Moreover, the university information technology (IT) staff charged with administering the network may have unquestioned authority in the implementation and use of these technologies. Yet, these staff members may have no understanding of their potential to significantly erode academic freedom.[280] As a result, they may increase the surveillance capabilities of these technologies without any consultation or collaboration, and without an understanding of the unintended legal consequences, including potential violations of academic freedom and invasion of privacy. Perhaps the greatest danger of surveillance creep upon academic freedom is that once these technological impediments are established "what was once seen as a shocking intrusion comes to be seen as business as usual."[281] Like water on rock, surveillance creep has the potential to gradually wear away long held notions of academic freedom and privacy.

The second significant problem that arises from network impediments is a technological arms race. In its normal state, P2P traffic travels over easily identifiable ports, however when technological impediments are put in place to block or throttle it, the authors of the programs modify them to defeat such efforts.[282] As a result, P2P technology is manifesting itself in harder to

---

[279] REZMIERSKI & ST. CLAIR, *supra* note 7, at 2.1. *See* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 203 (noting that "[o]nce installed on an institution's network, [logging and monitoring technologies] could be used for copyright control today, and the control of ideas tomorrow").

[280] *See* discussion, *infra* Part IV.C. To be fair, some of the most ardent supporters of academic freedom work in information technology. *See*, *e.g.*, Joanne Straggas, *All Eyes on Napster: The Digital Copyright Controversy*, I/S (Nov. 2000), at 2, *available at* http://web.mit.edu/ist/isnews/v16/n02/160201.html (discussing MIT's information technology staff's longstanding commitment to uncensored internet access).

[281] Marx, *supra* note 276, at II7.

[282] Verma, *supra* note 20, at 68.

manage forms, making it difficult to track and control.[283] For example, critics already have serious doubts about the efficacy of CopySense, calling its blocking technology "trivial to defeat."[284] In fact, if history is any lesson, there will always be a way to defeat these technological solutions.[285]

The impact of this reality is twofold. First, universities must carefully consider the risks of investing in expensive software applications that may quickly become obsolete.[286] Even when these applications can be modified, modification will be a costly countermeasure to file-sharing.[287] Second, and more importantly, universities must decide if someone else's copyright battle is worth driving P2P technology underground.[288] Since academic freedom thrives upon the free flow of ideas and the open exchange of information, adherents to these principles cannot at the same time marginalize the means by which that freedom travels.[289] Considering the myriad of uses of P2P technology in academia, P2P traffic must remain identifiable to be managed appropriately and used without fear or suspicion.[290]

Lastly, the type of network monitoring required to utilize blocking technology like ICARUS and CopySense may lead to

---

[283] Schiller Statement II, *supra* note 227.

[284] Palmer, *supra* note 116.

[285] Graham Spanier, *quoted in* THE CHRONICLE OF HIGHER EDUC., NEW APPROACHES TO FILE SHARING (May 2003), *available at* http://chronicle.com/colloquylive/2003/05/sharing/ (noting that it is "debatable whether there is a technology out there that could prevent a determined person from gaining access to what he or she wants").

[286] Palmer, *supra* note 116.

[287] Fred von Lohmann, *quoted in* Stefanie Olsen, *Hollywood's New Lesson for Campus File Swappers*, CNET News.com (Apr. 19, 2004), http://news.com.com/Hollywoods+new+lesson+for+campus+file+swappers/2100-1027_3-5194341.html.

[288] Matthew Fordhal, *Internet Evolves in Wake of Music-Swapping Suits*, USA TODAY, Oct. 5, 2003, *available at* http://www.usatoday.com/tech/webguide/internetlife/2003-10-05-internet-underground_ x.htm (noting that "P2P file-sharing programs are shifting away from the open Internet by using encryption and anonymity tools to evade "copyright cops").

[289] *See* discussion, *supra* Part II.

[290] *See* discussion, *supra* Parts II-III.

actual or constructive "knowledge" of copyright violations, and as a result a university will incur additional obligations under the DMCA.[291] If a university with "knowledge" fails to remove infringing content and deal with infringing users, it may lose the immunity granted to it under the "safe harbor" provisions of the DMCA.[292] In other words, a university is likely to be much better off by not operating networks with applications that monitor or log traffic.

IV. RECOMMENDATIONS

Universities and colleges have many choices as to how to deal with the infringing use of P2P technology. While the use of technological impediments is one option, educational initiatives and consistent enforcement of network acceptable use policy will suffice. Universities that already follow this approach can provide guidance to other universities wishing to pursue this least restrictive model. Moreover, all university stakeholders must be involved with the implementation of campus network use policy, including the use of any technological impediments, in order to protect fully the academic freedom and privacy rights of the campus body.

A. Education and Enforcement are Key

"Education, education, education."[293] Universities across the country are aggressively addressing the P2P piracy problem without banning access to P2P applications or employing invasive technology.[294] They have achieved this through a combination of educational initiatives and enforcement of network use policy.[295] The legal motivation for this is quite clear, as long as universities

---

[291] *See* discussion, *supra* Part I.E.

[292] Hawke, *supra* note 94, at 690. S*ee also* discussion, *supra* Part I.E.

[293] Andrea Foster, THE CHRONICLE OF HIGHER EDUCATION: COLLOQUY LIVE, NEW APPROACHES TO FILE SHARING (May 22, 2003)*, available at* http://chronicle.com/colloquylive/2003/05/sharing/ (quoting Graham Spanier).

[294] *Id*.

[295] *Id.*

comply with the "safe harbor" provisions of the DMCA, they will not be liable for copyright violations.[296] Compliance means providing clear and obvious acceptable network use policy and notification to infringing users. There is no language nor policy that suggests that universities need to employ technological restrictions to comply with applicable copyright law. In fact, just the opposite is true.[297] Moreover, by emphasizing educational initiatives rather than engaging in any of this technological warfare universities avoid many of the risks and unintended consequences associated with their use.[298]

B. M.I.T.—A Model Use Policy

Citing core values of academic freedom such as a commitment to openness and the free and open exchange of information of all types,[299] many universities have resisted the demands to restrict the use of P2P file sharing applications.[300] MIT is a strong proponent of this policy, and the school offers a model network use policy that other colleges and universities should follow.[301]

Professor James D. Bruce, Vice President for Information Systems at MIT makes MIT's commitment to academic freedom on the internet very clear, stating:

> MIT has had a long history of providing its faculty, staff, and students with uncensored access to the Internet and its vast array of resources. . . . [W]e do not monitor or bar access to use the Internet. This policy is consistent with MIT's educational mission and our deeply held values of

---

[296] *See* discussion, *supra* Part I.E.

[297] *Id.*

[298] *See* discussion, *supra* Part III.

[299] *See Peer-To-Peer File-Sharing on University Campuses: Testimony of Molly Corbett Broad*, *President of the University of North Carolina*, *House Subcomm. on Courts, The Internet, and Intellectual Property*, 108th Cong. (2003) (statement of Molly Corbett Broad); Hess Statement, *supra* note 68; Spanier Statement, *supra* note 5.

[300] Chmielewski, *supra* note 205.

[301] MIT STOPIT: COPYRIGHT NOTICE PROTOCOLS (2003), *available at* http://web.mit.edu/stopit/infringe-proc.html.

academic freedom.[302]

MIT and other universities are not simply throwing caution to the wind, exercising very poor legal judgment. To the contrary, in its "Rules of Use" network policy manual, MIT's copyright policy is expressly stated: downloading unlicensed copyrighted material is prohibited[303] and violators are disciplined accordingly.[304]

MIT, and most universities following this model, employ a three step disciplinary process. When a copyright owner identifies a member of the university community for the first time as having shared copyrighted material without authorization, the member receives a warning.[305] On the second offense, they receive an immediate, but temporary, suspension of their network access.[306] On the third offense, they receive an immediate, and indefinite, suspension of network access.[307] Many universities report that by following this procedure, they have been able to virtually eliminate the incidence of repeat offenses.[308]

By adopting use policies that clearly inform all network users of a termination policy for repeat infringers, universities satisfy all the "safe harbor" provisions of the DMCA.[309] As a result, universities like MIT have managed to preserve their longstanding commitment to academic freedom while insulating themselves from charges of vicarious and contributory liability. Moreover, by not employing technological impediments, universities following this type of least restrictive use policy greatly diminish their exposure to breach of contract suits from professors and other researchers who rely on unfettered internet access to conduct

---

[302] Straggas, *supra* note 280.

[303] Athena Rules of Use, *Rule 4*, *available at* http://web.mit.edu/olh/Rules/#rule_4.

[304] MIT INFORMATION SERVICES AND TECHNOLOGY, MIT STOPIT: COPYRIGHT NOTICE PROTOCOLS (2003), *available at* http://web.mit.edu/stopit/infringe-proc.html.

[305] *Id*.

[306] *Id*.

[307] *Id*.

[308] Hess Statement, *supra* note 68.

[309] *See* 17 U.S.C. § 512 (2000).

research and experiments.[310]

C. Collaborative Consultation

So why do not all universities follow the MIT model? One problem is that despite its rapidly growing popularity, P2P technology is relatively nascent and many academics are not aware of its beneficial use.[311] As more academics become comfortable with P2P, and seek to use it in the classroom and in research, restrictive network use policies will come under greater scrutiny.[312]

This lack of knowledge and experience with P2P, however, implicates a larger and more central problem. University network administrators are instituting technological safeguards suited to their convenience without sufficient collaborative consultation with all of the other university stakeholders, which include professors, administrators and students.[313] For example, only a fragment of university presidents have any knowledge about the implications of technological impediments to academic freedom as "presidents tend not to get involved in information-technology problems but rather leave them for others to solve."[314]

Similarly, the LAMP project notes that with the "lack of policies and training regarding regulations, law, fair information practice, and data protection, college and university personnel are pursuing abusers of their systems . . . on their own."[315] In other words, many university stakeholders are not even aware to what extent network use policies can erode academic freedom. The LAMP project found that system administrators had no bright line

---

[310] *See* discussion, *supra* Parts I.B & II.B.

[311] *See generally* J.J. Fino, *Campus Software Regulations Can Threaten Academic Freedom*, FOOTNOTES (Fall 2001), *available at* http://www.aaup.org/publications/Footnotes/FN01/fn01jf.htm.

[312] *Id*.

[313] REZMIERSKI & ST. CLAIR, *supra* note 7, at 6.6; Fino, *supra* at 311.

[314] Sheldon E. Steinbach, *quoted in* Vincent Kiernan, *Higher-Education Organizations Urge a Crackdown on Illegal File Sharing*, CHRONICLE OF HIGHER EDUCATION (Oct. 10, 2002), *available at* http://chronicle.com/free/2002/10/2002101002t.htm.

[315] REZMIERSKI & ST. CLAIR, *supra* note 7, at 6.6.

rules regarding content monitoring and "in some instances the line may not even exist as system administrators have received no help in drawing it."[316] Once universities better educate themselves to the implications of poorly crafted network use policies, it is likely that they will change them immediately.[317]

Since a network is a shared resource, all of the major stakeholders in the university community need to be involved in crafting a school's network use policy.[318] It is unacceptable to allow IT staff to guide this implementation policy alone.[319] When IT staff unilaterally determines what type of applications may run on the campus network, "they control course curriculum and classroom pedagogy."[320] This is a clear violation of academic freedom because it is as if an "administrator determined textbook style or content" or "edited or restricted faculty notes or handouts."[321] While they are proficient in their field, network administrators are not charged with upholding the culture of the institution and the decisions that they make do not necessarily reflect the values of the institution as a whole. [322]

---

[316] *Id*.

[317] For example, the University of Wyoming discontinued its use of CopySense. *See* Newitz, *supra* note 269.

[318] *See* Virginia E. Rezmierski & Aline Soules, *Security vs. Anonymity: The Debate Over User Authentication and Information Access*, 28 EDUCAUSE REV., Mar.-Apr. 2000, at 22, *available at* http://www.educause.edu/ir/library/pdf/erm0022.pdf. The authors note that: "For a policy to be effective in guiding community behaviors, it must reflect the full range of the community's values, must be understood and embraced by community members, and must reinforce the most important values of the institution as a whole. An effective policy requires campus-wide discussion and the involvement of each of the major constitutencies of the community." *Id.*

[319] Fino, *supra* note 311, at 271 ("Software for faculty evaluation, classroom instruction, or research should never unilaterally be subject to selection or control by administrators.").

[320] *Id.*

[321] *Id.*

[322] *See* Rezmierski & Soules, *supra* note 318.

CONCLUSION

Universities must comply with all applicable copyright law and protect themselves from costly litigation.[323] However, universities should not serve as the copyright police.[324] Defending the copyright concerns of content providers through technological impediments, especially when universities are under no legal obligation to do so, is not enough of a compelling interest for universities to betray and undermine their own educational mission.[325] As such, university stakeholders must act with great reluctance and careful consideration before instituting technological measures that may, however inadvertently, erode the means by which academic freedom flows in the interest of countervailing parochial concerns. Network use policies do not require technical safeguards to comply with the law and banning P2P technology is antithetical to the university mission.[326] A strongly worded policy that clearly informs all network users of its termination policy for repeat infringers and an effective means of enforcing this policy will suffice.[327] In the event that a university must monitor its network due to bandwidth limitations, it should monitor for traffic flow only and should not monitor content.[328] Universities currently employing overly restrictive technological impediments must re-evaluate their network use policies because fighting copyright infringement should not compromise academic freedom and privacy rights.

---

[323] *See* discussion, *supra* Part I.D-E.

[324] Wayne D. Powell, *P2P and MP3's: Staying Out of the Middle*, EDUCAUSE, Jul./Aug. 2003, at 65.

[325] *See* Hilden, *supra* note 252. *See* discussion, *supra* Parts II-III.

[326] *See* discussion, *supra* Parts II-III.

[327] *See* discussion, *supra* Part IV.A.

[328] *See* discussion, *supra* Parts III, IV.B.