Giles Turner Non-Profit Technology Transfer – Fall 2008

Caught in the Middle: Universities as Intermediaries between Copyright Owners and On-Campus Copyright Infringers.

I. Copyright Law and Peer Infringement on University Networks

Technological advances in computer and communications technology have drastically increased access to information for students and researchers in educational institutions. Colleges, universities, and other institutions of higher education have certainly benefited from this development. However, with the technological benefits come collateral problems for educational institution administrators and legal staff. The particular problem addressed in this paper is copyright infringement by student and faculty users of campus networks. This paper focuses on two objectives. The first objective is to provide a recent history of some of the legal issues related to campus copyright infringement. The second objective is to provide a non-comprehensive examination of practices available to institutions of higher education in addressing copyright infringement.

The U.S. copyright statute provides protection for "original works of authorship" that are "fixed in a tangible medium of expression."[1] The works of authorship relevant to this paper are "sound recordings" and "motion pictures."[2] Sound recordings are "works that result from the fixation of a series of musical, spoken, or other sounds," while motion pictures are "audiovisual works consisting of a series of related images which, when

[1] 17 U.S.C. §102(a) (2006)
[2] *Id.*

shown in succession, impart an impression of motion, together with accompanying sounds, if any."[3]

Motion picture and sound recordings are of particular relevance because of their popularity among students and the ease of transmitting these works to and from campus networks.[4] Copyright owners may authorize transmission of these copyrighted works though online vendors, but the works are often transferred and copied without authorization.[5]

Owners of copyright have six exclusive rights vested in their works. The two exclusive rights most relevant to digital transmissions on campus networks are the rights to "reproduce" and "distribute" the copyrighted works.[6] The technologies addressed in the case law discussed below require storage of a copy of the copyrighted work in a storage medium such as a hard drive or similar apparatus and transmission of a separate copy of the work to another computer through a network and typically the internet.[7] When unauthorized, these acts give rise to legal claims for violation of copyright owners' exclusive right to distribute the copyrighted works by transmission over networks or the internet, and violation of the exclusive right to reproduce the copyrighted works by creation of an unauthorized copy in the process of the transfer.[8]

---

[3] 17 U.S.C. §101

[4] RIAA.com, News Room, Feb. 28, 2007, *RIAA Launches New Initiatives Targeting Campus Music Theft,* http://www.riaa.com/newsitem.php?news_month_filter=2&news_year_filter=2007&resultpage=&id=0BB7A35D-544B-2DD2-F374-4F680D6BAE9B, (last visited November 11, 2008)

[5] An example of a popular legal download site is Apple, Inc.'s iTunes.

[6] 17 U.S.C. §106

[7] Under 17 U.S.C. §101 there is a noted distinction between "phonorecords," the legally defined material objects in which sound recordings are fixed, and "copies," the material objects in which other types of works such as motion pictures are fixed. For the sake of maintaining simplicity, this paper uses the terms copy or file to describe the medium in which both sound recordings and motion pictures are fixed on computers and transmitted through networks.

[8] *E.g., London Sire Records, Inc. et. al. v. Doe 1 et. al.*, 542 F.Supp.2d 153, 159 (D. Ma. 2008)

A. Copyright Infringement via Peer-to-Peer Networks

The most notorious cases addressing the type of copyright infringement described above involved Peer-to-Peer (P2P) networks. The courts found the P2P network operators liable for secondary copyright infringement. There are several types of secondary copyright infringement including vicarious, contributory, as well as inducement to infringe copyright. Under federal copyright common law, vicarious copyright infringement requires a party have the right and ability to supervise the infringing activity, as well as the ability to direct the financial interests of the infringing activity.[9] The courts define contributory copyright infringement as providing others with a means for infringing copyrights and knowing infringement is occurring.[10]

Napster stands as the most notorious P2P network. In 1999, a college freshman in computer science at Northeastern University dropped out of school to set up Napster.[11] Napster provided access to centralized online servers that indexed copyrighted works stored on individual users' personal computers. A user of Napster could log on to the network, search the centralized index, find another user storing a desirable sound recording, connect directly to the other user's computer, and download an unauthorized copy of the sound recording for free. The U.S. recording industry took immediate action. The Ninth Circuit affirmed Napster had the "ability to locate infringing material listed on its search indices and the right to terminate users' access to the system."[12] The court

[9] *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 261-64 (9th Cir. 1996).
[10] *Fonovisa,* 76 F.3d at 264.
[11] Spencer E. Ante, *Inside Napster,* BusinessWeek, Aug. 14, 2000, *available at* http://www.businessweek.com/2000/00_33/b3694003.htm.
[12] *A & M Records, Inc. v. Napster, Inc,* 284 F.3d 1091, 1097-98 (9th Cir. 2002) (quoting *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023-24 (9th Cir. 2001)).

stated Napster could only avoid vicarious infringement by policing its system and preventing access to all unauthorized sound recordings.[13]

Following the *Napster* decision, designers of P2P networks became more creative in attempts circumvent secondary copyright infringement. One innovative P2P network software package, distributed for free by a company known as Grokster, disposed of the use of central networks by organizing users' computers to serve as indexes for the file transfer network.[14] Again, the movie and music industry took legal action and filed suit. The case against Grokster rose to U.S. Supreme Court. The Court held Grokster liable for inducing copyright infringement by "distributing a device with the object of promoting its use to infringe copyright, as shown by clear expression or other steps to foster infringement."[15]

In the midst of the suits against P2P networks, trade organizations such as the Recording Industry Association of America (RIAA) began filing copyright infringement complaints against individuals using the P2P networks.[16] The RIAA represents a group of record companies in business and legal matters. The activities of the RIAA include investigating copyright infringement, filing legal actions, and lobbying for stronger intellectual property rights.[17]

Lawsuits against individual infringers on P2P networks pose a particular hurdle for plaintiffs. The only identifying information publicly accessible when examining P2P

---

[13] *Id.*
[14] *Metro-Goldwyn-Mayer Studios v. Grokster Ltd*., 545 U.S. 913, 919-20 (2005).
[15] *Grokster*, 545 U.S. at 936-37.
[16] RIAA.com, News Room, December 16, 2004, *RIAA Files New Copyright Infringement Lawsuits Against 754 Illegal File Sharers, available at* http://www.riaa.com/newsitem.php?news_month_filter=&news_year_filter=2004&resultpage=&id=536FB56E-E24D-C9F6-9F47-4BF90B54DF01, (last visited November 1, 2008) (actual suits against direct infringers started in 2003)
[17] RIAA – Who We Are, available at http://www.riaa.com/aboutus.php (last visited Nov. 15, 2008).

network activity is a P2P user's Internet Protocol (IP) address and possibly a network username.[18] Without the legal identity of a defendant, it is difficult for a copyright owner to file and complete a successful lawsuit.

Typically, a copyright owner will use a third party investigator to uncover IP addresses of the alleged infringers using P2P networks. For example, the RIAA uses a company called MediaSentry that poses as a normal P2P user. MediaSentry logs on to P2P networks and finds sound recording files stored on P2P users' computers, where the users offer the recordings for unauthorized download.[19] MediaSentry downloads the sound recording file, records the IP address of the P2P user offering copyrighted materials for unauthorized download, and provides the IP address to the copyright owner or the RIAA.[20]

B. The Digital Millennium Copyright Act

Originally copyright owners obtained the legal identities of alleged P2P infringers using the subpoena provision of the Digital Millennium Copyright Act (DMCA) of 1998.[21] The DMCA was enacted to address technological changes in copyright infringement. Congress drafted the DMCA subpoena provision to allow a copyright owner to obtain a subpoena from a clerk of the court without filing suit.[22] An issued DMCA subpoena normally contained an alleged P2P infringer's IP address. The plaintiff served the subpoena on the alleged infringer's Internet Service Provider (ISP),

[18] An IP address is formed in a series of numbers separated by decimals. IP addresses are assigned to subscribers by an Internet Service Provider (ISP). IP addresses represent an individual internet connection. A subscriber's ISP is identifiable by a consistent group of numbers in each IP address issued by the ISP. A separate part of the address contains a number that is unique to each subscriber and represents the individual connection to the internet.
[19] *London Sire,* 542 F.Supp.2d at 159-60; Kim F. Natividad, *Stepping it up and Taking it to the Streets,* 23 Berkeley Tech. L. J. 469, 472 (2008).
[20] *London Sire,* 542 F.Supp.2d at 159-60.
[21] 17 U.S.C. §512(h).
[22] §512(h)(1).

compelling the ISP to match the IP address to a subscriber's legal identity and disclose the identity to the copyright holder.

The DMCA provides four safe harbors for an ISP under §512 of the copyright statute.[23] The safe harbors insulate an ISP from secondary liability related to the ISP subscribers' copyright infringement. The safe harbors only provide immunity from secondary liability if an ISP meets certain qualifying conditions. For example, the first safe harbor insulates an ISP from secondary liability for the copyright infringement of its subscribers whose infringing "transitory digital network communications" pass through the ISP's network and into the internet.[24] In order for an ISP to qualify for immunity, (1) the infringing transitory communications must be initiated by a person other than the ISP, (2) the routing of the infringing communication must be automatic and not directed by the ISP, (3) the ISP cannot select the recipients of the infringing communication, (4) no copy of the copyrighted material may be maintained in the ISP's network for a period longer than necessary to transmit the communication, and (5) the infringing material must be transmitted without modification by the ISP.[25]

The other three safe harbors include immunity from secondary liability due to a subscriber's infringing "system caching," or intermediate and temporary storage of a copyrighted work on an ISP network at the direction of a subscriber; immunity from infringing "information residing on systems or networks at direction of users [subscribers];" and "information location tools" used by subscribers to locate infringing materials.[26] The last three safe harbors contain similar qualifications and limitations to

[23] §512(a)-(d).
[24] §512(a).
[25] §512(a)(1)-(5).
[26] §512(b)-(c).

those required in the first safe harbor. Despite the safe harbors, ISPs are still subject to injunctions and the special subpoena powers codified within the DMCA.[27]

As mentioned above, the DMCA subpoena provision, §512(h), does not require judicial oversight and only requires a minimal evidentiary showing to a clerk of the court. More specifically, §512(h) requires the copyright owner or its agent present a proposed subpoena, a sworn declaration of the rights to be protected, and what are called the notice and take down elements of §512(c)(3)(A). The notification under §512(c)(3)(A) requires the copyright owner provide "substantially the following" elements of notice: (1) a signature of a party authorized to act on behalf of the copyright owner; (2) identification of the copyrighted work or works allegedly infringed; (3) identification and location of the allegedly infringing material so that it may be removed or its access blocked by the ISP; (4) contact information of the complaining party; (5) a statement of good faith belief of infringement; and (6) a statement that the information provided is accurate.[28] Problems arise for copyright owners under the DMCA subpoena process because, as stated above, the only evidence copyright owners hold when applying for a DMCA subpoena is an alleged P2P infringer's IP address and the identity of the allegedly infringed copyrighted work.

The subpoenas on ISPs to obtain legal identities of P2P users using the DMCA provisions were largely unsuccessful. The problem arose due to the nature of the P2P file transfers and the statutory construction of the DMCA. ISPs challenged the validity of the subpoenas based on the language of the statute.[29] The court in *Recording Indus. Ass'n of Am., Inc. v. Verizon Wireless Servs.,* held transfers of digitized copyrighted works

[27] §512(h) and (j).
[28] §512(c)(3)(A)(i)-(vi).
[29] *Recording Indus. Ass'n of Am., Inc. v. Verizon Wireless Servs.,* 351 F.3d 1229, 1234-35 (DC Cir. 2003)

between P2P users only qualified as "transitory digital communications" under §512(a), to which the notice and takedown provisions of §512(c)(3)(A) did not apply.[30] The court reasoned that ISPs had no way of removing or disabling access to content that was merely transmitted through the ISPs' networks, and the subpoena provisions of §512(h) only applied to the storage functions of the ISP, §512(b)-(d), pertaining to caching, storage on network servers, and information location tools.[31] After the *Verizon Wireless* case, the courts began to uniformly deny the §512(h) subpoenas in P2P infringement actions.[32]

C. Current Trend in P2P Litigation

The sound recording industry, represented by the RIAA, changed its strategy and started filing complaints under the Federal Rules of Civil Procedure. These complaints are filed against John Doe defendants because only an IP address and possibly a P2P username are known by the plaintiff. After filing a compliant, it is customary practice for a plaintiff to immediately file an *ex parte* application to take leave for immediate discovery under Fed. R. Civ. P. 26(d)(1), which states:

> "A party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except… when authorized by these rules, by stipulation, or by court order."

Immediate or expedited discovery is regularly supported on the argument that one party is unidentified at the time of filing the complaint and there is no other way to conduct a pre-trial discovery conference as required by Fed. R. Civ. P. 26(f). In the

[30] *Verizon Wireless,* 351 F.3d at 1234-35.
[31] *Id.* at 1235-37.
[32] *See, e.g., In re Charter Communications, Inc, Subpoena Enforcement Matter,* 393 F.3d 771, 780-81 (8th Cir. 2005) (holding the subpoena provisions of the DMCA to not apply to an ISP serving as a conduit); *In re Subpoena to Univ. of N. Carolina at Chapel Hill*, 367 F.Supp.2d 945, 956 (MD NC 2005) (stating a "construction of the DMCA to allow subpoenas on Section 512(a) service providers would amount to a re-writing of the DMCA.").

context of the P2P infringement cases, an *ex parte* application for expedited discovery is filed in order to subpoena the alleged infringer's ISP.[33] Once subpoenaed, an ISP must match an alleged infringer's IP address with the relevant identifying information such as the alleged infringer's name and address, and disclose the information to the court.

This process poses a number of difficulties for ISPs because IP addresses are not always static and often the ISP assigns a new IP address to a particular computer each time it connects to the internet.[34] The process is further frustrated by the fact that more than one computer may be connected to a single IP address through a wireless router. In customary practice, an ISP maintains a log of IP addresses assigned to particular subscribers. The identity of a subscriber may be determined from an IP log, but ISPs only retain a log for a certain period of time, after which they are deleted.[35]

In the event an ISP fails to respond to a subpoena, the ISP will likely be subject to a motion to compel disclosure of the identities of the alleged infringers under Fed. R. Civ. P. 37(a). If the ISP fails to respond to an order compelling disclosure, the court may order sanctions against the ISP or hold it in contempt.[36] It is important to note the Rules allow ISPs some leeway with respect to electronically discoverable information. Fed. R. Civ. P. 37(e) provides that "[a]bsent exceptional circumstances, a court may not impose sanctions… for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system." However, when an ISP expects electronic information such as IP address logs will be needed for litigation,

[33] Fed. R. Civ. P. 45.
[34] *E.g.*, *London Sire,* 542 F.Supp.2d at 160.
[35] *Id.*
[36] Fed. R. Civ. P. 37(b).

subsequent destruction of the logs, even if carried out in the regular course of business, will likely negate the "good faith" exemption provided under 37(e).[37]

The picture becomes more complicated when universities, colleges, or other non-profit learning institutions (hereinafter universities) serve as an ISP to campus subscribers. Often, additional legal duties are imposed on universities as compared to commercial ISPs. The legal obligations imposed on university ISPs are related to privacy of the student, liability as an employer, as well as the liabilities imposed on all ISPs.

D. Universities Caught in the Middle

In 2007 the RIAA began a wide spread program of sending what it called pre-litigation settlement letters to colleges.[38] Each letter contains an IP address of an alleged infringer. The RIAA requests the university match the IP address to one of the university's subscribers. The letter also requests the university forward the letter to the alleged infringer once it identifies him, though the universities are under no legal obligation to do so.[39] The letter usually states a record label owning copyrighted sound recordings is about to file an infringement suit against an unnamed university subscriber the label alleges infringed the copyrighted recordings. The letter offers twenty-day period in which the alleged infringer may settle the claims for a sum well below what is

[37] *Doe v. Norwalk. Cmty. Coll.,* 248 F.R.D. 372, 378 (D. Conn. 2007).
[38] RIAA.com, News Room, February 28, 2007, *RIAA Launches New Initiatives Targeting Campus Music Theft, available at* http://www.riaa.com/newsitem.php?news_month_filter=2&news_year_filter=2007&resultpage=&id=0BB7A35D-544B-2DD2-F374-4F680D6BAE9B, (last visited November 11, 2008)
[39] RIAA.com, News Room, February 28, 2007, *RIAA Launches New Initiatives Targeting Campus Music Theft;* Natividad, *supra* at note 17, at 475; Electronic Frontier Foundation, *RIAA v. The People: Five Years Later,* September 2008, p.7-8, *available at* http://www.eff.org/files/eff-riaa-whitepaper.pdf, (last visited October 20, 2008).

available to the plaintiff under the copyright statute.[40] The statutory minimum damages available for each infringement of a copyrighted work are $750.[41]

It does not take long to imagine the astronomical damages that could be calculated from a single college student's computer. As the RIAA expected, many recipients of the letters chose to settle for lesser sums. The RIAA operates a website where recipients of the pre-litigation letters may pay a settlement using a credit card, without a formal complaint filed by the plaintiff.[42]

If there is no response from the university or the alleged infringers, the copyright owner files a complaint. Courts usually join many John Doe defendants at a single university into a single legal action. Once the suit is filed, the plaintiff files an *ex parte* motion for leave to take immediate discovery under Rule 26(d)(1).

The *ex parte* motions to take leave for expedited discovery regularly hinge upon whether the plaintiff has shown "good cause."[43] For example, in *Arista Records, LLC v. Does 1-7,* Arista Records filed a complaint against John Doe defendants who allegedly used the University of Georgia's campus network to infringe copyrighted sound recordings.[44] The court held the plaintiff had shown "good cause" in its *ex parte* application and issued a subpoena on the University of Georgia. The court found "good cause" because the plaintiff had no other means to obtain the basic identifying information of the alleged infringers, the plaintiff supplied sufficient evidence of *prima*

---

[40] Electronic Frontier Foundation, *RIAA v. The People: Five Years Later,* September 2008, p.7-8.
[41] 17 U.S.C. §504(c)(1); *see also, London Sire,* 542 F.Supp.2d at 161(stating the "approximate settlement range appears to be $3000 to $6000 per defendant").
[42] P2PLawsuits.com, https://www.p2plawsuits.com/P2P_00_Home.aspx, (last visited, October 23, 2008).
[43] See, e.g., *Virgin Records America, Inc. v. Does 1-33,* No. 3:07-CV-235, 2007 WL 3145838, at *1-2 (E.D. Tenn. 2007); *Arista Records, LLC v. Does 1-7*, No. 3:08-CV-18(CDL), 2008 WL 542709, at *1 (M.D. Ga. 2008); *Arista Records LLC v. Does 1-19,* 551 F.Supp2d 1, 6 (D.D.C. 2008); *London Sire,* 542 F.Supp.2d at 163.
[44] *Arista v. Does 1-7*, 2008 WL 542709, at *1.

facie copyright infringement, and time was of the essence because the ISPs only temporarily retain IP address logs.[45] Many orders granting *ex parte* applications for expedited discovery turn on similar facts and result in a court issuing a subpoena on a university.[46] At least one court has refused to grant expedited discovery in P2P infringement case, but this is an exception to what appears to be an accepted procedure.[47]

After receiving an issued subpoena, universities faced the options of complying with the subpoena, notifying the alleged infringers, and filing a motion to quash the subpoena under the Federal Rules of Civil Procedure. Typically, universities are subject to an additional order to notify the alleged infringers that their identifying information is subject to subpoena.[48] Once the alleged infringers have notice of the suit, they may file motions to quash the subpoena as anonymous John Doe defendants.

E. Procedural Challenges to Discovery of John Doe Identities

Motions to quash subpoenas fall under the Fed. R. Civ. P. 45(c)(3)(A), which forces a court to a quash subpoena that requires disclosure of "privileged or other

---

[45] Many courts interpret *prima facie* copyright infringement to be the elements articulated in *Feist Publications, Inc. v. Rural Telephone Service.* 499 U.S. 340, 361 (1991) (stating "To establish infringement, two elements must be proven: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original.").

[46] *See, Capitol Records, Inc. v. John Doe,* No. 07-cv-1570-JM(POR), 2007 WL 2429830, *1 (S.D.Cal. 2007) (finding good cause in allegations of copyright infringement, danger that Univ. of California-San Diego will not preserve the relevant IP information, narrow tailoring of the discovery request, lack of prejudice on the defendant, need to move the case forward); *Warner Bros. Records Inc. v. Does 1-20,* No. 07-cv-01131-LTB-MJW, 2007 WL 1655365, at *1 (D. Colo. 2007) (finding good cause in immediate need for the identifying information before it is erased by the ISP); *Arista Records LLC v. Does 1-9,* No. 07-cv-00628-EWN-MEH, 2007 WL 1059049, at *1 (D. Colo. 2007) (finding good cause in the need to discover the identity of the defendants and move the suit forward).

[47] *Capitol Records v. Does 1-16,* No. 07-485 WJ/LFG, 2007 WL 1893603, *1-2 (D. N.M. 2007) (stating *ex parte* proceedings should be the exception and not the rule, the information sought is highly confidential and sensitive, there is no irreparable harm, there is no way to know whether the defendants will have the opportunity to oppose the subpoena, and the plaintiff's must meet with the University so that it may be heard and so that a process may be established for notice and discovery).

[48] *E.g., Arista Records LLC v. Does 1-19,* 551 F.Supp2d 1, 5 (D.D.C. 2008) (reviewing an order issued to George Washington University to notify defendants within five days of receiving the subpoena, order to preserve subpoenaed information pending a timely motion to quash the subpoena).

protected matter," or that "subjects a person to undue burden."[49] In order to defeat a subpoena issued in expedited discovery, the defendant or subpoenaed party must file a motion to vacate the order granting expedited discovery by demonstrating "good cause" did not exist in the *ex parte* motion for expedited discovery, and file a motion to quash the subpoena by showing the subpoenaed information is protected, privileged, or subjects a person to undue burden.[50]

Arista Records LLC v. Does 1-19 is a typical example of a John Doe defendant's procedural challenges to a plaintiff's expedited discovery and subpoena. The plaintiff in *Arista v. Does 1-19* was granted an *ex parte* motion for leave to take immediate discovery of identities of a list of John Doe defendants at George Washington University (GW). The defendants allegedly used GW's campus network infringe copyrights via P2P file transfers.[51] The court issued a subpoena on GW demanding it to recover and present "information sufficient to identify each defendant, including name, current (and permanent) addresses, telephone numbers, email addresses, and Media Access Control (MAC) addresses."[52]

Doe # 3 filed motions to vacate the order granting expedited discovery, to quash the subpoena on GW, and to dismiss the complaints.[53] GW filed a motion for extension of the deadline for response to the subpoena, which the court temporarily held pending

[49] Fed R. of Civ. P. 45(c)(3)(A)(iii) and (iv).
[50] *See, Warner Bros. Records Inc. et. al. v. Does 1-6,* 527 F.Supp.2d 1, 3 (D. D.C. 2007) (stating that expedited discovery requires a showing of good cause for the discovery sought).
[51] 551 F.Supp2d at 3.
[52] *Id.* at 4; *See also, Fonovisa, Inc. v. Does 1-19,* No. 07-1515, 2008 WL 919701, at *8 n.14 (W.D. Pa. 2008) (defining a Media Access Control address as comprising "six two-digit hexadecimal numbers separated by colons, that uniquely identifies each piece of computer hardware connected to the university's network.")
[53] *Arista v. Does 1-19,* 551 F.Supp2d at 3-4.

resolution of the defendant's motions.[54] The defendant argued the subpoena was impermissible under (1) 17 U.S.C. §512(h) of the DMCA, (2) 47 U.S.C. §551(c)(2)(B) of the Cable Communications Act, (3) 20 U.S.C. §1232g(b)(2) of the Family Educational Rights and Privacy Act (FERPA), and (4) the Federal Rules of Civil Procedure.[55] The legal arguments raised in *Arista v. Does 1-19* are typical of those made by many Doe defendants in P2P infringement cases.

In *Arista v. Does 1-19,* the plaintiff conceded the DMCA subpoena provision §512(h) did not support the motion for subpoena. This concession was likely made because §512(h) was inapplicable to "transitory digital communications" after *Verizon Wireless*.[56]

The court in *Arista v. Does 1-19* held §551(c)(2)(B) of the Cable Communications Act only applied to government entities seeking subpoenas on cable providers, and the statute was inapplicable to a private party seeking a subpoena.[57] Other cases have interpreted the Cable Communications Act in the same manner by reasoning even if universities were cable operators within the meaning of the statute the government is the only party that may seek such a subpoena on a cable service provider.[58]

The court in *Arista v. Does 1-19* quickly rejected FERPA, 20 U.S.C. §1232g(b)(2), as grounds to quash the subpoena.[59] Other courts have ruled in the same manner. For example, in *Virgin Records America, Inc. v. Does 1-33,* a University of

---

[54] *Id.*
[55] *Id.* at 5- 9.
[56] *Id.* at 5; *Verizon Wireless,* 351 F.3d at 1235-37.
[57] *Arista v. Does 1-19,* 551 F.Supp2d at 5.
[58] *See, e.g., Interscope Records v. Does 1-7,* 494 F.Supp2d 388, 390-91 (E.D. Va. 2007) (granting motion to quash subpoena on the College of William and Mary, because 47 U.S.C. §551(c)(2)(B) is inapplicable to private parties seeking to subpoena information from cable service providers); *Sony BMG Music Entm't v. Does 1-12,* No. 07-232 (S.D. W.Va . 2007).
[59] 551 F.Supp2d at 5-6.

Tennessee student, Doe #28, argued the information sought in the subpoena violated his privacy rights under §1232g of FERPA, which he had not waived.[60]

FERPA protects only "educational records" and "personally identifiable information" other than "directory information" from disclosure without prior written consent of the parents.[61] Section 1232g(d) states a student's privacy rights initially vest in his parents but transfer to the student once he reaches the age of eighteen. Section 1232g(a)(4)(A) of FERPA defines "educational records" as "records, files, documents, and other materials which (i) contain information directly related to the student; and (ii) are maintained by an educational agency or institution."

Section 1232g(a)(5)(A) of FERPA defines "directory information" as "the student's name, address, telephone listing, date and place of birth, major field of study, … dates of attendance, … and the most recent previous educational agency or institution attended by the student." Additionally, FERPA requires educational institutions providing public access to "directory information" give public notice of the nature of the "directory information" and give parents or students a reasonable period in which to demand that the student's "directory information" not be disclosed without prior waiver.[62]

The court in *Virgin v. Does 1-33* read FERPA to expressly authorize educational institution's disclosure of a student's "directory information," without prior written consent.[63] The court examined the University of Tennessee's FERPA policy and found that all of the information demanded in the subpoena was listed in the policy, with the

[60] No. 3:07-CV-235, 2007 WL 3145838, at *1 (E.D. Tenn. 2007).
[61] 20 U.S.C. §1232g(b)(1).
[62] §1232g(a)(5)(B).
[63] *Id.* at *2; 20 U.S.C. §1232g(b)(1) (2006).

exception of the MAC address.[64] The court held the MAC addresses did not meet the definitions of "educational records" or "personally identifiable information" under the statute. The court stated there were no filings by the student or his parents requesting the "directory information" be kept confidential. The court concluded all the directory information sought in the subpoena was discoverable and not protected.[65] The court also denied the defendant's motion to quash the subpoena by finding no undue burden in requiring disclosure of the defendant's name, permanent address, telephone number, and email address, because college students are transient in nature and move residences frequently.[66]

Ex parte applications for expedited discovery may be challenged under the Federal Rules of Civil Procedure. For example, the defendant in *Arista v. Does 1-19*, argued a concrete showing *prima facie* copyright infringement was required to establish "good cause" in support of expedited discovery under Fed. R. Civ. P. 26(d)(1).[67]

Some courts cite *Feist Publications, Inc. v. Rural Telephone Service,* 499 U.S. 340, 361 (1991), as defining *prima facie* copyright infringement. [68] *Feist* stated copyright infringement requires "(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original."[69]

The court in *Arista v. Does 1-19* rejected a need for a showing of *prima facie* copyright infringement and held that the plaintiff had shown good cause through his need to identify the defendant so the trial could proceed. The court also found good

[64] *Virgin Records v. Does 1-33,* 2007 WL 3145838 at *2.
[65] *Id.*
[66] *Virgin,* at *1.
[67] *Arista v. Does 1-19,* 551 F.Supp2d at 6.
[68] *E.g., UMG Recordings, Inc. v. Doe,* No. C 08-1193 SBA., 2008 WL 4104214 at *5 (N.D. Cal. 2008).
[69] 499 U.S. at 361.

cause due to the limited time available to recover the identifying information before it was deleted from GW's IP logs.[70] It is worth noting an inconsistency exists between the courts because some require a *prima facie* showing of copyright infringement to establish good cause for expedited discovery.[71]

Other courts require a prima facie showing of copyright infringement in the context of a First Amendment defense of anonymous speech in P2P file-sharing. In *London Sire Records, Inc. et. al. v. Doe 1 et. al,* a student from Boston University, John Doe #3, moved to quash a subpoena, by raising a first amendment anonymous speech defense.[72] The court stated that the party moving to quash the subpoena must show a "clearly defined and serious harm," and required an examination of whether anonymous speech was entitled privilege or protection under Fed. R. Civ. P. 45(c)(3)(A)(iii).[73]

The court in *London Sire* stated there was at least some degree of self-expression in the manner in which an individual arranges copyrighted works together on their computer by "the association of one recording with another by placing them in the same library, the self-expressive act of identification with a particular recording, [and] the affirmation of joining others listening to the same recording or expressing the same idea."[74] The court found a limited protectable right in anonymous speech on P2P networks.[75] The court added that the anonymous activity must actually be speech and "copyright infringement per se is clearly not speech entitled to first amendment

[70] *Id.* at *7; *see also,* notes 41-43 *supra.*
[71] *E.g., UMG. v. Doe,* 2008 WL 4104214 at *5; *Arista v. Does 1-7*, 2008 WL 542709, at *1.
[72] 542 F.Supp.2d at 161-64.
[73] *Id.*
[74] *Id*. at 163.
[75] *Id*. at 164.

protection."[76] It is important to note that many courts find first amendment challenges to expedited discovery and subpoenas to be insufficient.[77]

The *London Sire* court balanced the harm between the plaintiff seeking the identity of an alleged infringer and the defendant who has a protectable interest in anonymous speech on the internet.[78] To balance the harm, the court used five factors including: (1) a requirement of a concrete showing of a prima facie claim of actionable harm (copyright infringement); (2) the specificity of the discovery request; (3) absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed information to advance the claim; and (5) the expectation of privacy of the party whose identifying information is sought.[79]

The *London-Sire* court stated that the first factor requiring concrete evidence of *prima facie* copyright infringement ensured the plaintiffs would not destroy the defendant's anonymity based on factually or legally unsupported pleadings.[80] Following the *Feist* factors, the court found the plaintiff owned valid copyrights and the defendant violated one of the owner's exclusive rights.[81] The defendant raised the issue that the plaintiff authorized MediaSentry to download the copyrighted works and there was no proof of violation of the distribution right.[82] The defendant argued the act of placing or

---

[76] *Id.* at 163-64 (citing *Harper & Row Publishers, Inc. v. Nation Enters*., 471 U.S. 539, 555-57, 560 (1985)).
[77] *See e.g., Arista,* 551 F.Supp2d at 8-9 (stating first amendment protection is small when the "speech" is alleged to be infringement of copyright); *Sony Music,* 326 F.Supp2d at 567 (finding plaintiff's right to use legal process to sue for copyright infringement outweighs the defendant's right to anonymous speech); *Arista Records LLC v. Does 1-11*, Civ. A. No. 07-568 (W.D.Okla. Nov. 14, 2007) (holding information sought in the subpoena did not violate the defendant's free speech rights); *Fonovisa*, 2008 WL 919701 at *9, (holding there is a minimal expectation of anonymity in illegally transferring copyrighted works).
[78] *London Sire,* 542 F.Supp.2d 162.
[79] *Id.* at 164-179 (citing the five factors from *Sony Music Entm't v. Does 1-40*, 326 F.Supp2d 556, 564-65 (S.D. N.Y. 2004)).
[80] *London Sire,* 542 F.Supp.2d at 164.
[81] *See, Feist,* 499 U.S. at 361.
[82] *London Sire,* 542 F.Supp.2d at 164.

"making available" a digitized sound recording on a computer hard drive, so others could download the file, was not a violation of the exclusive right of distribution without proof of an actual unauthorized download.[83] The court ruled that actual distribution must occur in order for a plaintiff to have a claim of copyright infringement, and "making available" did not constitute an actual distribution.[84] However, despite the plaintiff being incapable of directly proving an unauthorized download, the court found the evidence and allegations sufficient to support an inference that at least one unauthorized distribution occurred for the purposes of a concrete showing of prima facie copyright infringement.[85]

The *London-Sire* court also examined the second balancing factor, the specificity of the discovery request. The court found a single IP address may be assigned to more than one computer, and the ISP may be unable to identify the infringing user with certainty.[86] The court reasoned an ISP presenting a long list of potential infringers to the plaintiff would allow him to go on a fishing expedition.[87] The court ruled the subpoena had to be modified to protect students' anonymity. The court held a second modified subpoena would allow the plaintiff to seek the identity of the alleged infringer "with a degree of particularity."[88]

The court examined the third factor, alternate means of obtaining the subpoenaed information, and found that the defendant had not suggested any other means for recovering the identifying information, and the court was unaware of any other

---

[83] *Id* at 164 -67; *see also*, *Atlantic Recording Corp. v. Howell,* 554 F.Supp.2d 976, 983 (D. Az. 2008) (holding "making available" is not a violation of the exclusive right of distribution); *Electra Entm't Group, Inc. v. Barker*, 551 F.Supp.2d 234, 244-45 (S.D. N.Y. 2008) (stating "making available" is not a statutory violation of the exclusive distribution right).
[84] *London Sire,* 542 F.Supp.2d at 169.
[85] *Id.* at 174-77.
[86] *Id.* at 178.
[87] *Id.*
[88] *Id.* at 178-79.

methods.[89] The court stated that the third factor cut against the motion to quash the subpoena.[90]

The court examined the fourth factor requiring the plaintiff's central need for the information in the subpoena. Much like other courts, the court found the plaintiff would not be able to protect his rights without the identities of the defendants.[91]

Finally, the *London-Sire* court examined the fifth factor, the defendant's expectation of privacy in the subpoenaed information. The Boston University ISP agreement was unavailable and the court was unable to determine the defendant's expectation of privacy when using the network.[92] The court emphasized the agreement would have been very helpful in resolving the issue.[93]

In the end, the *London Sire* court granted the motion to quash, holding that the subpoena lacked specificity and inadequately addressed the alleged infringer's expectation of privacy.[94] The court stated the next subpoena must require the ISP's response containing the private information be submitted to the court under seal for review in camera.[95] The court also required the new subpoena specify and explain any uncertainty as to the match of an IP address to a particular student or a list of students.[96] The next subpoena was to require Boston University submit a copy of the terms of its ISP agreement with its users, or a statement explaining the contractual relationship.[97]

---

[89] *Id.* at 179.
[90] *Id.* at 178.
[91] *Id.*
[92] *Id* at 179.
[93] *Id.* at 180.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*

Additionally, Boston University was not to disclose any information without order of the court.[98]

As can be seen from the *London-Sire* decision, the court took a more protective stance regard to the privacy of the Doe defendant's. The *London-Sire* order serves as a good guideline for universities for developing policies and ISP agreements that protect network subscriber privacy.

Universities rarely file motions to quash the subpoenas. *Arista v. Does 1*-17 is an example of a university filing a motion to quash based on undue burden.[99] The University of Oregon filed a motion to quash a subpoena arguing it could not identify any of the alleged infringers with specificity.[100] The University argued it knew the dorm room occupants matched to the IP addresses but was uncertain about the identities of the persons who performed the alleged copyright infringement.[101] Additionally, many of the alleged infringers were connected to the University network by wireless, complicating matters further.[102] The University argued interviews and forensic investigation were required to identify the alleged infringers with any certainty.[103] In the alternative, the University argued the plaintiff misrepresented a potential for spoliation of evidence by the university in the plaintiff's *ex parte* application for expedited discovery.[104]

The court in *Arista v. Does 1*-17 held the subpoena's lack of specificity placed an undue burden of the University and a second subpoena with narrowed scope should seek

---

[98] *Id.*
[99] *Arista Records, LLC v. Does 1-17,* No 07-6197-HO, *1-3 (D. Or. 2008).
[100] *Id.*
[101] *Id.* at 3.
[102] *Id.*
[103] *Id.*. at 3 n.1.
[104] *Id.* at 4-7.

alleged infringers information with greater specificity.[105] The motion to quash based on the plaintiff's misrepresentations was dismissed by the court, which stated that the plaintiff was primarily seeking to identify the infringers, and any misrepresentations were honest mistakes.[106]

In sum, many courts address *ex parte* applications for expedited discovery and resultant motions to quash subpoenas in favor of copyright owners. It is still important that university administrators and legal departments address the rights of their students and faculty when responding to subpoenas.

II. Practical Tips for Universities to Address Individual Copyright Infringement

University administrators and legal staff are under pressure to comply with subpoenas seeking disclosure of campus copyright infringers. This section of the paper provides a quick, high-level overview of practices university administrators may use to face issues regarding campus copyright infringement. The following overview addresses the issues raised in the court proceedings described above and provides a quick exploration of some additional issues to consider. The intent of this section is to serve as a helpful starting point for addressing campus copyright infringement and creating a balance between protection of intellectual property and protection of the privacy of network subscribers. This section is not a comprehensive examination of legal issues related to campus copyright infringement.

A. Shaping University Policies to Address the Legal Issues

Universities should align their written policies to address campus copyright infringement. Universities are required to give public notice of their definition of

[105] *Id.* at 2.
[106] *Id* at 7 (stating that the plaintiff was unable to comply with Fed. R. Civ. P. 45(b)(1) because the identity of the adverse party was unknown).

"directory information" under FERPA.[107] A university should publicly disseminate the FERPA or at least require students and parents to review the policy. A university's should carefully draft a FERPA policy to define "directory information" to include all types of potentially subpoenaed personally identifying information. The terms included in the policy definition should be analogous and within the scope of the FERPA definition of "directory information."

For example, subpoenas frequently seek disclosure of MAC addresses. MAC addresses are not included in the language of the FERPA statute but should be included in a university's FERPA policy definition of "directory information." Inclusion of similar network address identification in the definition will place parents and students on notice that FERPA does not protect network address "directory information."

Prior to allowing students access to campus networks, it may be wise practice for a university to require a student and her parents to read and understand the FERPA policy. This practice will provide notice that prior consent is not required for disclosure of "directory information."[108] FERPA permits a student or parent to place a hold on the student's directory information so that it remains confidential undisclosed without consent.[109] It is unclear what result such a hold would have in the face of a subpoena. Nonetheless, upon receipt of a subpoena seeking identifying information, universities should review all identities retrieved to ensure the information is not confidential under FERPA.

A university providing internet services should draft an internet service agreement to expressly state the subscribers' privacy rights. The internet service agreement should

[107] 20 U.S.C. §1232g(a)(5)(B).
[108] *Id.*
[109] *Id.*

spell out the university's protocol for responding to subpoenas seeking a subscriber's identifying information. Both the university and the subscriber should retain a copy of the internet service agreement. This procedure will ensure the subscriber has knowledge of the policy and will serve as notice of a subscriber's expectation of privacy, should litigation or a subpoena arise.

Some colleges, such as the University of California - Berkeley require students to attend an informational seminar on campus connectivity and copyright infringement prior to gaining access to the campus network.[110] Alternatively, a university may use literature and contractual clauses in ISP agreements to inform students they are not to infringe copyrights using the university network.

Many universities establish written disciplinary policies related to copyright infringement using the university's network. Some universities, such as Stanford University have established strict policies with regard to subpoenas and campus copyright infringement. For example, Stanford's policy resembles a "three strikes and you're out" disciplinary procedure.[111] Upon receipt of the first subpoena or complaint, Stanford forwards a copy of the complaint to the student and instructs the student to remove infringing content from the University network. The instruction requires the student reply to the University within 48 hours, after which the University interrupts their network connection. If the student replies to the complaint or subpoena, the University will reconnect after payment of a $100 fine. On the second complaint, Stanford again sends the student the complaint, but also sends a copy to the residence dean. The

[110] Electronic Frontier Foundation, *When Push Comes to Shove: A Hype-Free Guide to Evaluating Technical Solutions to Copyright Infringement on Campus Networks,* p.10, *available at* http://www.eff.org/files/univp2p.pdf, (last viewed November 11, 2008).
[111] Stanford University, *Student DMCA Complaint Policy & Reconnection Fee, available at* http://www.stanford.edu/dept/legal/Recent/DMCA_Reconnect_fee_Final1007.pdf.

University immediately disconnects the student until he responds to the complaint. If the complaint is resolved, the student may reconnect to the network after payment of a $500 fine. On the third complaint, the University disconnects the student from the network and files a disciplinary action against the student. Stanford will reconnect the student to network if the student indemnifies Stanford from copyright infringement and pays a $1000 fine.

The University of Kansas takes a more aggressive approach. When the University receives notice of a copyright violation, it immediately terminates the alleged infringer's network connection. The University gives the alleged infringer five days to resolve the issue and file an appeal. If the appeal is denied, the alleged infringer's connection is permanently terminated.[112]

These policies may seem aggressive, but universities must respect intellectual property rights such as copyright. The DMCA conditions an ISP's immunity from secondary liability on the termination of a subscriber's connection if he is a repeat offender of copyright infringement.[113] Additionally, universities are developers of intellectual property such as patents and copyrights and should ensure respect and protection of these legal rights.

B. Managing Campus Networks

University legal staff and network departments should align their procedures to ensure efficiency and common objectives in the management of logs of personal identifying information, such as IP logs. The following outlines a few basic principles,

[112] The University of Kansas, IT ResNet, *ResNet and Illegal Downloading, available at* http://www.resnet.ku.edu/newpolicy.shtml (last visited November 20, 2008).
[113] 17 U.S.C. §512(i)(1)(A).

but a full examination of the legal rules and technical details in this field is beyond the scope of this paper.

A university legal department should determine which State and Federal laws are applicable to the retention and destruction of personal identifying information stored on a university network. For example, a university data retention policy should account State and Federal regulations on the retention of personal identifying data, but may also account for current case law defining the boundaries of "good faith" data destruction within the meaning of Fed. R. Civ. P. 37(e) or analogous State civil procedure codes.

A university's stance on the balance between copyright protection and privacy will certainly be a factor to consider when determining how much data to retain outside the bounds of the law. Another factor will be the economics of searching retained data. Once a university is issued a subpoena to disclose personal identifying information of a network user, the university is compelled to search its retained data to find the pertinent information. The more data that is retained outside the bounds of the law, the more resources a university will be forced to expend in searching the database and verifying the retrieved information. In most cases, the university will be expected to use its own resources and will not be compensated. Therefore the university should only retain as much data as required by State and Federal law, and operation of its network.[114]

C. University Response to Legal Process

A university legal staff will certainly follow the university's protocol for responding to subpoenas served on the university. Such a protocol will account for the State and Federal legal rights of university students, staff, and faculty. The protocol will

[114] Electronic Frontier Foundation, *Best Practices for Online Service Providers,* June 2008, p. 6, *available at* http://www.eff.org/files/eff-ospbp-whitepaper.pdf (last visited October 30, 2008).

also comply with jurisdictional and university rules for response to judicial process and the Federal Rules of Civil Procedure.

Informal pre-litigation letters sent to a university should be treated with the same or similar protocol. A pre-litigation letter serves as notice to the alleged infringer. The sooner the alleged infringer has notice, the sooner he will be able to protect his rights and address a pending complaint. A plaintiff will certainly file suit against an alleged infringer if there is no settlement or response to the letter. Upon receipt of a pre-litigation letter inquiring into the personal identifying information of a campus network user, a university should expeditiously search its available records in an attempt to match the IP address to the identifying information of the user. Thereafter the university should give the user notice of the letter.

When a university receives a subpoena, the university should put the alleged infringer on notice as soon as it ascertains his identity. It is common for a university to be subject to a court order requiring the university inform the network user of the legal action. When a University serves notice on the alleged infringer, it allows him to address the complaint and file motions to quash the subpoena and vacate the order granting expedited discovery. If the university is unable to uncover the identity of the alleged infringer in a reasonable amount of time within the subpoena response period, a university should file a motion for extension of time to respond to the subpoena. Courts sometimes issue orders requiring universities allow an alleged infringer sufficient time to file a motion to quash before disclosing any identifying information.[115]

Once the university has knowledge of the alleged infringer's identity, the university's legal staff should consult with the student regarding the nature of his online

[115] *E.g., London Sire,* 542 F.Supp.2d at 161.

activities. The legal staff's inquiry should determine whether the plaintiff's P2P investigator committed any error when obtaining the alleged infringer's IP address. For example, there may have been a false positive detection of copyrighted materials on the alleged infringer's computer.[116] In addition, the alleged infringer may have used the copyrighted work for an educational purpose, a fair use under the copyright statute.[117]

There are a number of circumstances when a university may file a motion to quash a subpoena. If the personal identifying information of the alleged infringer is subject to statutory protection or privilege, the university may file a motion to quash the subpoena under Rule 45(c)(3)(A). The alleged infringer will usually file a motion to quash the subpoena on the same grounds.

Under Fed. R. Civ. P. 45(d)(1)(D), a "person need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost." Under these circumstances a university will have the burden of proving the undue burden or cost. As examined in the cases reviewed above, the subpoena may lack sufficient specificity to enable a university to reply or uncover the subpoenaed information. Additionally, an IP address for a computer connected to the university network may have multiple users. To complicate issues even further, the IP address may be assigned to a computer with a wireless router. Determining the identities of the actual alleged infringers may absorb an unduly burdensome amount of university resources. The university network department may need to perform a forensic investigation of all the personal computers involved with an IP address, as well as an investigation of network logs.

---

[116] Michael Piatek, et. al., *Challenges and Directions for Monitoring P2P File Sharing Networks,* June 1, 2008, *available at* http://dmca.cs.washington.edu/dmca_hotsec08.pdf.
[117] 17 U.S.C. §107.

A university may also file motions to quash a subpoena or vacate a grant of expedited discovery based on a plaintiff's insufficient or misrepresented evidence. A university may request copies of the evidentiary affidavits filed by the plaintiff's P2P investigator. If the university determines there is no *prima facie* showing of copyright infringement, the university may file motions to quash the subpoena and possibly vacate the order granting expedited discovery. If a university thinks that expedited discovery was not justified because of its lengthy retention of IP logs, the school may challenge the discovery on those grounds as well.

However, university legal departments should keep in mind that motions to quash a subpoena usually only result in a second subpoena of narrowed scope. If a subpoena of narrowed scope is the remedy the university seeks due to the burden of the first subpoena, the cost of the motion may be justified. However, due to the expense many universities face in simply complying with subpoenas, it may only be practical to do the best job possible in obtaining the identifying information of the alleged infringers without becoming involved in the judicial process. A university may also view a copyright owner's interests as greater than those of a network user and refrain from contesting discovery for that reason.

There are simple actions the university should take in filing a response to a subpoena. The response should be submitted to the court under seal. The university should not disclose the subpoenaed information to any party other than the court. Additionally, the university should not disclose indentifying information without order of the court. If there is uncertainty as to the identifying information supplied in the response to the subpoena, the university should explicitly describe the source of the uncertainty in

the response. A university may also submit a copy of its policies regarding campus connectivity to the internet and a copy of the university's internet service agreement. These documents will aid the court in determining the privacy rights of the alleged infringers.

D. Compliance with the DMCA

As described in the first section of this paper, ISPs must meet certain requirements of the four DMCA safe harbors in order to obtain immunity from secondary liability for copyright infringement. Despite the fact the DMCA subpoena provisions do not apply to ISPs serving as conduits of infringing communications under 17 U.S.C. §512(a), university ISPs are still subject to injunctions or other equitable relief under the DMCA. Universities should ensure all conditions are maintained under all four safe harbors, §512(a)-(d), so the university's immunity is not compromised.

Some copyright owners put pressure on universities to adopt technological measures, such as software or hardware, to monitor network activity and prevent transmission of copyrighted materials.[118] Universities should be aware there is no legal obligation to adopt these measures, and the technologies will actually increase a university's responsibilities and liabilities.[119] Not only are the technologies expensive, they must be continuously adapted to evolving P2P networks.[120] Usually a staff must be in place to operate and monitor the technology, further depleting university resources without any cost to the copyright owners.

---

[118] Electronic Frontier Foundation, *When Push Comes to Shove: A Hype-Free Guide to Evaluating Technical Solutions to Copyright Infringement on Campus Networks,* p.1-3, *available at* http://www.eff.org/files/univp2p.pdf, (last viewed November 11, 2008).
[119] *Id.* at 2.
[120] *Id.* at 6-8.

Universities should avoid extra-legal monitoring technologies because knowledge of infringement on campus networks imparts further liability and a duty to stop the infringement.[121] For example, the *Napster* court held "contributory liability may potentially be imposed only to the extent that Napster: (1) receives reasonable knowledge of specific infringing files with copyrighted musical compositions and sound recordings; (2) knows or should know that such files are available on the Napster system; and (3) fails to act to prevent viral distribution of the works."[122] Also, the language of the DMCA conditions an ISP's immunity on the ISP's non-interference with the transmission and storage functions of its network.[123] Once an ISP has knowledge, or "awareness of circumstances from which infringing activity is apparent," the ISP must quickly disable access or remove the material in order to maintain immunity.[124] Therefore, by implementing monitoring technologies, ISPs and universities are effectively creating unnecessary work and liability.

It is also important that universities observe the "limitations on liability of non-profit educational institutions" under §512(e) of the DMCA. Section 512(e) applies to faculty and graduate student employees who infringe copyrights. A university's exemption from liability as an ISP applies when a faculty member or graduate student performs an infringing teaching or research function using "transitory digital network communications" under §512(a) or "system caching" under §512(b). Under those circumstances, the graduate student or faculty member is considered a person other than the university for the purposes of liability. The limitation on university liability also

[121] *Id.*
[122] *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1027 (9th Cir. 2001).
[123] 17 U.S.C. §512(a)(2); §512(b)(2)(C)(i).
[124] §512(c)(1)(A)(i)-(iii); §512(d)(1)(A)-(C).

applies when a graduate student or faculty member knowingly infringes copyrights using by providing "direction" to infringing content on the university network under §512(c) or by using "information location tools" to find infringing content under §512(d).

The above limitations on liability require specific actions by the university and its employees. Specifically, the immunity is contingent on the faculty member or graduate student not recommending or requiring online access to infringing materials in a course taught at the university.[125] Also, a university must not have received a 512(c)(3) notice for take down of infringing materials used by the graduate student or faculty member within the preceding three years.[126] As a final requirement, the university must provide information to user's of its network regarding the promotion of compliance with copyright laws.[127]

E. Sovereign Immunity

Congress attempted to abrogate the 11th amendment sovereign immunity of the States with the Copyright Remedy Clarification Act of 1990 (CRCA).[128] Using its Article I powers, Congress added the CRCA to the copyright statute. Section 511 (the CRCA) of the copyright statute reads, "any State, instrumentality of a State, and any officer or employee of a State" is not immune from copyright infringement under the federal copyright statute, notwithstanding the 11th amendment.[129]

However, in *Seminole Tribe of Florida v. Florida,* the Supreme Court held that the States' sovereign immunity cannot be abrogated by an act of Congress based on

[125] §512(e)(A).
[126] §512(e)(B).
[127] §512(e)(C).
[128] §511.
[129] *Id*.

Article I powers.[130] In a later case, *Florida Prepaid Postsecondary Education Expense Board v. College Savings Bank*, the Supreme Court held Congressional legislation eliminating State's sovereign immunity from patent infringement to be unconstitutional, because it was based on Article I powers.[131] Therefore, by implication the CRCA is no longer valid. Since the *Florida Prepaid* decision, a number of lower federal courts across several jurisdictions have held the CRCA unconstitutional.[132]

The details of what constitutes waiver or abrogation of a State's sovereign immunity is beyond the scope of this paper. However, a State may waive its sovereign immunity if it invokes federal jurisdiction.[133] The waiver must be a voluntary invocation of federal jurisdiction or a "clear declaration" by the State that it intends to waive the immunity.[134] Additionally, an injunction may be issued against a State officer, whose actions have connection with enforcement of an unconstitutional State law.[135] State university legal staff should become familiar with this area to understand the limits of sovereign immunity for their institution.

F. Conclusion

Federal law related to peer-to-peer copyright infringement is constantly evolving in response to technological advances. University legal staff must keep abreast of developments in strategies used by copyright owners in protecting their intellectual

---

[130] 517 U.S. 44, 72-73 (1996)
[131] 527 U.S. 627, 647-648 (1999) (holding that Article I does not give Congress the power to enact such legislation).
[132] See, e.g., *Rodriguez v. Texas Comm'n on the Arts,* 199 F.3d 279, 281 (5th Cir. 2000); *Chavez v. Arte Publico Press,* 204 F.3d 601, 607-8 (5th Cir. 2000); *Mktg. Info. Masters, Inc. v. Bd. of Tr. of California State Univ. Sys*, 552 F.Supp.2d 1088, 1093-95 (S.D.Cal. 2008); *Nat'l Ass'n of Bd.s of Pharmacy v. Board of Regents of University System of Georgia*, No. 3:07-CV-084 (CDL), 2008 WL 1805439 at *16 (M.D.Ga. 2008).
[133] *College Sav. Bank v. Florida Prepaid Postsecondary*, 527 U.S. 666, 675-76 (1999) (companion case to *Florida Prepaid,* 517 U.S. 44).
[134] *Id.*
[135] *Ex parte Young*, 209 U.S. 123, 157 (1908).

property. A balance between protection of intellectual property rights and protection of university network user privacy should be an ideal underlying policies and practices of institutions. Hopefully this paper provides useful tips to maintain and establish such a balance in the midst of the changing legal and technological climate.