INTELLECTUAL PROPERTY AND FREE SPEECH IN THE ONLINE WORLD:

How Educational Institutions and Other Online Service Providers Are Coping with Cease and Desist Letters and Takedown Notices

A Public Policy Report

by Laura Quilter and Marjorie Heins

BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
FAIR USE NETWORK

The Brennan Center for Justice, founded in 1995, unites thinkers and advocates in pursuit of a vision of inclusive and effective democracy. The Free Expression Policy Project, founded in 2000, provides research and advocacy on free speech, copyright, and media democracy issues. FEPP joined the Brennan Center in 2004, and developed the Fair Use Network in 2006.

Michael Waldman
Executive Director

Deborah Goldberg
Director
Democracy Program

Marjorie Heins
Coordinator
Free Expression Policy Project

This report (version 1.0.2, Feb. 14, 2007) is available online at http://fairusenetwork.org/resources/OSPreport-2007.pdf .

Thanks to Evan Hill-Ries, Kate Kaufmann, Shilpa Malik, Nicholas Smallwood, and Rob Stillwell for research assistance.

Thanks to Howard Besser, Strata Chalup, Julie Cohen, Karl Fattig, Eric Goldhagen, Bill Humphries, Jason Schultz, Chris Shaffer, and Heather Whipple, for referrals and suggestions. Additional thanks to Eric Goldman, Liz Henry, Jack Lerner, Wendy Seltzer, and Jennifer Urban for reviewing the manuscript and for offering valuable suggestions throughout the project and about the manuscript.

Finally, deep appreciation to all the people we interviewed who spent so much time discussing their perspectives and the challenges they face. Needless to say, without them, this report would not have been possible.

We acknowledge the generous support of the Rockefeller Foundation, the Educational Foundation of America, and the Andy Warhol Foundation for the Visual Arts.

© 2007 Laura Quilter and Marjorie Heins
This work is licensed with the Creative Commons "Attribution – Noncommercial – Share Alike" 2.5 license. It may be reproduced in its entirety as long as the Fair Use Network is credited, a link to the website (http://fairusenetwork.org/) is provided, and no charge is imposed. If derivative works are created from this report, they must also be licensed under the Creative Commons "Attribution – Noncommercial – Share Alike" license.

CONTENTS

I. INTRODUCTION AND SUMMARY OF FINDINGS

Following up on our 2005 report, *Will Fair Use Survive?*,[1] the Free Expression Policy Project undertook a survey of 25 online service providers to learn how they handle notices asking them to remove material that the sender alleges violates her copyright or trademark rights. These notices typically take the form of either "cease and desist" letters or takedown notices sent in accordance with § 512 of the Copyright Act.[2] We wanted to learn whether service providers, including educational institutions, consider their users' free speech interests in the course of responding to copyright and trademark owners' complaints; and if so, how they act on those considerations. We also wanted to know how well the takedown process is working for service providers, for users, and for copyright owners.

Service providers are crucial gatekeepers, providing access to a vast quantity of opinion, news, information, and creative expression of all kinds. Service providers are also significant platforms for speech, hosting websites, mailing lists, Usenet newsgroups, bulletin boards, wikis, blogs, and discussion forums of all conceivable types. Because service providers play such a critical role in free expression, we wanted to understand the forces that determine their responses to fundamental policy questions such as when and how to terminate users or take down user-generated material from the Internet. We also wanted to understand the effects of such decisions. Our goal was to identify factors that shape service providers' policy development. By identifying such factors, we hoped to be able to recommend changes that would better shape the environment in which service providers operate, fostering free expression while at the same time respecting the needs and interests of service providers, rightsholders, and users.

Our findings, as described in this report, can be summarized as follows:

First, we learned that large educational institutions and other service providers are swamped by notices about peer-to-peer filesharing ("P2P") and "abuse" complaints relating to spam, viruses, phishing, and network security. This environment shapes service providers' policies for handling takedown notices of all sorts. Thus, notices that raise significant free speech concerns are handled under procedures developed to mass-process a flood of P2P and "abuse" complaints. Institutions that offer multiple types of Internet services operate on a "most restrictive" basis, failing to take full advantage of the immunities

[1] Marjorie Heins and Tricia Beckles, *Will Fair Use Survive? Free Expression in the Age of Copyright Control* (Free Expression Policy Project, 2005) (hereafter "Fair Use Report").

[2] 17 U.S.C. § 512, passed as part of Title II of the Digital Millennium Copyright Act ("DMCA").

from liability, as well as the "safe harbors," made available by the law. In particular, we found that service providers extend the takedown procedure outlined in § 512(c) of the copyright law to notices targeting P2P, which is covered by a different section, § 512(a). Section 512(a) does not require takedown. Additionally, floods of complaints about filesharing, spam, and so forth, lead to strong institutional responses that pose new threats and challenges for free speech. Among these responses are network monitoring, policing, unbalanced education about copyright, and automatic cutoff of access to the Internet or to the campus network.

Second, the flood of P2P notices places significant burdens on service providers. The situation is particularly acute for large educational institutions, which, while protected from liability for the majority of the complaints, are not protected from political pressure to respond to the complaints. The costs of responding to § 512 notices also affect free expression, by redirecting resources away from institutions' educational and nonprofit missions, and by forcing them to trade substantive reviews and free expression defenses for automated, standardized, and risk-averse behaviors.

Third, although takedown procedures differ among educational institutions and other service providers, when in doubt, and when forced to deal with floods of notices and/or political pressure, institutions tend to take a much more restrictive stance than is warranted by the law. Ignoring possible fair use and other defenses reduces the access of both online speakers and the general reading and communicating public to the free-expression resources of the online world.

Fourth, this restrictive stance is driven in part by the confusing nature of the law and the lack of solid information and model policies for service providers. While large institutions can afford to pay for policy and copyright counsel, even they can be confused by the structure of § 512. Small institutions, whether educational, other nonprofit, or commercial service providers, depend on external sources of information, and unfortunately, there are few outside experts and models. Some professional associations have produced useful materials in this area, but much remains to be done.

Lastly, while the institutions that operate as gatekeepers to online speech are wrestling with these questions, the situation for users is grim. Users have little access to information about how commercial service providers handle speech-related complaints, and little recourse should an educational institution or other service provider take an overly strict or inflexible approach to responding to copyright or trademark complaints.

Throughout the report, we offer a series of recommendations and proposed "best practices" for service providers. The most important of these are founded on principles of ***transparency***, ***process***, and ***education***—principles that benefit service providers, users, and senders alike.

- *Transparency* means disclosing publicly institutional procedures for handling speech-related complaints; sharing information about how and by whom the process is used; and disclosing the costs of enforcing the claims of copyright owners.
- *Process* means establishing fair procedures—following the law closely, and not extending it to cut off Internet access, take down materials, or divulge user information without an opportunity for the user to respond to the complaint and participate in the decision-making process.
- *Education* means providing people with accurate and complete information about their legal duties and rights.

These best practices, along with model policies and notices, will be released in separate "toolkits" aimed at helping online service providers establish practices that are both legally prudent, responsive to the "bottom line," and protective of free expression.

We hope this report will be of use to service providers, both as an introductory reference for § 512 and the larger legal environment of intellectual property, and as a means to assess risk and balance their own goals with their duties to their users and to copyright holders. We also hope the report will be helpful to users who have found themselves entangled in intellectual property disputes or who are concerned about their rights and responsibilities. Finally, we hope the report will advance the dialogue on free expression balances to intellectual property rights.

II. BACKGROUND

A. Methodology

We conducted in-depth interviews with representatives of 25 service providers—eight educational institutions, nine nonprofits, and eight commercial service providers.[3] We supplemented this research with reviews of publicly available information from 52 service providers about their policies, and discussions with experts, to develop a broader picture of policies that different service providers adopt, and the factors that affect their decisions.

We chose our 25 service providers based on market shares and known experiences with or leadership roles on copyright or free speech issues. Because we were interested in identifying best practices, we particularly sought to include service providers with experiences to share, as well as service providers with little experience. Although the service providers we talked to did not represent a random sample, we were careful to include a variety of them in our survey, ranging from small nonprofits to large

[3] The Appendix lists all of those interviewed and their institutional affiliations.

for-profit corporations, and educational institutions of different sizes. In some instances, we talked with more than one institutional representative.

We gave each interviewee the opportunity to review our notes for accuracy. Most of them spoke with us only on condition of anonymity regarding specifics of their situation.

B. Terminology

Because this report crosses technological, business, and legal worlds, it necessarily contains legal and industry-specific terminology, which we have defined below.

Two major statutes protect service providers from liability for material posted by their users: **§ 230**,[4] which establishes a broad **immunity** from liability as a "publisher" for user-created material, and **§ 512** of the Copyright Act, which provides a contingent **"safe harbor"** from liability for copyright infringement. We describe these statutes in greater detail in Section C.

Although our report is focused primarily on the § 512 takedown process and therefore copyright issues, service providers do not always distinguish in practice between copyright and other types of intellectual property such as trademark or right of publicity, or even between intellectual property and other types of rightsholder complaints, such as invasion of privacy or defamation. Consequently, we specify **"copyright"** or **"copyright holder"** where appropriate, but otherwise use more general terms such as **"intellectual property"** (or **"IP"**).

We use **"copyright industry"** for the large industries that take mass action to enforce their copyrights, including publicity, litigation, and enforcement campaigns. **"Enforcement company"** refers to businesses set up primarily or substantially to locate potential infringing online files and send notices or complaints about them.

We use **"complaint"** to refer to any notice or letter sent to a service provider regarding a user's content. It includes both takedown notices sent under §§ 512(c) and (d), and filesharing complaints sent to Internet access providers (§ 512(a) services). "Complaint" also includes cease and desist letters that assert copyright, trademark, or other legal claims. We use **"takedown notices"** to describe copyright complaints sent under §§ 512(c)-(d) to request removal of hosted materials or of links to allegedly infringing content.

[4] Section 230 is the common name for 47 U.S.C. § 230, passed, with the Communications Decency Act, as part of the 1996 Telecommunications Act.

We also use the term **"user,"** which, while not ideal, encompasses all users of OSP services, including students, staff, and faculty at educational institutions, subscribers of commercial service providers, individual subscribers of hosting services, and subjects of indexing services. We use **"targeted user"** to refer to users who are the subject of cease and desist or § 512 takedown notices. **"Subscriber"** we reserve for those users who pay for hosting or Internet access services.

We use **"service provider"** or **"online service provider"** to refer to the broadest set of online service providers, encompassing Internet access providers, content hosts and publishing platforms, and search engines and information location tools. No other term uniquely encompasses the wide variety of services covered by the term service provider, and the term "ISP" ("Internet service provider") carries multiple meanings. Moreover, many services providers offer multiple services.

To refer only to specific sectors within the service provider industry, we use the following terms: **"Internet access provider"** describes entities offering dial-up, cable, DSL, or leased-line Internet access. These services are covered by § 512(a). **"Host"** or **"hosting provider"** describes entities that own or operate servers or networks, on which their "users" or "subscribers" place their own content, ranging from comments, email messages, websites, databases, or files such as software programs, music recordings, or video files. This category includes web hosting services such as blog hosts, video hosts (like YouTube), wikis (like Wikipedia), and mailing list archives. These services are covered by § 512(c).

Colocation services (or **"colo's"**) provide a facility (a "data center") for machines. Typically, colocation services include Internet access, power management, and climate control; the subscriber owns the server, and is responsible for its maintenance and management.

Hosting services have proliferated in the past few years. **Web and blog hosts** permit users to develop and load websites that can include a variety of content. A minimal web host might permit only limited ability for users to manipulate their websites and publish different kinds of files. A full-scale web host permits users to run their own programs, databases, and a variety of web services, such as streaming files. **Host resellers** are webhosts that permit and facilitate their subscribers to "resell" their hosting subscriptions, thus permitting subscribers to easily become webhosts themselves.

Media and file hosts permit their users to upload files and make them available via the Internet. Media hosts—most commonly found in the commercial service provider sector—permit users to upload media files, such as videos (Bolt, Vidiac, YouTube) or photos (Flickr, Ofoto, Shutterfly). Often, these sites offer the subscriber the opportunity to restrict public access; permit public interactivity, such as

commenting or keyword tagging ("tagging"); or permit the public to buy copies of the work printed on tangible goods such as mugs or t-shirts.[5]

Search engines and **"information location tools"** permit users to locate information and files. Section 512(d) defines this category broadly, to include "a directory, index, reference, pointer, or hypertext link."

Finally, **"fair use"** refers to the legal right to copy and distribute parts, or sometimes all, of a copyrighted work without permission, for purposes such as commentary, research, and teaching. Fair use is one of several substantive defenses to claims of copyright infringement.[6]

C. The Legal Environment for Service Providers: Section 230 Immunity and Section 512 "Safe Harbors"

Service providers operate in a rapidly changing technological, economic, and legal environment. The industry itself is relatively new, and has shifted dramatically over its lifespan, from small and hobbyist-run dial-up bulletin board systems ("BBS's") in the 1970s and '80s to a mass-consumer industry by the mid-late 1990s. Numerous private and proprietary commercial networks, including cell phone networks, continue to flourish, often offering access to the Internet.

This evolution did not occur in a legal and regulatory vacuum, driven only by economic and technological forces. Law and government regulation have shaped the service provider industry, particularly since the mid-1990s. Since 1996, Congress has enacted numerous laws that significantly affect service providers, beginning with the 1996 Telecommunications Reform Act.[7] Courts, similarly,

---

[5] Other types of services included in our report, but not discussed specifically, include *collaborative services hosts* that permit collaborative development of resources, such as wikis, groupware, or collaborative databases; and *communications hosts*, which offer communications services such as email, mailing lists, discussion groups, bulletin boards, chat and instant messaging, and real-time communication.

[6] Fair use is codified at 17 U.S.C. § 107. For more information, see http://fairusenetwork.org/ .

[7] Major statutes include the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified at scattered sections of 47 U.S.C.) (which included the Communications Decency Act ("CDA"), 47 U.S.C. § 223, struck down in *Reno v. ACLU,* 521 U.S. 844 (1997)); revisions to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000), ("CFAA") in 1994, 1996, and 2001; the No Electronic Theft Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified at 17 U.S.C. 101, 506-07, 18 U.S.C. 2319-20, 28 U.S.C. 994, 1498 (2000)); the Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, Title XIII (1998) (codified at 15 U.S.C. §§ 6501-6506) ("COPPA"); the Child Online Protection Act, Pub. L. No. 105-277, 47 U.S.C. 231 (1998) ("COPA"; a preliminary injunction was entered against COPA's enforcement and at this writing, the case has not been finally decided; *see Ashcroft v. ACLU*, 542 U.S. 656 (2004)); the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.) ("DMCA"); the Anticybersquatting Consumer

have closely reviewed the duties of service providers with respect to their users' speech, considering the impact of both new statutes and traditional laws on the online medium. Issues have included service providers' potential liability for "publishing" defamatory speech posted by users, for secondary copyright infringement, and for invasion of privacy.

The spate of litigation and proposed legislation spurred service providers to organize and lobby Congress. Their first efforts were in response to the legislative proposals that became the Communications Decency Act ("CDA"), which purported to regulate "indecent" speech online. Service providers initially resisted the regulation, but ultimately dropped their resistance in exchange for a section of the law that not only immunizes service providers' from liability for efforts they may take to block material that is considered "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable," but provides even broader immunity by declaring that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[8] While the CDA was struck down as a violation of the First Amendment in *Reno v. ACLU*,[9] the immunity provision, known as § 230, survived. Today, § 230 case law provides a robust set of protections for service providers against potential liability for statements made by their users, applying to numerous legal claims including invasion of privacy and discrimination.[10] Section 230 is a straightforward immunity that applies to virtually all service providers.

Protection Act ("ACPA," 1999); the Children's Internet Protection Act, Pub. L. No. 106-554 (codified at 20 U.S.C. § 9134(f) (2000) and 47 U.S.C. § 254(h) (2000)) ("CIPA"), upheld in *U.S. v. American Library Association*, 539 U.S. 194 (2003)); the CAN-SPAM Act of 2003, Pub. L. No. 108-187 (codified at 15 U.S.C. § 7701-7713, 18 U.S.C. § 1037, 28 U.S.C. § 994 (2003))—and those are just the major federal laws.

[8] 47 U.S.C. §230(c)(i) and (ii). *See Barrett v. Rosenthal*, 40 Cal. 4th 33, 146 P.3d 510, 51 Cal. Rptr. 3d (Cal. Sup. Ct., Nov. 20, 2006), available at http://eff.org/legal/cases/Barrett_v_Rosenthal/ruling.pdf (review of the legislative history, pp. 17-21 of the PDF).

[9] See note 7, *supra*.

[10] One of the earliest, and broadest, readings of § 230 held that it establishes immunity "to any cause of action that would make service providers liable for information originating with a third-party user of the service." *Zeran v. AOL*, 129 F.3d 327, 330 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998). Section 230 has subsequently been applied in more than 50 cases, almost all of them protecting the service provider from liability. *E.g.*, *Carafano v. Metrosplash.com*, 339 F.3d 1119 (9th Cir. 2003) (website operator immune for dissemination of private information); *Fair Housing Council of San Fernando Valley v. Roommate.com, LLC*, Case 4:05-cv-00010-RAS, 2004 WL 3799488, 2005 WL 3299077 (C.D. Cal. Sept. 30, 2004) (online bulletin board systems not liable for dissemination of discriminatory housing postings); *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, No. 1:06-CV-00657, 2006 WL 3307439 (N.D. Ill., Nov. 14, 2006) (same).

Service providers were soon faced with another threat: possible liability for their users' copyright infringements. Section 230 specifically excludes intellectual property claims from its immunity,[11] and a series of cases left service providers concerned that they could be held liable for their users' infringements.[12] Consequently, large commercial service providers, primarily Internet access providers, asked Congress for relief, also seeking to stave off aggressive liability rules for which the copyright industries were lobbying. Although service providers had a strong argument that, like telephone companies, they were simply conduits, and should not be held liable for the speech of their users,[13] Congress developed a compromise: a contingent safe harbor for service providers, exempting them from liability for their users' copyright infringements, so long as they took certain actions.[14] The required actions were based on the type of service the service provider offered.

The contingent safe harbor from copyright liability, known as § 512, lays out a much more elaborate regime than the straightforward immunity provided by § 230. Sections 512(a), 512(c), and 512(d) establish criteria and procedures for three different classes of online service.[15] Internet access services are covered by the straightforward safe harbor of § 512(a), which protects service providers from

[11] 47 U.S.C. §230(e)(2). Section 230's application to state intellectual property claims, such as trade secrets, state trademark, right of publicity, or common law copyright, is unclear.

[12] *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fl. 1993) (bulletin board Frena was directly liable for violating Playboy's rights of distribution and display) and *Sega Enterprises Ltd. v. MAPHIA*, No. CIV. A. 93-4262 CW, 1997 WL 337558 (N.D. Cal. June 9, 1997) (finding MAPHIA liable for contributory infringement for its bulletin board users' infringements of Sega's copyrights). Service providers were also concerned about the expansive reading of vicarious liability in *Fonovisa v. Cherry Auction*, 76 F.3d 259 (9th Cir. 1996), which found an auctioneer liable for copyright infringement for providing facilities to vendors selling bootlegs.

[13] See Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act," 22 *Santa Clara Comp. & High Tech L.J.* 621 (2006) (hereafter "Takedown Notices Study"), § III; Cassandra Imfeld and Victoria Smith Ekstrand, "The Music Industry and the Legislative Development of the Digital Millennium Copyright Act's Online Service Provider Provision," 10 *Comm. L. & Pol'y* 291 (2005); and Jessica Litman, *Digital Copyright: Protecting Intellectual Property on the Internet* (2000), for detail on the legislative maneuvering.

[14] The Online Copyright Infringement Liability Limitation Act ("OCILLA"), Title II of the DMCA (1998), codified at 17 U.S.C. § 512.

[15] Sections 512(b) and 512(e) provide slightly different safe harbors. Section 512(b) provides a safe harbor for network caching, but was applied to search engine caching in 2006, in *Field v. Google,* 412 F. Supp. 2d 1106 (D. Nev. 2006), and *Parker v. Google*, 422 F. Supp. 2d 492 (E.D. Pa. 2006). Because the scope of this safe harbor remains unclear, and it seems at any rate to have been little used, we exclude it from this discussion. Section 512(e) is a safe harbor for educational institutions, and we discuss it at greater length in Section III.B.1 below.

money damages for their subscribers' copyright infringements.[16] These include broadband and leased-line services provided by Comcast, AT&T, Verizon, and the like, and Internet access (wireless or Ethernet) to campus residence halls and other buildings for students or others to use with their own laptops. Eligibility for § 512(a)'s straightforward safe harbor is *not contingent* on "taking down" allegedly infringing material. It is only contingent on § 512(i), which requires that service providers "accommodate … and [] not interfere with standard technical measures" and "adopt [] and reasonably implement[] … a policy that provides for the termination in appropriate circumstances of subscribers and account holders … who are repeat infringers."[17]

Section 512(c) covers hosting services: the websites, chatrooms, bulletin boards, blogs, gaming networks, and wikis that reside on someone else's machine but permit users to connect and interact, and also to store, manipulate, and publish data or other material. Hosting services are given a safe harbor contingent on their "expeditious" compliance with "takedown notices." Under § 512(g), if the hosting service notifies its subscribers of § 512(c) takedowns, and accepts and processes "counternotices," then it also receives a safe harbor from liability for wrongful takedowns.[18] The counternotice procedure thereby offers subscribers a way to get material reinstated, but only 10-14 days after the subscriber submits the counternotice; material is thus offline for at least 10 days.

Section 512(d) offers a safe harbor to "information location tools"—including search engines—if they remove links to allegedly infringing content on receipt of a takedown notice.[19] By its terms, the counternotice applies to § 512(c) notices; however, language within the statute arguably suggests that it

---

[16] Sections 512(a)-(d) offer safe harbor against money damages. All service providers are subject to court actions for injunctive relief to terminate a subscriber under § 512(j).

[17] Failure to comply with the specifics of § 512 has cost service providers their safe harbor. In the *Aimster* case, for example, the instant message-based P2P service had failed to have a § 512(i) policy for terminating repeat infringers. *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003). In *Ellison v. Robertson*, the service provider (AOL) had failed to update its email address with the Copyright Office per § 512(c). 357 F.3d 1072, 1080 (9th Cir. 2004).

[18] Service providers also typically preclude such liability in their "terms of service."

[19] Even without the safe harbor, it is unlikely that links pose a significant risk of copyright liability. One case suggests links could support liability, but other cases have indicated otherwise. *See Intellectual Reserve, Inc. v. Utah Lighthouse Ministry*, 75 F. Supp. 2d 1290, 1294-95 (D. Utah 1999); *compare Perfect 10 v. Google*, 416 F. Supp. 2d 828 (S.D. Cal. 2006) (appeal pending) (no liability for linking to infringing materials); *Ticketmaster v. Tickets.com*, No. CV 99-7654 HLH(BQRX), 2000 WL 525390 (C.D. Cal. Mar. 27, 2000) (not reported) (issuing a preliminary order denying an injunction because, in part, there was no liability for linking); *Bernstein v. J.C. Penney, Inc.*, No. 98-2958 R EX, 1998 WL 906644 (C.D. Cal. Sept. 29, 1998) (linking was neither contributory nor direct infringement).

may also be applicable to § 512(d) notices.[20] Even if the counternotice provisions are applicable to § 512(d) service providers, however, the statute offers little incentive for them to provide a "counternotice" procedure. The statutory counternotice provision offers the service provider immunity from liability to its subscriber; but it is questionable whether search engines would ordinarily be liable for failing to include content in their index. Offering a counternotice option may not always be feasible, in any case; search engine companies do not necessarily have easy access to contact information for the person or entity who posted the allegedly infringing content.

A service provider may be eligible for protection under multiple subsections of § 512,[21] but as discussed below, may not find it feasible to treat notices differently in its procedures.

User safeguards include the § 512(g) counternotice procedure, which, however, appears to be little used (see Section III, Findings and Recommendations, below); and § 512(f), which provides penalties for "knowing material misrepresentations" made in a notice or counternotice.

While § 512 offers service providers safe harbor from liability for copyright infringements committed by their users, it is important to understand that it is not settled that service providers necessarily would be liable for such infringements in the absence of § 512. Courts have examined relatively few cases that relate to service provider liability for their users' infringements, and those few cases have had some conflicting outcomes.[22] Section 512 provides service providers certainty against the

---

[20] Section 512(g) offers a safe harbor "for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing…." The safe harbor is contingent on the service provider notifying the subscriber, accepting counter notification, and replacing material. Because § 512(g)(2) describes material "to which access is disabled," the provision arguably applies to § 512(d) providers as well.

[21] 17 U.S.C. § 512(n); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, n. 26 (C.D. Cal. 2002).

[22] The relative dearth of cases is certainly due in part to the takedown remedy offered by § 512. Those cases available have been somewhat inconsistent. For example, a couple of cases, prior to the enactment of § 512, found service providers liable. *See Sega Enterprises Ltd. v. MAPHIA*, No. CIV. A. 93-4262 CW, 1997 WL 337558 (N.D. Cal. June 9, 1997) (bulletin board MAPHIA was contributorily liable for its bulletin board users' infringements of Sega's copyrights) and *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fl. 1993) (bulletin board Frena was directly liable for violating Playboy's rights of distribution and display). A few other pre-§ 512 cases found service providers liable where they engaged in some editorial functions. *See, e.g., Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 513 (N.D. Ohio 1997) (service provider that screened uploads was liable for users' copyright infringements) and *Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F. Supp. 543, 552 (N.D. Tex. 1997) (service provider that edited and distilled the content of Usenet postings to select the adult photos was liable for copyright infringement where Usenet-posted materials infringed). But several other cases have found no liability for the service provider. *See Costar Group v. Loopnet, Inc.*, 373 F.3d 544 (4th Cir. 2004) (service provider not directly liable for copyright infringement); *Marobie-FL Inc. v. National Assoc. of Fire Equip. Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997) (service provider not directly or

possibility of liability for money damages, as long as they follow its requirements and do not possess knowledge of conduct that would raise a "red flag" for infringement. As one scholar recently put it, § 512 is "more an encouragement than a requirement."[23]

To summarize the rather convoluted statutory scheme, service providers have an immunity under § 230 for most legal claims against their users. They also have a safe harbor against copyright claims if they comply with the provisions of § 512. Takedown notices sent under § 512 therefore have legal consequences. Cease and desist letters, by contrast, may be sent to anyone; they are intended to put their recipient on notice of the claimed infringement—and often, to pressure the recipient into compliance—but they generally have no independent legal force.

Unfortunately for the best-laid plans of Congress and the rightsholder industries, even as § 512 was being passed, new technologies were rendering it obsolete. Peer-to-peer ("P2P") software enabled users to share files directly without "hosting" their sites on a remote server, obviating the entire notice-and-takedown process elaborated by § 512. Because the files are shared directly from one user's machine to another's, and not stored on a remote server, P2P services are not easily classified according to the subparts of § 512. Moreover, P2P services themselves have used varying technologies, further complicating any attempt to fit this class of services and software into the § 512 regime. P2P software is not the only class of online service that does not fit well within § 512,[24] and it is certain that more services will be developed that will not fit into the specific and detailed structure. The complex and detailed system set forth in § 512, in retrospect, was overengineered, in contrast with the simple immunity established in § 230.

Because users have largely turned to P2P networks to share copyrighted files, rightsholder industries' enforcement efforts have likewise focused on P2P networks. But because P2P software does not fit closely within § 512's services categories, rightsholder industries have taken two principal approaches toward eliminating the "P2P menace." First, they have targeted P2P software developers, arguing that they are guilty of "secondary" copyright liability or even direct infringement. These attacks

---

vicariously liable for hosting infringing material, but potentially liable for contributory infringement); and *Religious Technology Center v. Netcom*, 907 F. Supp. 1361 (N.D. Cal. 1995) (service provider not directly liable for hosting infringing material; but court suggested that, while Netcom was not liable in this case for contributory or vicarious infringement, such secondary liability was a possibility); *see also* note19, *supra*, discussing one case finding potential liability for linking (*Utah Lighthouse Ministry*) and three finding no liability for linking (*Perfect 10 v. Google*; *Ticketmaster*; and *Bernstein*).

[23] Jonathan Zittrain, "A History of Online Gatekeeping," 19 *Harv. J.L. & Tech.* 253, 268 (2006).

[24] For instance, the "age verification" services offered by an online service provider in the adult content area were troubling to a court, which considered them within § 512(d) but noted the misfit. *Perfect 10 v. Cybernet*, 213 F. Supp. 2d 1146, 1175 and n.19, *supra* note 21.

have resulted in a series of P2P-related decisions, beginning with *Napster* and *Aimster*,[25] culminating in the Supreme Court's 2005 decision in *Grokster*,[26] and including *UMG v. Bertelsmann*[27] (alleging that venture capital support of a P2P company constitutes a form of secondary, or more properly, tertiary, infringement).

The rightsholder industries' second mode of attack has been to target P2P users, rather than the P2P software developers, most often by sending notices about their alleged infringements to their service providers.[28] By all accounts, large-volume rightsholders have sent *at least* tens of thousands of P2P filesharing complaints, asking for material to be taken down or removed.[29] P2P users' service providers are, of course, acting as Internet access providers, protected by the § 512(a) safe harbor that imposes no obligation to take down material on receipt of a complaint. Nor could it; Internet access providers do not control the user's machine. The service provider's options are to ignore the complaint; notify the user about the complaint; ask or demand that she remove the material; or cut off her Internet access.

---

[25] *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001) ("Napster I") (affirming a preliminary injunction against the online service because Napster's centralized architecture rendered it likely liable for control of the service; and holding that the § 512 safe harbors were inapplicable to Napster services because Napster had "red flag" knowledge of infringement and had no copyright compliance policy under § 512(i)); *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2002) ("Napster II"), affirming 2001 US Dist. LEXIS 2186 (N.D. Cal. Mar. 5, 2001); *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003) (liability because of knowledge of infringement, and lack of evidence of noninfringing uses; § 512 safe harbors inapplicable because *Aimster* did nothing to stop repeat infringers and thus did not implement § 512(i)).

[26] *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (reversing a judgment that filesharing services were not liable for secondary infringement because their technology was capable of substantial noninfringing uses, and strongly suggesting that the services would be liable because they knowingly induced infringement by their users).

[27] *UMG Recordings, Inc. v. Bertelsmann AG*, 222 F.R.D. 408 (N.D. Cal. 2004) (allowing a secondary liability claim to go forward against Napster's investors, finding that they had assumed substantial control) (appeal pending). On appeal, five cases by recording industry companies against investors in Napster were consolidated; oral arguments were heard Sept. 13, 2006.

[28] They have also sued users directly, resulting in one decision, *BMG Music v. Gonzalez*, 430 F.3d 888 (7th Cir. 2005), which held that downloading and retention of files from a P2P network was direct copyright infringement. Several others are in litigation. *See Recording Industry vs the People* at http://recordingindustryvspeople.blogspot.com/ (last visited Jan. 13, 2007). The copyright industries have relied on § 512(h), which allows them to subpoena information from service providers in certain circumstances, but lost the battle to apply these subpoenas to Internet access services. *RIAA v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 543 U.S. 924 (2004).

[29] *See* Takedown Notices Study, *supra* note 13, 22 *Santa Clara Comp. & High Tech L.J.* 652, n.99. These reports suggest individual large Internet access providers receive tens of thousands of notices per year, per service provider. It is likely that, across all service providers and over the years since § 512 was passed, the total number of notices has amounted to more than a million.

Nevertheless, based on our interviews, it appears that many service providers that offer both hosting and access services treat a P2P filesharing notice as a *de facto* § 512(c) notice, and while they cannot "take down" the file, they "take down" the user—cutting off network or Internet access. Needless to say, this is a significantly broader remedy than that offered by 512(c), which authorizes only removal of the allegedly infringing *content.*

The § 512(c)-(d) notice and takedown procedures are used very differently. According to the only study thus far on the issue, these provisions are largely used by small rightsholders of various sorts,[30] although in some sectors of the service provider market, such as video hosts, the situation may be different.[31] Small copyright holders are often trying to protect photographs, poems, graphics, news, or commentaries; but a significant number of small copyright holders target competitors. Others attempt to route around § 230 by reconfiguring their privacy, trademark, defamation, and other complaints as copyright claims that can be addressed under § 512.[32] Abuses, misuses, and over-uses may stem in part from legitimate confusion on the part of small rightsholders.

The ability of rightsholders to target users through their service providers was a choice Congress made, balancing the potential harms to individual users from overreaching by copyright owners against the potential gains to the copyright industries in combating copyright infringement on the Web. As previous studies have found, however, there have been significant misuses of the statute, to the likely detriment of free speech and fair use, and little apparent benefit to large rightsholders in combating copyright infringement online.[33] Service providers are caught in the middle, and their role as gatekeepers is as crucial today as it was prior to the passage of § 512 and § 230.

---

[30] Takedown Notices Study, *supra* note 13, 22 *Santa Clara Comp. & High Tech L.J.* at 651, found 6% and 3% of notices sent under §§ 512(c) and (d), respectively, were sent by or on behalf of the movie or music industries. The major exception was the software industry, which sent numerous notices to Google and Blogger; however, these notices generally involved alleged anticircumvention of digital locks of various types, which are not copyright infringement, and, consequently, are not eligible for the § 512 process. *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 217 (S.D.N.Y. 2000).

[31] Video websites such as Vidiac, in our survey, and YouTube, more famously, report receiving notices from large copyright industry rightsholders. These services were not included in the Takedown Notices Study; more comprehensive, and ongoing, study is definitely needed.

[32] Takedown Notices Study, *supra* note 13, 22 *Santa Clara Comp. & High Tech L.J.* at 651 and 678 (finding significant use of § 512 by persons asserting privacy or other non-copyright interests; more than half of notices sent regarding Google's search engine were competition-related).

[33] Fair Use Report, *supra* note 1; Takedown Notices Study, *supra* note 13.

III. FINDINGS AND RECOMMENDATIONS

In section A below, we describe one striking feature of the takedown process, as revealed by our survey. We then discuss challenges and opportunities applicable to three categories of service providers—educational institutions, nonprofit service providers, and commercial service providers. In each section, we also highlight particular challenges to free expression and an open information ecology.

A. Rights Enforcement Companies: Hired Guns in the Copyright Wars

A major complaint of both educational institutions and larger commercial service providers concerned rights enforcement companies and agencies. The copyright industries hire companies such as BayTSP and NetEnforcers to detect possible copyright infringement; these companies send the vast majority of notices to the service providers we interviewed.[34] Other frequent industrial-sized senders include a few large individual rightsholders such as Universal or Paramount, and rightsholder associations such as the Recording Industry Association of America ("RIAA"), Motion Picture Association of America ("MPAA"), Entertainment Software Association ("ESA"), and Business Software Association ("BSA"), which send notices on behalf of their constituent members.

There are just a few rights enforcement companies, and they generally keep their clients and methods secret.[35] However, by all accounts, they have sent hundreds of thousands, if not millions, of machine-generated complaints, largely targeting filesharing; most of the service providers we spoke to said these complaints comprised 75-95% of their § 512 notices. The complaints receive little or no human review before being sent,[36] which is unfortunate, because they are subject to inaccuracies both in

[34] Few service providers were willing to share their numbers publicly—indeed, educational institutions were uniformly reticent about this, a reflection of the intense scrutiny they have received. *See* Section III.B.1. However, several service providers stated that at their peak, apparently 2002-2004, many thousands of P2P filesharing notices were arriving per year. Most reported that the overall volume of P2P notices seemed to be falling, although the evidence for that is equivocal—at least two institutions reported that the volume of notices varied so significantly that it was difficult to say whether the volume was increasing or decreasing.

[35] *See, e.g.*, BayTSP client list describing only "strong partners and affiliates" (http://baytsp.com/about_clients.html, last visited Jan. 13, 2007); NetEnforcers client list, listing only "client industries" (http://netenforcers.com/clients.cfm, last visited Jan. 13, 2007).

[36] The RIAA has stated that an RIAA employee "manually reviews and verifies the information" in the notices that it sends out. Testimony of Mitch Bainwol, "Privacy and Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry", Sen. Committee on Governmental Affairs, Hearing, Sept. 30, 2003, available at Senate Committee on Homeland Security & Governmental Affairs website, http://hsgac.senate.gov/ , under "View all listings" under "Hearings and Nominations." The inaccuracies in notices reported elsewhere suggest this may not

identifying files and in identifying the users;[37] moreover, they cannot make any legal assessment of whether a file is actually infringing.

Enforcement companies generally identify files automatically with a basic search algorithm.[38] Such algorithms are subject to significant flaws. To the extent an algorithm is based on recognizing the names of titles or artists in filenames, it has the same flaws as any such technology. For instance, since titles themselves are not copyrighted, the same title may apply to multiple works, including public domain works. Titles of files may also indicate not that the file contains a copyrighted work, but that it contains, for instance, a noninfringing paper *about* that work.[39] Fingerprinting technology—another form of mechanized search—is also subject to significant flaws.[40]

Both the large commercial service providers and the educational institutions in our survey reported that they routinely received complaints about copyright infringement occurring at IP addresses that were "non-routable" or "impossible." The University of Indiana, Georgia Tech, the University of California, and its UC-Berkeley campus all received complaints about IP addresses that weren't assigned at the time they were alleged to host infringing files, couldn't host files, or were definitely not running filesharing software at the time in question. The commercial service provider ThePlanet also received

---

always be true. *See, e.g.*, Sonia Katyal, "The New Surveillance**,"** 54 *Case Western L.Rev*. 297, 345-346 (2004). Regardless of the RIAA's practices, there is no indication that other associations or private rights enforcement companies manually review and verify the complaints. *See also* Electronic Frontier Foundation, *Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands*, Sept. 26, 2003, at http://www.eff.org/IP/P2P/20030926_unsafe_harbors.pdf , for more examples.

[37] *See, e.g.*, *Foundation v. UPC Nederland*, Cause-List Number 1457/05 KG (Amsterdam Court of Appeal July 13, 2006), English translation available at http://www.ilrweb.com/viewILRPDF.asp?filename=foundation_upcnederland_060713AffirmanceonAppeal (finding the services do not reliably identify users or files).

[38] *See* Brad King, "Pirates Beware: We're Watching," *Wired*, Jan. 3, 2001, *available at* http://www.wired.com/news/technology/0,1282,40866,00.html, for a more detailed description of an early iteration of rights enforcement company methods.

[39] Such incidents are documented in the Chilling Effects database, at http://chillingeffects.org/ . Gigi Sohn described one incident, involving a "Harry Potter" book report, in testimony at "Piracy of Intellectual Property on Peer-to-Peer Networks" before the House Subcomm. on Courts, the Internet, and Intellectual Property, of the Comm. on the Judiciary, 107th Cong. Sept. 26, 2002 (available via http://commdocs.house.gov/committees/judiciary/).

[40] *See generally* Katyal, *supra* note 36. Copyright filtering software companies described in general terms how these technologies work (but did not discuss their failures) in *amicus curiae* briefs in the *Grokster* case. *See Brief of Amicus Curiae Bridgemar Services, Ltd. D/B/A Imesh.com in Support of Neither Party* (undated, from Jan. 2005); *Brief of Amici* [sic] *Curiae Snocap, Inc. in Support of Neither Party* (undated, from Jan. 2005); and *Brief Amici Curiae of Audible Magic Corporation, Digimarc Corporation and Gracenote in Support of Neither Party* (Jan. 24, 2005). All briefs available at http://www.eff.org/IP/P2P/MGM_v_Grokster/ .

complaints about IP addresses in ranges that didn't even belong to them. Hurricane Electric, another commercial service provider we interviewed, received numerous complaints about "dummy content" files, seeded by rights enforcement companies to pollute the filesharing networks. The service providers we interviewed also described receiving multiple notices targeting the same material in a short period of time.

These machine-generated complaints, compared to "spam" by more than one service provider, are virtually costless to the sender. Unlike spam, which can be filtered or deleted by individuals with relatively minimal hassle (albeit considerable annoyance), the "takedown spam" sent by rights enforcement companies imposes a significant cost on the service provider in terms of manually managing and processing each individual complaint.[41] The vast majority of these complaints appear to be generated in response to potentially infringing files accessed via Internet access services—services for which service providers have a straightforward § 512(a) safe harbor, with no notice and takedown provisions. Of the service providers we interviewed, virtually all those offering Internet access services nevertheless respond to the complaints, at a minimum forwarding them to subscribers and tracking the process. Additionally, educational institutions and small- to medium-sized service providers often cut off Internet access on a first complaint.

With intensive processing required, a sudden flood of possibly inaccurate "takedown spam" can incapacitate any service provider department or group that provides any personal review and attention to the notices. The University of Indiana, ThePlanet, and Hurricane Electric described significant problems contacting rights enforcement companies when they received a flood of problematic notices. Staff at Indiana said that phone calls, faxes, and emails about erroneous notices, or about counternotices, were ignored or went into a "black hole." Indiana ultimately contacted the original rightsholder's attorney about the problem and was able to stem the tide of "impossible" complaints that way. Hurricane Electric called rights enforcement companies multiple times before "finally" getting through to someone and working it out. The attorney at ThePlanet reported that finding a human being to talk to at the company made a difference for her, because she was able to cc: the individual she knew on every response pointing out errors—more than forty a day, in one instance—until the problem was resolved. Benny Ng, at Hurricane noted that the complaints are sent with generic return addresses (such as "no-reply-copyright@company-name.com") that make it difficult to get back in touch with the senders. He suggested that a better-streamlined process would benefit both senders and service providers.

[41] This is not to minimize the tremendous costs imposed by spam; just to distinguish them in kind.

Service providers invest significant resources in processing these machine-generated complaints—from validating their IP addresses, to contacting the targets, to processing any responses the targets offer. These costs are hidden from users and funders, though they are passed on to them. The copyright industry thus manages to externalize its copyright enforcement. For educational institutions, the costs are tucked into public and private education budgets. The significant expenses dedicated to licensing entertainment alternatives to file-sharing, creating monitoring technologies, enforcing the copyright industries' claims, and educating students on the industries' view of the law are difficult to account for separately, but total, no doubt, millions of dollars each year, a remarkable public investment in private copyright enforcement.[42] The cost is high, not just in terms of dollars and cents, but in terms of opportunities: With limited budgets and staff, time spent attending to masses of machine-generated complaints is time *not* spent dealing with other network abuse issues, such as spam and viruses. Every technical staff person we spoke with noted the trade-off, which had become particularly acute with the increase in spam over the months we conducted the interviews.[43]

Recommendations for further research:

- Research needs to be done with both commercial service providers and educational institutions to understand the total expenditures made on behalf of the copyright industries. Costs include, at least, the person-hours attributable to § 512 compliance, and the costs of informational material for users and subscribers. Educational institutions should include these costs in their publicly available budgets. Identifying the costs of dealing with other network problems, such as spam, viruses, and security would help put copyright policing costs in perspective.
- Research is also needed on the specific technologies and procedures used by the large notice-senders, particularly the rights enforcement companies.

B. The Institutional Contexts of Online Service Providers

1. Pressures, Costs, and Multiple Approaches in Colleges and Universities

Colleges and universities have been in the spotlight on copyright matters, and in the forefront of developing responses to the copyright industries' complaints. We spoke with ten information technology ("IT") administrators and attorneys at eight institutions about their experiences and the educational

[42] Graham Spanier, President of Pennsylvania State University and a promoter of proactive campus involvement in copyright enforcement, noted that copyright enforcement is "very costly for universities … it ends up being reflected in the cost of tuition that goes back to students." "Campus Downloading" (2006) video, available at http://campusdownloading.com/ .

[43] Spam, which has become more pervasive in part due to viruses and other network security breaches, has become an even more significant problem for network administrators in 2006. *See also* Brad Stone, "Spam Doubles, Finding New Ways to Deliver Itself," *N.Y. Times*, Dec. 6, 2006.

environment, generally: the University of California[44] ("UC" and "UC-Berkeley), Cornell, Georgetown University, Georgia Institute of Technology ("Georgia Tech"), Indiana University, Reed College, Stanford, and the University of Texas system ("UT"). What we learned suggests that despite substantial immunities and safe harbors from liability for copyright infringement—far more than are available to any other category of service provider—educational institutions are cautious and risk-averse with respect to copyright issues, an attitude that Harvard's Berkman Center for Internet and Society recently characterized as "unduly cautious."[45]

Educational institutions have access not just to the immunities and safe harbors previously discussed, but also to additional legal protections. Within copyright law alone, these include § 512(e), which protects nonprofit institutions of higher education from liability for their academic personnel's non-teaching-related infringements; §107 of the Copyright Act, which protects fair use and specifically offers educational uses as examples; and the "good faith" fair use defense, which provides that, should a nonprofit educational institution believe mistakenly but in good faith that the use was fair, courts must remit statutory damages entirely.[46]

We were initially curious to learn whether educational institutions take advantage of these numerous legal protections in responding to takedown notices. In particular, do educational institutions distinguish between providing Internet access to students, for which they have a § 512(a) safe harbor; hosting services for students, for which they have a § 512(c) contingent safe harbor; and non-teaching activities of academic staff, for which they have immunity under § 512(e)? The answer, so far as we can tell, is generally no, although this is an area where it would be fruitful to do a full-scale study of educational institutions.

---

[44] We spoke with two representatives of UC, one from the UC Office of the President, and one from UC-Berkeley.

[45] William McGeveran and William W. Fisher, "The Digital Learning Challenge: Obstacles to Educational Uses of Copyrighted Material in the Digital Age" (2006), pp. 86-87, available at http://cyber.law.harvard.edu/media/education/projectstatus and http://cyber.law.harvard.edu/home/uploads/823/BerkmanWhitePaper_08-10-2006.pdf.

[46] 17 U.S.C. § 504(c)(2). Educational institutions enjoy a variety of other exemptions, intended to protect educational uses such as research, commentary, and scholarship, in copyright, trademark, right of publicity, and other intellectual property laws. *See, e.g.*, the TEACH Act, 17 U.S.C. § 110(2) (copyright exemptions for distance education); Lanham Act, 15 U.S.C. § 1125(c)(3) (exemptions from trademark dilution liability for fair use, comparative advertising, parodies, criticism, news reporting, and noncommercial uses); Cal. Civil Code § 3344 (exemptions to right of publicity for news, public affairs, and other purposes). State educational institutions might also rely on the Eleventh Amendment's guarantee of sovereign immunity from federal claims.

Despite the abundance of education-specific legal safeguards and defenses against liability for secondary copyright infringement, the colleges and universities we surveyed described institutional responses that go far beyond commercial and nonprofit service provider responses, and far beyond their legal duties. Colleges and universities described a multi-pronged approach in responding to copyright complaints, including education, monitoring, and purchasing licensed entertainment for their students; as well as responses to cease and desist and takedown notices that include termination of network access and academic discipline.

While the desire of universities to be good citizens and responsibly educate their students offers a partial explanation for the disparity between their responses and their legal duties, there seems little question that intense industry pressure, along with media and political scrutiny, affect the debate and constrain educational institutions' actions. Representatives of UC, particularly in the limelight as the nation's leading public institution, said they took a "conservative" approach, and all the other schools we interviewed indicated similarly. Indeed, the scrutiny and pressure are so intense that few educational institutions are willing to go on record with numbers of complaints received or actions taken. In the academy, dedicated to openness and free exchange of information, this is a telling indictment of the extent to which educational institutions have borne the brunt of the copyright industry's battles.[47] Policies conceived in the face of such unremitting pressure might well be expected to be disproportionately harsh or severe in comparison with policies for other infractions, and this seems to be the case.

Our interviews also suggested that the complexity of the statutory framework contributed to educational institutions' overreactions, rendering it impractical to take different approaches to § 512(a) and § 512(c) notices. The staff we spoke with agreed that the complex structure set forth in § 512 was a source of confusion for many educators, particularly the distinctions between § 512(a) and § 512(c). Experts in the field such as Georgia Harper at UT, Tracy Mitrano at Cornell, and Karen Eft at UC reported that on listserves they often saw queries from confused IT administrators and other staff, particularly from smaller schools, and just as frequently saw misinformation passed on.

This is unsurprising: Large campuses typically have a general counsel's office, policy departments, and substantial resources to address IP complaints, but the work on the ground is most often handled by staff in IT departments. (See figure 1.) Stanford, Indiana, Cornell, and UC all emphasized the importance of strong connections between the IT department and departments with legal or policy expertise, but not every school has such open channels of communication. As Reed College pointed out, some small colleges have no legal department or in-house copyright expertise, and must rely on outside

[47] In light of this pressure, we are particularly grateful to those institutions and individuals who did participate in our study.

legal counsel. Georgia Harper, who conducts numerous copyright workshops for educational institutions through professional associations, reported that these educational workshops were very helpful; staff at UC agreed, and thought more resources were needed, particularly to support small institutions.

Takedown, Cutoff and Discipline.

Every educational institution we spoke with included punitive measures as part of its response to copyright complaints, including cutting off access to the Internet or to the institution's internal network, and referral to academic discipline processes. First-time complaints, which form the bulk of complaints for every institution we interviewed, are typically handled by the IT department. Individuals who are the subject of multiple complaints are "escalated" to the legal or campus administrative departments, although some institutions escalate even first-time complaints.

Universities have implemented stringent policies on copyright infringement, triggering strong procedures in response even to the automated machine-generated notices that have such significant flaws. Cornell and Indiana, for instance, disable Internet access as soon as they get a complaint (except where they find obvious technical errors), and require students to pass a quiz about copyright law before access is re-enabled. Stanford forwards the complaint with information about copyright law to the student and requires a response within 24 hours. No program claimed to universally review complaints on the merits, generally because there are too many of them to review each one individually, and because filesharing is presumed to be infringement.[48] In determining who the alleged infringer was, IT departments typically review the complaint to determine whether an IP address is "impossible" or not, and a significant number of complaints are bounced due to senders' errors in identifying the alleged infringer's address. If the complaint is not bounced for a technical reason, then the network access / discipline procedure is triggered.

According both to our interviews and to reviews of publicly available policies, most schools cut off student access to the campus network, the Internet, or both, at some point after receiving a filesharing complaint. Cutting off network access in response to an initial P2P complaint is an extraordinarily strong

[48] P2P filesharing of copyrighted material is regularly described as "illegal" in the U.S. media, and the U.S. Supreme Court in the *Grokster* case assumed that it is. 545 U.S. 913, 125 S.Ct. 2764, 2773. In Canada, however, a court has reached a contrary conclusion, holding that under Canadian law, downloading for personal use is legal. *BMG Canada Inc. v. John Doe*, 2004 FC 488, *aff'd* 2005 FCA 193 (2005), under appeal to the Canadian Supreme Court. This followed an administrative hearing that held that downloading appeared to be legal. Copyright Board of Canada, *Copyright Board's Private Copying 2003-2004 Decision*, Dec. 12, 2003, at pp.19-20, available at http://www.cb-cda.gc.ca/decisions/c12122003-b.pdf . The rulings are premised on Canadian law's broad exemption for personal copying. Canadian Copyright Act, s.80 ("[T]he act of reproducing all or any substantial part of … a sound recording … for the private use of the person who makes the copy does not constitute an infringement of the copyright in the musical work, the performer's performance or the sound recording.").

measure given the safe harbor provided by § 512(a), which is contingent only on section § 512(i)'s requirement that service providers "accommodate … and [] not interfere with standard technical measures" and adopt and reasonably implement a policy to terminate "repeat infringers."[49] Cutting off access based on the notice alone essentially conflates "repeat infringer" with "alleged infringer," a move that holds troubling implications for free expression and institutional due process. This practice is particularly troubling given the evidence of identification error as well as legal error in the machine-generated filesharing complaints. It is also far in excess of what is required by the § 512, which certainly does not require cutoff of Internet access for first-time infringers, much less first-time alleged infringers; educational institutions do so as a matter of institutional policy, not law. Given the pressures on educational institutions to deal with the "crisis" and police their students ("in loco parentis," indeed), it is likely that many institutions developed their policies in crisis-mode and with an eye to the external pressures. Some educational institutions that developed their policies in such a manner may not have had a cogent, campus-wide conversation about institutional values, needs, and proportionality. In developing or revising their copyright policies, we recommend that educational institutions examine the policies in light of their institutional values, as well as infrastructure management needs, political demands, and other policies regarding student or staff behavior., network use, intellectual property, and free expression Ideally, institutions should craft policies that are consistent, coherent, and proportionate.

While rights enforcement companies typically request the disabling of user accounts or Internet access in each of their notices, whether for first-time or repeat infringers, service providers are shielded from having to honor such extreme requests. Even the § 512(c) takedown procedure established for hosting services authorizes only the removal of the *infringing* content, not *all* content. Disabling access to the Internet—the predominant platform for speech and information in the 21st century—is an extraordinarily harsh remedy.

However, some schools have implemented processes that ameliorate the potential free expression problems. For instance, Cornell and Georgia Tech, among others, distinguish between Internet access and network access, cutting off *only* Internet access, and leaving access to campus educational resources. While this is not ideal, it is an important first step. Educational institutions harm their students and themselves unnecessarily by cutting off access to campus networked resources in response to a complaint

[49] Automatic termination of users repeatedly *alleged* to infringe is not required by § 512. In *Perfect 10, Inc. v. CCBill, LLC*, for instance, the court held that CCBill's failure to "keep a log" of § 512 notifications received did not harm its § 512 safe harbor eligibility. 340 F. Supp. 2d 1077 (C.D. Cal. 2004). In *Corbis Corp. v. Amazon.com, Inc.*, Amazon's failure to terminate zShops accounts that were repeatedly alleged to infringe did not cost it its § 512 safe harbor, because the activities were not, themselves, blatantly infringing, and Amazon could take into account fair use or other factors that might affect the evaluation of a copyright infringement claim. 351 F. Supp. 2d 1090, 1104-05 (W.D. Wash. 2004).

about filesharing on the Internet. However, even cutting off only Internet access can thwart academic purposes—university libraries are not the only source of information, and particularly for original research, Internet access is essential. Here, Stanford's policy of re-enabling Internet access with a commitment from the student to use it only for academic purposes provides a useful model. This policy properly recognizes that the Internet is a vital educational resource.

In addition to the network consequences, students accused of P2P filesharing often face academic discipline. Virtually all the policies we reviewed, as well as the descriptions from schools we interviewed, included academic discipline, up to and including expulsion. The policies often incorporate copyright infringement in the campus "terms of service," which include harsh penalties aimed at curtailing hacking, harassment, and other criminal activities. In addition to academic discipline, it is not uncommon to see language in the policies threatening legal action or criminal liability. The schools we interviewed indicated that low rates of "recidivism"—meaning repeated receipt of filesharing complaints—meant that the most extreme disciplinary measures were rarely triggered. Indiana reported that discipline was used primarily to stop repeat infringers, and after instituting a quiz for first-time infringers, referrals to the Dean of Students diminished significantly; only the occasional student who has a "philosophical problem" with the law, or who fails to take the quiz, ends up with the Dean of Students. In other words, once a user had been targeted and gone through the institution's process for first-time complaint targets, very few are targeted again. The schools we interviewed attributed this low "recidivism" to their extensive education and enforcement programs.

By all accounts, students file few "counternotices" in response to P2P filesharing complaints, although most of the institutions we spoke with included some information about counternotice options in their communications with students. The "Will Fair Use Survive?" report speculated that the low incidence of counternotices may in part be a result of the intimidating language included in § 512(g) for the counternotice, which states that the target agrees to accept jurisdiction of a U.S. federal court.[50] Our conversations suggested that schools may, perhaps inadvertently, compound the intimidation factor by including this frightening language in filesharing situations—language that is meaningless for people in the U.S. because anyone can be sued, whether or not he consents to it.[51] The § 512(g) language is not required in communications about P2P filesharing complaints sent regarding § 512(a) network access services. However, it is undoubtedly a best practice for institutions that choose to respond to § 512(a) notices to implement "counternotice" and dispute procedures equivalent to those available for § 512(c)

[50] Fair Use Report, *supra* note 1, at 54-55.

[51] The language is probably meaningful for people outside the U.S., who "consent" to jurisdiction in the U.S.

takedown notices. In both situations, potentially intimidating language, such as that specified in § 512(g), should be balanced with accurate information that explains the significance of the language.

However, it is equally important that—in contrast to the procedures required under § 512(c) and § 512(h)[52]—institutions *not* turn student information over to anyone who has simply filed a § 512(a) filesharing complaint. Sending student information to § 512(a) complainants is a voluntary action, not authorized by the DMCA, and it may raise issues under the Family Educational Rights and Privacy Act (FERPA).[53] Retention of data relating to complaints also poses a policy concern, as Reed College pointed out. While tracking "repeat infringers" may be necessary to "reasonably implement" repeat infringer policies under § 512(i), these data are educational records under FERPA and must be protected.

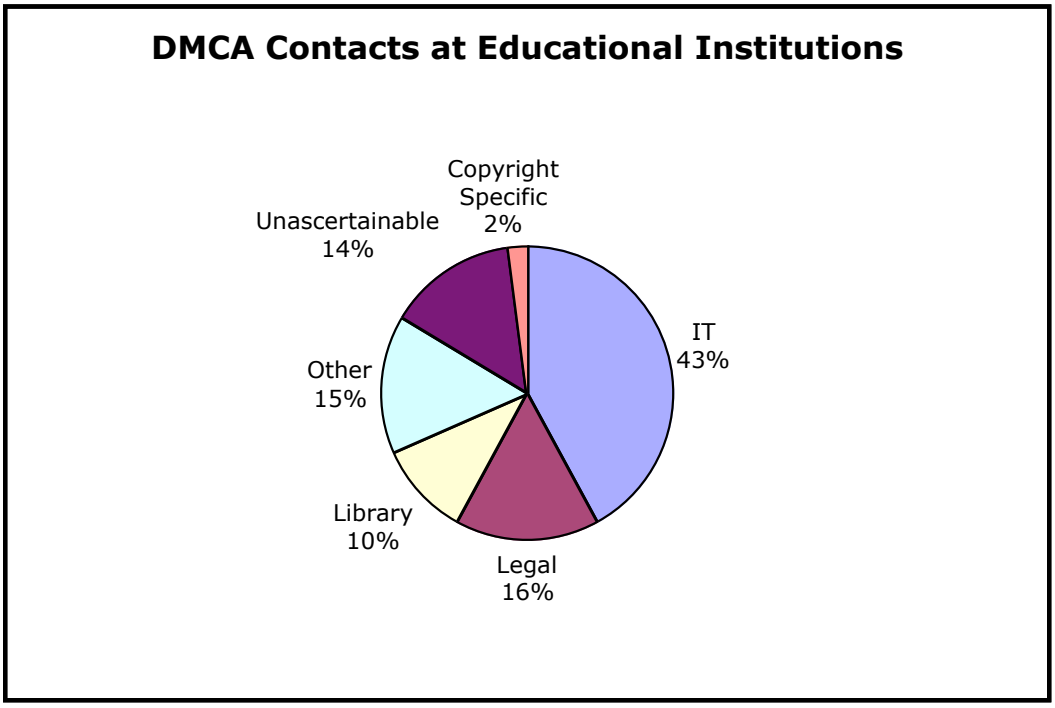

Figure 1. We reviewed the § 512 contacts that educational institutions had registered with the Copyright Office's § 512 contacts registry, randomly looking at every fifth institution for a total of 177 contacts. 43% of all contacts were in the IT office, and only 18% were in the legal department or focused on copyright. Ten percent of the contacts were in the library. (Research conducted by Nicholas Smallwood, November 2006.)

[52] Section 512(h) requires a subpoena. Section 512(c) doesn't authorize the release of information generally, but if the user files a counternotice, § 512(g) offers the safe harbor from liability to users *only* if service providers forward the notice (with the user's identifying information) to the original complainant.

[53] FERPA generally prohibits the release of information from a student's education record without written permission from the student or guardian, except under certain circumstances or with a judicial order or lawfully issued subpoena. 20 U.S.C. § 1232g; 34 CFR § 99.

Network Controls: Monitoring and Policing.

In addition to responding to complaints, many schools take a variety of proactive steps, including network monitoring and network "shaping"—that is, shaping the online environment by "throttling" or blocking particular kinds of traffic. Institutions might block or restrict traffic based on any number of factors: total traffic volume, data transfer protocols, network ports, file types (such as music or video files), filenames; or they might examine the data in the file. For instance, the program ICARUS, a system developed by the University of Florida, extensively monitors the network, including network port traffic and data transfer protocols. It blocks P2P traffic entirely, including private filesharing networks and server applications, and suspends access to the Internet if a data transfer that appears to be P2P is initiated.[54] The student must then agree to cease using P2P software in order to regain Internet access. Administrators at Berkeley, Stanford, Georgia Tech, and Texas said that educational institutions need to "throttle" individual users' bandwidth use in order to prioritize educational uses. Some institutions do so via overall usage quotas; others monitor or restrict access to ports and protocols used for entertainment or P2P filesharing.

These types of policing—in particular, monitoring of student or faculty Internet use—pose risks to free expression and privacy, risks that are particularly acute in the educational setting. The educational staffers we interviewed were well aware of these risks. All pointed to their educational mission as one of the factors in their policy development, and several (at Stanford, Cornell, and Berkeley) stated outright that it would be "anathema" or against academic freedom to monitor their users' speech—although some felt that the copyright industries were pressuring them to do so.

While network management is beyond the scope of this report, we recommend campuses approach the issue with sensitivity to free speech and academic freedom concerns. First, institutions should consider whether, and what forms, of network shaping and monitoring are necessary. Cornell, rather than engaging in network shaping, charges students for total network use. This does not restrict

---

[54] *See* Written Testimony of Norbert W. Dunkel and Rob Bird, before the House Subcomm. on Courts, the Internet, and Intellectual Property, of the Comm. on the Judiciary, 107th Cong. Sept. 22, 2005, available at http://www.judiciary.house.gov/media/pdfs/dunkel092205.pdf (noting that ICARUS blocks P2P as well as "residential 'Dark Nets,'" a term used to describe private filesharing networks) and Katie Dean, "Florida Dorms Lock Out P2P Users," *Wired News*, Oct. 3, 2003, at http://www.wired.com/news/digiwood/1,60613-1.html (describing blocks to server-based applications like networked games). *See also* http://uf.freeculture.org/wiki/ICARUS for an assortment of links to media coverage about the program. ICARUS is marketed as cGRID by a spin-off company, Red Lambda. See http://redlambda.com/ (last visited Dec. 20, 2006). Other similar programs include Audible Magic and Packeteer. *See* Electronic Frontier Foundation, (2005) "When Push Comes to Shove: A Hype-Free Guide to Evaluating Technical Solutions to Copyright Infringement on Campus Networks," available at http://www.eff.org/wp/univp2p.pdf for more detail about the technologies available to campuses for network shaping and monitoring.

individuals from whatever network activities they deem necessary, although it has the effect of reducing unauthorized filesharing. UC-Berkeley, similarly, restricts only total volume of bandwidth usage, and only in residential housing. Should it be necessary for network management to screen or shape content in more intrusive ways, then shaping based on transfer protocol or data port is preferable, from a free expression perspective, to screening based on filenames, filetypes, and file content. However, as staff at UC Berkeley and Georgia Tech both pointed out, particular types of technology (ports and protocols) may have legitimate educational purposes. Campuses should carefully review such technologies in light of institutional policies regarding record retention and academic freedom.

Second, monitoring and network-shaping should not trigger academic disciplinary processes, or termination of network access. Use of filesharing software alone should not be a basis for cut-off of Internet or network access. As the administrator of a computer science department at Georgia Tech put it, "any program that uses filesharing isn't implicitly a bad tool; research can be mistaken for illegal filesharing."[55] Thus, universities should carefully consider the potential chilling effects of network monitoring. Where it is deemed essential for network maintenance purposes, the least harmful application closely ties both monitoring and security notices to users actual network risks; does not retain such notices or logs; makes it clear to the user that the notice is part of an automated alert that does not trigger any academic or network consequences; and provides information that helps the user assess her own network information. Stanford's processes, for example, are responsive to these concerns. While Stanford monitors network use, it sends "security" notices to its users with information about detecting whether a machine has been compromised. The notices are solely informational, with no adverse consequences.

Third, any institution that purchases network monitoring technologies, or contracts out network management, should be aware of the significant free expression and privacy implications. As UC and Reed College pointed out, small colleges are particularly likely to "outsource" network management, and institutions of any size may invest in network management technologies. Educational institutions should carefully review *all* network monitoring and data retention settings, standards, and notices offered by contractors or set as defaults in network management software. These should be reviewed against institutional academic freedom and privacy guidelines.

---

[55] *See also MGM v. Grokster*, 9th Cir. 2003, Brief of Amici Curiae ACLU and libraries, available at http://eff.org/IP/P2P/MGM_v_Grokster/?f=20030926_aclu_amicus.txt, and *MGM v. Grokster*, Sup. Ct. 2004, Brief of Computer and Communications Industry Assn and Internet Archive opposing petition for certiorari, available at http://eff.org/IP/P2P/MGM_v_Grokster/20041109_Jaszi_finalbrief.pdf (both documenting numerous legal applications of filesharing software).

Copyright Education

Unsurprisingly, educating students about copyright is a popular approach on college and university campuses, and one encouraged by § 512. The limited § 512(e) safe harbor for educational staff's non-teaching material, for instance, is only available if the institution "provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright."[56] This accords with the mission of educational institutions, generally; Gary Schlickeiser at Reed College observed that educating students about copyright law fit with its philosophy of treating students like adults.

Schools were happy with their educational programs and felt they were successful. Indiana, for instance, attributed a decline in second-time complaints to its quiz, which requires 100% correct answers after reviewing copyright information before reinstatement to the network; Cornell has a similar program. Stanford, similarly, attributed a decline in "recidivism" to its stepped-up "education." Virtually all of the schools we interviewed include copyright information in new student orientations.

However, while educational programs are to be preferred over disciplinary approaches, their implementation poses some challenges for educational institutions. In our interviews, some staff questioned whether their effectiveness had peaked. Our interviews highlighted the cost of educational programs, a cost silently tucked away in the institutional budgets. Finally, the content and purposes of such programs, and the availability of accurate and unbiased information about copyright law and free expression, also raise concerns for institutions.

Some staff wondered whether campus copyright education had run its course. A few schools noted that the "teaching moment may have passed" with regard to copyright law and P2P filesharing. As staff at UC said, six years ago people came to universities who had never had Internet access, and that offered an educational opportunity for the university. Now, students arrive accustomed to filesharing in high school, and are surprised to find that it is under such a spotlight. Staff at Indiana observed that by the time students get to college now, their patterns, expectations, and opinions are already shaped—they've been downloading files at home for years. Tracy Mitrano at Cornell and Merri Beth Lavagnino at Indiana noted that efforts to engage students in the issue politically had not been very successful. While they had tried for several years to make it clear to students that information and copyright policy are political issues, the message didn't seem to go very far.

Our interviews also made it clear that these educational programs can be quite costly. The materials available from the copyright industries were, in the view of university staff that had reviewed

[56] 17 U.S.C. § 512(e)(1)(C).

them, not of high quality and biased to the point of unusability,[57] leaving educational institutions to develop their own. The cost of developing, producing, and distributing materials, however, was quite high—for Indiana, tens of thousands of dollars each year. UC noted that time, effort, and money spent on educating students about copyright was time, effort, and money *not* spent educating students about other network risks, such as the dangers of posting highly personal information in their MySpace profiles. Staff at Indiana and UC noted that public institutions' investments in copyright education effectively channel public funds into enforcing the copyright industries' business models. Meanwhile, smaller institutions, which often lack the resources to develop their own materials, must make do with biased industry models or with whatever materials are made available by the larger schools online.[58] Most staffers at both small and larger institutions were also not familiar with sources of consumer-oriented information, such as the clearinghouse of notices and copyright information provided by Chilling Effects.[59]

Even materials developed by the institutions themselves may not be wholly neutral, given the enforcement context in which they are developed. Several schools frankly acknowledged that their purpose, when they first encounter students regarding a takedown notice, is to "scare them" with stories of what could happen.[60] Programs placed great emphasis on the direst potential outcomes, including criminal penalties, large fines, and academic consequences. One staffer indicated to us that although the university knew it was unlikely that the students would get targeted again, or sued, they chose not to share the actual statistics with the students. This aspect of copyright education, at least, is aimed at altering

---

[57] An opinion shared rather widely. *See, e.g.*, Greg Sandoval, "RIAA copyright education contradictory, critics say," clnet News.com, Aug. 31, 2006, at http://news.com.com/2102-1027_3-6111118.html?tag=st.util.print. We reviewed the RIAA's most recent materials targeted at educational institutions, which they told us were being adopted by "many" universities (available at http://campusdownloading.com, *supra* note 42). As might be expected, the material characterizes filesharing as theft; focuses solely on reproduction and distribution of entertainment media; and does not present a well-rounded or balanced picture of copyright law, its limitations, and its defenses. Copyright materials from the Business Software Alliance take a similar approach. *See* "Define the Line" at http://www.definetheline.com/ (last visited Jan. 21, 2007).

[58] Most of the schools we interviewed made significant sets of materials available online, but not all such materials—the copyright quizzes, for instance. Institutions could also facilitate the widespread adoption of their own developed materials by using open content distribution licenses such as Creative Commons (see http://creativecommons.org).

[59] Chilling Effects is an online public clearinghouse of cease and desist letters, complaints about content, and § 512 takedown notices; as well as information about the applicable bodies of law (*see* http://chillingeffects.org/). The site is operated by Wendy Seltzer, the Electronic Frontier Foundation (EFF), and several law school clinics. (Disclosure: Laura Quilter is affiliated with the Samuelson Law, Technology & Public Policy Clinic, which maintains the § 512 section of Chilling Effects.)

[60] This sort of "scared straight" tactic is also taken by the recording industry in its recent video, "Campus Downloading," *supra* note 42.

specific behaviors, rather than the general liberal arts critical thinking purpose that universities foster elsewhere in their curriculum. The value of such education to the copyright industries and the universities is evident; to the students, though, its value as education is somewhat less apparent.

Licensed entertainment subscriptions

In partial response to industry and policymaker pressure, a number of major educational institutions have signed up, since 2001, with commercial for-profit digital music services. While cost figures are scarce,[61] institutions apparently pay in the tens of thousands of dollars annually to subscribe to services such as Napster 2.0, Rhapsody, Ruckus, Ctrax, MusicRebellion, RealNetworks, and iTunes. These arrangements were touted by some as educational institutions' response to students' filesharing. Scores, perhaps hundreds, of higher education institutions signed up during 2004-05.[62]

However, the services have not been without their critics, and many schools have refrained from such agreements. Some students and observers have critiqued the use of education dollars or student fees on licensed music services, characterizing the expenditures as subsidizing either student entertainment or the music industry.[63] Georgia Harper noted that it was not part of the University of Texas's educational

---

[61] Most campuses have kept the terms of their deals private. However, the rates typically are based on $2-$3 per student. *See* Brock Read, "More Colleges Strike Up Music-Sharing Deals, Despite Lukewarm Response in Dorms," *Chronicle of Higher Education*, Aug. 22, 2005, available at http://chronicle.com/free/2005/08/2005082201t.htm . Middlebury College reported that its Student Government Association had allocated $10,000 in 2005 for Napster 2.0, a revamped, licensed and authorized version of the original online music service, and predicted annual costs of $20,000; the total cost was believed to have been close to $40,000. "Music Service Draining Student Activities Fee," *MiddleburyCampus.com: The Student Weekly of Middlebury College*, Feb. 24, 2005, *available at* http://www.middleburycampus.com/media/paper446/news/2005/02/24/CenterSpread/Music.Service.Draining.Student.Activities.Fee-874910.shtml.

[62] Graham Spanier, "Peer to Peer Piracy on University Campuses: An Update," Testimony to the House Judiciary Committee, Oct. 5, 2004, available at http://president.psu.edu/testimony/articles/161.html (as of October, 2004, "at least 20 different universities have already signed agreements to legally deliver entertainment content to students"); Brock Read, "More colleges Strike Up Music-Sharing Deals, Despite Lukewarm Response in Dorms," *Chronicle of Higher Education*, Aug. 22, 2005, available at http://chronicle.com/free/2005/08/2005082201t.htm ("more than 50 campuses have signed deals… up from about 20 last fall"; 6% of colleges have or are getting them and 17% are considering doing so, including nearly half of the doctoral-granting research institutions). A Campus Computing Project 2005 survey found more than 120 educational institutions have purchased access to licensed music subscription services that would be free or subsidized for their students. Campus Computing Project, *The 2005 Campus Computing Survey Report*, available at http://www.campuscomputing.net/summaries/2005/ . Among the schools we spoke with, Stanford, UC-Berkeley, Indiana, Georgia Tech, and Cornell had subscribed to such services; Georgetown, the UT system, and Reed College had not.

[63] *See, e.g.*, Jefferson Graham, "More schools offer cheap music downloads for students," *USA Today*, Dec. 12, 2004 ("I didn't want tuition dollars being used for entertainment," University of Michigan associate provost James Hilton), available at http://www.usatoday.com/money/industries/technology/

mission to provide entertainment for its students. Research on the educational uses of these programs—access to music for classroom use, for instance—would shed light on other potential benefits, as Clifford Lynch, at the Coalition for Networked Information, pointed out.

The evidence is mixed as to whether these services succeed in diminishing unauthorized filesharing. The music services and copyright industries tout the success of the services at reducing P2P network traffic. However, while some of the subscribing schools attributed the decline in P2P-related complaints in part to these services, they also acknowledged problems with the services. The services are unpopular with students, with much less uptake among than anticipated, and press accounts suggest that schools without the services reported little or no demand from students for them.[64] Interviewees whose campuses had subscribed to services noted problems with them, such as incompatibility with Macintosh or Linux systems and restrictive digital rights management ("DRM"). The DRM employed by the services prevents music purchased from being moved easily from one machine to another, or deletes the music if a student lets her subscription lapse (a "tethered download").[65] These observations accord with analyst and industry observers, who have seen a general decline in use of the services, largely attributed to the DRM restrictions.[66] It appears that after rapid expansion into the educational markets in 2004-05, the growth of licensed entertainment arrangements may have slowed, as universities began dropping unpopular and little-used services.

Reductions in filesharing complaints (and a presumed reduction in filesharing) may also be attributable to two factors unrelated to the success or popularity of exclusive campus deals with music

---

2004-12-12-campus-music_x.htm; Benny Evangelista, "Back to School," *San Francisco Chronicle*, Aug. 15, 2005 (similar position expressed by UCLA); Derek Slater, "More Crummy Reporting on Penn State's Music Service," *A Copyfighter's Musings*, Nov. 6, 2003, available at http://blogs.law.harvard.edu/cmusings/2003/11/06/more-crummy-reporting-on-penn-states-music-service/ (noting that agreements put public dollars into subsidizing the services and their selection of artists).

[64] Our interviewees' experiences generally accorded with press accounts. *See e.g.*, Andrea L. Foster, "Colleges Split Over Effects of Court Ruling on File Sharing," *Chronicle of Higher Education*, July 8, 2005, available at http://chronicle.com/free/v51/i44/44a00101.htm , quoting Margaret L. O'Donnell, assistant general counsel at Catholic University of America that she has heard "mixed reports on whether students actually take advantage of the services." On Aug. 22, 2005, the *Chronicle* reported that 41% of American University students said their use of Ruckus had fallen considerably at the end of a three-month pilot period. The *Register* reported that University of Rochester students had essentially stopped purchasing songs, although 47% did stream music and 39% had purchased a "tethered download." http://www.theregister.com/2005/07/09/napster_rochester_survey/print.html

[65] *See* Ashlee Vance, "Penn Students Revolt Against Napster, DRM Invasion," *Register.com*, Nov. 7, 2003, at http://www.theregister.co.uk/2003/11/07/penn_state_students_revolt_against/ .

[66] *See, e.g.*, Nick Timiraos, "Free, Legal and Ignored," *Wall Street Journal*, July 6, 2006, p. B1, available at http://online.wsj.com/public/article/SB115214899486099107-vuoIhGUthiYcFwsQK0DjegSRPwQ_20070706.html?mod=blogs .

services. First, several of our interviewees suggested that the reduction in complaints was probably attributable to the availability of commercial alternatives that were more acceptable to consumers, most notably iTunes. Reed College and Stanford both expressed hope that the TV and movie industries would move quickly to disseminate files through iTunes and other relatively consumer-friendly formats, thus forestalling the problems the music industry had.

***Recommendations*:**

- In responding to takedown notices, educational institutions should ensure that all staff members handling copyright complaints have ready and frequent contact with a legal or policy department trained to evaluate free expression issues. The same standards apply to students and staff involved in disciplinary proceedings. Additionally, any disciplinary proceedings should be conducted with an awareness of the significant rates of error in machine-generated complaints, and an opportunity for free expression and fair use defenses to be heard. Disclosure of student identity information in response to P2P filesharing complaints—as opposed to authorized subpoenas—is not appropriate. Section 512(h) subpoenas, moreover, apply *only* to § 512(c) hosting activities—not to provision of Internet access services.[67] Eliminating network or Internet access in response to a first P2P filesharing complaint is not required by § 512, and its appropriateness should be reconsidered in light of the important expressive and academic values enabled by network and Internet access.
- Educational materials for students and staff about copyright law should include not just information about penalties and the industry perspective, but also information about fair use and free expression, the political and economic contexts of copyright law, and the § 512 takedown and counternotice process. It should also include current information about legislative initiatives and political organizations working on all sides of the issue as well as references to the Chilling Effects public clearinghouse of takedown notices, and neutral and consumer-oriented information resources such as the Fair Use Network.[68] Educational institutions that have developed significant, unbiased information resources for copyright education may wish to facilitate their adoption by including Creative Commons or open distribution licenses that permit others to adapt the materials.[69]
- Educational institutions should gather and make publicly available the total costs of copyright enforcement, including IT management, copyright education, licensed entertainment, monitoring, and filtering programs. This information should be put in

---

[67] *See Recording Industry Ass'n of America v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 543 U.S. 924; *In re Subpoena to University of North Carolina at Chapel Hill*, 367 F. Supp. 2d 945 (M.D.N.C. 2005); *In re: Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2005).

[68] Fair Use Network, http://fairusenetwork.org/ .

[69] Educational service providers have better access to information, developed by their relevant professional associations, than do commercial or nonprofit service providers. Among the resources are: EDUCAUSE, which includes a database of relevant news articles, presentations, and white papers (available at http://educause.edu/); the National Association of College and University Attorneys ("NACUA"); and reports such as the American Association of Universities, "Campus Copyright Rights and Responsibilities" guide (available at http://aaupnet.org/aboutup/issues/Campus_Copyright.pdf). *See* the Fair Use Network toolkits, forthcoming, for a further list of relevant resources.

context and compared with other costs and burdens. Due to the sensitivity of information regarding numbers of complaints received, a large-scale comprehensive research project should be developed that can offer anonymity to the institutions surveyed.

2. The Vulnerabilities and Value of Nonprofit Service Providers

Nonprofit service providers, and independent service providers serving nonprofits, artists, and activists,[70] support valuable political and artistic speech and have been targeted in a number of high-profile § 512 takedown incidents.[71] We included nine of these service providers in our survey: Electric Embers Cooperative, Infoshop News, Interactivist.net, Laughing Squid, Mayfirst.org, Online Policy Group ("OPG"), Open Flows, Riseup.net, and the WWW Artists' Coalition.

As might be expected from organizations dedicated to social change, political comment, and artistic expression, the staff members at the nine nonprofit service providers we interviewed were quite savvy about free expression concerns.[72] They also indicated knowledge of some of the key players in the field that might offer them expert and pro bono legal assistance. However, their resources are limited, and they may not have the information they need to establish policies and take advantage of available safe harbors for service providers. Although generally knowledgeable about free expression issues, they were often unclear about § 512. While several of the people we spoke with had received a cease and desist letter, few felt they fully understood the § 512 classifications. Many expressed confusion between trademark and copyright (as did small commercial service providers; see Section III.B.3).

Although the nonprofit service providers we spoke with are small in comparison with commercial service providers and many educational institutions, their size and services vary significantly. Nonprofit service providers most commonly offer web hosting, mailing lists, and colo services. Their web hosting and hosted mailing list archive services are covered by § 512(c), which affords them a safe harbor as long as they implement a notice and takedown process. Nonprofit colo services may be covered by both, or either, §§ 512(c) and 512(a), depending on the precise network configuration and services offered.

---

[70] The service providers we interviewed all serve nonprofits, political, or arts communities and have a social or political mission. Some are technically 26 U.S.C. § 501(c)(3) nonprofit corporations, and at least one was a 501(c)(4). Laughing Squid operates a webhosting business that underwrites its cultural and community work; we have referenced it in both this and the following section, but counted it only once.

[71] For instance, web host Thing.net and its upstream provider, Verio, received a takedown notice for one of Thing.net's subscribers' parody of the Dow Chemical website. Matthew Mirapaul, "Cyberspace Artists Paint Themselves Into a Corner," *New York Times*, Dec. 23, 2002 (available at http://www.nettime.org/Lists-Archives/nettime-l-0212/msg00113.html). *See also* text accompanying note 74, describing Diebold's targeting of OPG.

[72] Their general awareness did not necessarily translate to an anti-copyright perspective. Indeed, as software developers, many of our interviewees had a vested interest in the copyright and patent system.

The nonprofit service providers we interviewed are funded through donations, grants, and nonprofit-tiered fees for services. They have few resources to expend on legal counsel, and simply cannot pay significant money damages or litigation expenses, without full pro bono assistance.

Their shoestring budgets also suggest that, as with educational institutions, copyright policing presents a significant opportunity cost. Of the nine nonprofit service providers we spoke to, only the largest, Riseup and OPG, had invested significant time or human resources in developing guidelines for responding to § 512 complaints. Rather, small service providers typically waited for a particular need—such as responding to a takedown notice. While this triage may be a sensible approach to prioritizing work given an extremely limited set of resources, it has a few significant disadvantages.

First, the opportunity to deliberate about the potential consequences and significance to their mission may be truncated if response is left until a demand comes in. Second, the service provider's subscribers, who have a vested interest in understanding how they will be treated in a given situation, have little opportunity to assess that in advance. Third, without some essential framework for response developed in advance, a notice that comes in at the wrong time—when staff are unavailable to process it, or when another crisis is looming—could prevent the service provider from handling the takedown notice or other crises effectively. In the worst case, it could result in the service provider itself being taken offline for some period of time.

Nonprofit service providers rarely face the mass quantities of machine-generated complaints about P2P filesharing. Instead, the complaints they face are more likely to be human-generated, legally sophisticated rather than formulaic, and targeted at the core of the nonprofits' expressive missions. While as a group nonprofit service providers had received relatively few notices, the notices posed significant free expression issues.

Openflows, for example, had received a trademark notice claiming that its domain, "StealThisEmail.com," an homage to Abbie Hoffman's book *Steal This Book*, infringed a trademark on the term "stealth." Infoshop News had received a trademark cease and desist about a webpage entitled "The Black Bloc for Dummies,"[73] which provided basic information about an anarchist movement, and another cease and desist about an online project called the "anarchist cookbook"—a collection of recipes alleged to infringe a publisher's right to the title *The Anarchist Cookbook*. The OPG, similarly, was embroiled in a § 512 takedown dispute over notices from the Diebold Corporation, a major manufacturer of electronic voting machines, seeking removal of an archive of internal memos revealing flaws in its equipment. (See description below.)

[73] http://www.infoshop.org/blackbloc.html (last visited Jan. 20, 2007).

In these examples, the notices presented a variety of legal claims, and represented relatively serious attempts to enforce what the senders viewed as their legal rights. In each of these instances, the service providers properly resisted the pressures. However, they highlight the vulnerabilities of both nonprofit service providers and their clients. Any nonprofit service provider may work with organizations or artists that raise the hackles of rightsholders because of the nature of their work. Those users' speech may be targeted for viewpoint-specific or other content-based reasons; and IP laws put powerful tools in the hands of those criticized by activists. The expeditious takedown encouraged by § 512 offers senders a simple and quick way to remove speech they dislike. In fact, the takedown procedures are the equivalent, in First Amendment terms, of a prior restraint on speech—that is, they cause the censorship of material without any finding that it is unlawful.[74] The strong safeguards that the First Amendment provides outside of the copyright context are not incorporated in the § 512 procedures. And the speech safeguards—the § 512(g) counternotice provision and the § 512(f) allowance for suits to remedy "knowing and material misrepresentations"—are inadequate and rarely used.

Upstream Vulnerabilities

Nonprofit service providers, like small commercial service providers, are also uniquely vulnerable to threats to their upstream service providers. Very small service providers may be relatively far "downstream," purchasing their own access from resellers, or hosting sites on a server out of their home, using home broadband service. Even the largest of the nonprofit service providers we interviewed, Riseup and OPG, rely on a single Internet access provider, with few or no mirrors or duplicate sites at other locations.[75] These service providers are therefore particularly vulnerable to attacks on their upstream providers, and the further "downstream" they are, the more vulnerable they are to multiple attacks on the chain of upstream providers. A complainant can send multiple notices at the same time, or over a period of time, targeting the alleged infringer, its service provider, and each and every service provider up the line. By targeting the service provider's upstream providers, a single § 512 takedown complainant can effectively hold hostage a service provider's entire client base, which can be taken offline for the full 10-14 day counternotice period.

While this is an unacceptable risk for any business, it weighs particularly heavily on nonprofit service providers, whose primary mission is to facilitate free political or artistic expression. And these

---

[74] *See* Wendy Seltzer, "Free Speech Unmoored in Copyright's Safe Harbor" (2007 draft on file with author) (arguing that § 512's takedown provisions constitute a First Amendment "prior restraint" by proxy).

[75] See "Internet service provider," Wikipedia, Nov. 4, 2006, permanent link at http://en.wikipedia.org/w/index.php?title=Internet_service_provider&oldid=85742770 (explaining that ISPs connect to the Internet through a variety of services and "upstream" providers).

service providers' clients—individual activists, artists, and small nonprofits—are themselves particularly vulnerable, with fewer resources to back up, recover, or move their sites elsewhere. Every nonprofit service provider we spoke with noted that in evaluating legal notices, they had to consider the possible effect on their other clients. Moreover, their clients are themselves likely to be vulnerable, as small organizations or individuals, lacking backups and "mirror" sites.

The Diebold Company's campaign against OPG illustrates the danger. In 2003-04, Diebold was in the center of a controversy regarding the reliability and security of its voting machines. After a set of Diebold's internal memos was leaked in 2003, numerous websites began reposting the memos, which highlighted the machines' potential for inaccuracy, tampering, and other security breaches. Diebold claimed copyright in the internal memos and accordingly sent § 512(c) takedown notices to service providers that were hosting or linking to them. A notice was first sent to San Francisco's IndyMedia, a political news website. After IndyMedia refused to comply, Diebold sent a notice to Indymedia's Internet access provider, OPG. As OPG's Executive Director at that time, Will Doherty, told us, OPG similarly refused to comply with the takedown notice. Diebold then approached OPG's upstream provider, Hurricane Electric. Hurricane notified OPG that it might have to terminate OPG's Internet access if Indymedia's link to the email archive was not removed, but after consultation with intellectual property and civil liberties attorneys, agreed not to act while the issue was being litigated.[76] OPG, represented by the Electronic Frontier Foundation, then brought a § 512(f) action against Diebold, and the court found that Diebold had intentionally misrepresented its copyright claims, because the reposting of the memos for discussion was clearly a fair use.

The OPG story was a success in part because Doherty was well-versed in electronic civil rights issues and had close relations with the Electronic Frontier Foundation, enabling OPG to find pro bono representation quickly. However, most small nonprofit service providers are not so well situated. Their staff members are less knowledgeable about § 512 and substantive copyright law, and have less ready access to pro bono counsel with Internet and intellectual property expertise to respond to their upstream providers when they are targeted.

Jeffrey Diehl, for instance, operated a webzine named *10 Zen Monkeys*, hosting it on a small commercial webhost. After *10 Zen Monkeys* published an article about an Internet controversy, illustrated

[76] *Online Policy Group v. Diebold*, 337 F. Supp. 2d 1195, 1198 (N.D. Cal. 2004) (available with other case documents at http://onlinepolicy.org/action/legpolicy/opg_v_diebold/). The case was brought on behalf of OPG and two Swarthmore College students who originally received the notices. Diebold ultimately agreed to pay damages and legal fees of $125,000, after a Sept. 30, 2004, court decision that it was liable under § 512(f) for "materially misrepresenting" that fair use of the memos was copyright infringement.

with a single image captured from a news broadcast on the same subject, Diehl's service provider and the service provider's upstream provider both received takedown notices. Although the use was obviously fair use, and the sender of the notice did not, as it turned out, even own the copyright to the image, Diehl was forced to remove the material under protest. He elected to relocate to Laughing Squid, a San Francisco-based arts and nonprofit-oriented service provider that would be more protective of its users' speech. The complainant then sent takedown notices to Laughing Squid and its upstream service provider, Rackspace—forcing Diehl to, once again, take down content he believed noninfringing.[77] While Laughing Squid was, as he expected, supportive of him, and in fact helped him find legal counsel at EFF, the notice essentially held hostage, to a single alleged infringement, Laughing Squid's entire customer base—artists, nonprofits, and bloggers, completely unrelated to Jeffrey Diehl and *10 Zen Monkeys*. As Scott Beale at Laughing Squid put it,

> Especially for smaller hosts, it's very scary wording from an upstream provider: 'If you don't comply we'll pull your connection.' … Everybody with virtual hosting now, shared hosting, everyone is at risk. We have [many] domains on a server. It puts everybody at risk, just the same as any other security issue.

Even large institutions with ready access to legal counsel may be taken off-guard by an approach to an upstream provider. In August, 2006, for instance, Wikipedia was taken offline for 2 hours: Two of its upstream providers were involved in a dispute unrelated to Wikipedia, and shut down a block of IP addresses, among which were Wikipedia's servers.[78] While this particular dispute was apparently not related to copyright, it illustrates a critical point: the Internet access and hosting industry are complexly layered and interconnected. Interventions that target a service provider, rather than the precise content, are overbroad not just with respect to the alleged infringer, but potentially with respect to numerous other people and other material.

Recommendations:

- More support is needed for nonprofit service providers, including a "toolkit" that includes model policies, responses and notices to users, counternotices, and basic information about § 512. This information should also be disseminated to nonprofit technical networks and nonprofit legal networks.
- Section 512 should be revised to address the upstream targeting problem, or, alternatively, courts should restrict targeting upstream providers. In particular, as soon as a counternotice regarding an alleged infringement is filed, no additional

[77] Like OPG, Diehl ultimately found representation at the Electronic Frontier Foundation, which has filed a § 512(f) complaint against Michael Crook, the sender of the takedown notices. *Diehl v. Crook*, Complaint filed N.D. Cal. Nov. 1, 2006, *available at* http://www.eff.org/legal/cases/diehl_v_crook/crook_complaint.pdf .

[78] "Wikipedia shut down for several hours," clnet News.com, Aug. 18, 2006, at http://news.com.com/2061-10802_3-6107367.html .

notices to upstream providers should be permitted. The claimant's recourse, once a target has responded and disputed the claims, is in a court of law.

3. Competitive Disadvantages for Commercial Service Providers

Commercial service providers offer the broadest array of services of our three categories, including Internet access, hosting, searching, and a plethora of variants. Unlike nonprofit service providers and educational institutions, which serve defined constituencies with services relevant to their mission, commercial service providers' services are limited only by market demand. We interviewed staff at eight commercial service providers of varying size and service levels: Google, focusing on its search engine procedures; Blogger, a blog hosting company owned by Google; ThePlanet, a major Internet access provider, web host, and colo provider; Hurricane Electric, a major Internet backbone, web host and colo provider; Dreamhost, also a major web host and colo provider; Hiwaay Internet Services, a medium-sized Internet access provider, web host, and colo provider; Vidiac, a medium-sized video host; and Cornerhost.com, a small web host.

Notice and Takedown Practices

While § 512 offers little incentive for substantive review of complaints, most of the service providers we interviewed stressed the value of offering some review of complaints to protect their subscribers against unwarranted harassment. For Hiwaay, reviewing complaints for validity of the underlying claim and the location of the material is a way to screen out harassment and invalid complaints, to avoid "impacting [its] customer" with an unnecessary takedown. Google noted that defending fair use was in its own business interests, and so it was important to push back on substantively invalid complaints. Dreamhost does a "sanity check" on complaints; if someone is "clearly misusing § 512 as a 'cudgel' in order to silence a critic," it confers with legal counsel on the merits of the complaint. ThePlanet screens out notices that don't conform to § 512's specifications, and those making non-§ 512 claims.

The service providers that substantively review notices report a mixed bag, including copyright complaints they perceive as legitimate, complaints that present issues of fair use, bad faith claims, and complaints presenting confusing questions of jurisdiction, law, and copyright ownership. Hurricane Electric and Blogger also described multiple incidents of webmasters including a single graphic or some text, and removing it promptly on notice. The video service Vidiac sees a wide variety of user-submitted content, from simple home videos, to video footage of events, to elaborate homemade fan videos of TV shows, with popular songs as the soundtrack. Vidiac screens out clips of obvious copyrighted TV shows and videos, but sometimes staff "scratch their head" over the legality of fan-authored content and material from other countries.

Several service providers also reported significant numbers of complaints that raise complex issues of fact and law. Benny Ng at Hurricane Electric noted that "anyone can send in complaints to get their competitors off; I definitely have seen bad faith complaints … typically previous business partners with some bad break-up, and they argue about the license to the material." ThePlanet and Hurricane Electric both reported receiving multiple complaints about expired or invalid licenses for web software packages. George Poletes, formerly of ThePlanet, noted, "If you boil it down from a pure copyright notice, this is not [copyright] infringement; it's a contract or licensing issue." Another service provider said: "They are using [§ 512] as a tool to force people to buy a license."

Contract, licensing and ownership issues raise complex questions of contract analysis and extrinsic evidence, even before getting to the question of copyright infringement. All the service providers reported receiving notices for a wide variety of legal claims, including trademark and even defamation claims sent under § 512. While many of the service providers give trademark claims the same *de facto* treatment as copyright claims, Dreamhost screens out these non-copyright claims, and complained that its biggest problem with § 512 is its misuse by people filing § 512 notifications to deal with non-copyright issues; dealing with these notices "takes up the vast majority of [its] time."

However, while service providers spoke of the benefits to their users and themselves of reviewing the notices, they also expressed frustrations with the process. They felt the scales are tilted against their users, and that their hands are tied when it comes to the counternotice and putback procedure. They also took a conservative approach to the process, granting themselves little discretion in evaluating the notices. For instance, while all the service providers we interviewed tried to verify the notice senders and targeted content, they didn't necessarily review for fair use, or took a very conservative approach to it. Vidiac was aware of fair use, but applying it in evaluating materials was sometimes tricky, and felt they "couldn't afford" to risk being on the wrong side. Hurricane Electric will keep material online if the subscriber claims the right to the material and indemnifies them. Google expressly said it looks for fair use defenses, but earlier studies of notices suggest that even of the notices Google processes, perhaps a quarter have substantive flaws or target material with a copyright defense.[79] While the service providers we interviewed tried to screen out clearly erroneous claims or procedurally flawed claims, they also felt they had to process the notice if it was borderline.

[79] Examining the Chilling Effects database, Heins and Beckles found that 24% of all trademark and copyright notices in the database for 2004 presented weak substantive claims or reasonable defenses (Fair Use Report, *supra* note 1, at 36); see also Takedown Notices Study, *supra* note 13 (finding that 29% of the § 512 notices sent to Google presented substantive flaws in the underlying claim or a copyright defense).

Whatever their criteria for accepting or rejecting a notice, the service providers reported that once a notice was accepted, they removed the material, and replaced it only if a counternotice was filed, and only after its having been offline for 10-14 days, as specified by § 512. Most service providers received few counternotices, and several expressed dissatisfaction with the counternotice procedure, describing it as unfair or unreasonable. One service provider described the counternotice procedure as "a joke." George Poletes noted that it is complex and poorly understood, and even if counternotices are filed, content has to be kept offline for the statutorily mandated 10-14 days. Andy Dorman of Hiwaay said:

> [T]he ten day period is ridiculous, because once you've established that the customer, the alleged infringer, does not believe they're infringing and they think they have a right to have it up and are willing to defend that right,… then what's the deal with the ten days? The alleged infringer still has to have material not available to the Internet for the ten days. … To me it's impacting my customer. I remember one particular case a few years ago where the issue involved something essential to their business process. We were forced to shut down their business for ten days, even though we didn't want to … and it was very obvious that they felt in the right to use the material.

By all accounts, counternotices are relatively few. People may not know about or understand the counternotice procedure, or may feel intimidated by the language required in counternotices, particularly the required statement of consent to be sued. Regardless of the merits of the situation, people may feel vulnerable to successive complaints to upstream providers, or repeated complaints to the same provider. People may simply not know how to assess the merits of a claim or their own defense.

Subscriber and User Information

One significant concern regarding commercial service provider procedures and policies is the lack of consumer access to information about them. While most service providers give users some basic information about § 512, few include detailed information about their procedures. For example, none of the service providers in either our interview set or our larger review of publicly available policies clearly explained in their policies what "takedown" meant, and whether it included deleting files or simply disabling public access to them. Many service providers linked their copyright policy information to their terms of use or terms of service, but without a resource to compare these policies across different service providers, there is little opportunity for user understanding, choice, and competition among services. Even among the small number of service providers we interviewed, practices regarding notification to their consumers varied significantly.

However, we did identify some practices that better served subscribers. Most service providers forwarded the complaint, along with relevant information from or a link to the service provider's terms of service. ThePlanet forwards notices that don't comply with § 512 to its customers, even as it contacts the sender to get a compliant notice. This practice permits customers to know that a potential dispute exists, deal with any issues that may be confusing, and prepare for a compliant notice. Several of the service

providers we spoke with, including Blogger and Dreamhost, provide information about Chilling Effects to their users. ThePlanet and Blogger both submit their notices to Chilling Effects, which they feel offers greater accountability, transparency, and user satisfaction, as well as facilitating assessment of their process.

Section 512(a) (Internet Access) Services

Of the service providers we interviewed, three offered both significant Internet access services (covered by § 512(a)) and hosting services (covered by the takedown procedure of § 512(c))—Hiwaay, Hurricane Electric, and ThePlanet. As with educational institutions, each of these reported receiving significant numbers of machine-generated complaints. ThePlanet estimated 75% of its IP complaints were related to filesharing; Hiwaay estimated 90%. Hurricane Electric tracked these complaints together with mass numbers of phishing scams and other complaints, but reported perhaps a third of its total were filesharing-related. As with educational institutions, service providers that offer both Internet access and hosting services effectively opt out of the more protective § 512(a) safe harbor, electing to enforce § 512(c)-like processes for both kinds of complaint: notifying users of the complaint, and disabling Internet access in lieu of removing access to a particular file. Like educational institutions, commercial service providers try to contact the senders to deal with floods of mistaken notices.

Section 512(d) (Information Location Tools) Services

The § 512(d) process for search engines presents a different, but equally troubling, issue. The single provider of search services that we interviewed, Google, reported that § 512(d) notices are increasing. Our interview with Google confirmed earlier research[80] suggesting that these notices are most often intended to affect the sender's own, and its competitors', search rank. Such notices generally target alleged infringement of product descriptions, press releases, and other factual content. They rarely target infringing copies of movies or music. This use of § 512(d) is certainly not what Congress intended. Removal from a search engine does not remove content from the Internet, but insofar as search is the only way to access information on the Internet unless one already knows a site's web address, removal of links is a significant hindrance to disseminating or accessing information.

While it may often be difficult for § 512(d) search providers to find contact information for those whose links or content is removed, Google attempts to remedy this difficulty and to notify search engine targets when possible. Google's § 512 online complaint form requests contact information, which Google uses to notify search engine targets if it can. Search engine targets also sometimes learn of their takedown by finding the notice in Chilling Effects. Google does accept counternotices, returning links to the

[80] Takedown Notices Study, *supra* note 13.

database where possible. Although neither notice nor counternotice/ putback are required by the statute, this is a best practice.

Access to Information and Counsel

Our interviews suggested that access to legal counsel with appropriate expertise is important for a service provider to feel comfortable challenging notices or even making substantive assessments. Dreamhost noted that "nuisance lawsuits are a real problem in this industry," but felt comfortable dealing with them because the company has skilled legal counsel. Hurricane Electric can turn to its attorney for any grey areas or issues that aren't "cookie-cutter." Google, Blogger, and ThePlanet have in-house legal counsel, and all felt comfortable parsing the legal issues and factual situations presented by § 512 takedown notices and other complaints. Hiwaay had gotten advice from a law librarian, expert in copyright matters, and was happy with its lawyer; it also felt comfortable reviewing notices for substantive compliance with § 512 and copyright law. By contrast, Cornerhost and Vidiac, which had not had the full benefit of experienced legal counsel, expressed uncertainty about how to apply § 512. Scott Beale, at Laughing Squid, described the situation faced by many small service providers:

> That's what happens … a small host doesn't have a legal staff and thinks they would have to hire a lawyer, so why not just get the customer to take it down because they're only paying us $10 a month. So economically it's not worth it for most hosts. We're a reasonably priced host, not even a $5 host—those guys [the discount host resellers] are going to totally roll.

The information access problems are not trivial. Finding counsel trained in the intricacies both of § 512's statutory framework and the technologies that startup companies employ can be "difficult," according to Vidiac, and finding affordable counsel with relevant expertise even more difficult. Cornerhost, the smallest service provider in our sample, felt daunted by the fees charged by legal counsel. Commercial service providers generally have no recourse to pro bono counsel. Trade associations, so helpful in the educational world, did not offer much for the commercial service providers we interviewed. Indeed, while there were many trade associations for service providers in the 1990s, the "dot-bust" and subsequent shifts in the service provider industry wiped many of them out. Those we surveyed had little in the way of best practices, guidelines, or other information to support their constituents.[81]

[81] Review of websites of 25 trade associations and service provider organizations found many state-based organizations no longer operational. Of the continuing organizations, only a few had any information about the DMCA, and only one, the Internet Service Providers Association (ISPA) had informational resources to help their members understand the DMCA. Research conducted by Kate Kaufmann in March 2006.

High Priorities and High Costs

The costs of the process weigh most heavily on the small and medium-sized service providers we interviewed. Hiwaay spoke of being beset by "razor-thin margins", and Vidiac described spending as much as 10% of its budget on copyright policing.[82] The potential, however slim, for ruinously high damages that could wipe out their business meant that copyright management is a top priority for the service providers we interviewed. These costs could be mitigated with venture capital ("VC"), according to Adam Bruce with Vidiac, but VC comes with a high cost of its own: the loss of autonomy and maybe even the loss of the business.

> One of the big reasons that we would have taken VC would have been purely to have had some deep pockets to help us out if we had ever ended up in a courtroom. [But] no one ever talks about the downside of taking VC…[they] can pull the rug out. … What's the VC's out plan—to sell you to Google or whatever? I'm happy just having a small mom and pop company. … We made the choice to not be Starbucks but to be the local coffee store. … As soon as we take that [VC] investment we will lose the lifestyle that we all wanted when we started this company.

Bruce worried that the picture was grim for such small independent businesses, and that in an industry driven by high-stakes copyright claims, the VC solution would clear the field of independent mom-and-pop operations.

Section 512's "expeditious" removal requirement for a safe harbor ensures that copyright issues move to the top of the queue—ahead of combating spam, viruses, or network security issues. Like educational and other nonprofit service providers, commercial service providers told us that they are "deluged" and "flooded" by spam, phishing, viruses, and security threats. Copyright enforcement thus poses a significant opportunity cost for these service providers that must be weighed against these other tasks. While they were resigned to these investments, service providers reasonably questioned why they should be involved at all. As Benny Ng at Hurricane Electric pointed out, electric companies also supply users with tools to run computers and networks, but they are not forced to handle copyright complaints.

Small commercial service providers, such as Cornerhost and Jeffrey Diehl's provider (described above), also face the same vulnerabilities to upstream providers faced by small nonprofit service providers. They may lack backup and mirror sites, and may be relatively far down in a hosting chain, with multiple upstream providers as potential takedown targets. The ease and simplicity of reselling plans permit almost anyone to become a webhost, whether they have access to a lawyer or not. This ease and flexibility drives a competitive and thriving market of webhosts offering different levels of support,

[82] These complaints from smaller service providers mirror similar complaints cited in a recent paper, which noted that "owners of smaller ISPs have complained that they are unable to afford to keep up with the number of requests and are at risk of becoming overwhelmed that they may actually be driven out of business." Alice Kao, "*RIAA v. Verizon*: Applying the Subpoena Provision of the DMCA," 19 *Berkeley Tech. L.J.* 405, 418 (2004).

service, and software packages. But understanding § 512's tiered services categories and requirements, the substantive underlying rules of copyright, distinctions between copyright and other forms of intellectual property, and distinctions between intellectual property and content protected by the § 230 immunity, are tasks beyond many attorneys, much less small webhost entrepreneurs.

Recommendations:

- Commercial service providers should include information about counternotice procedures, consumer education resources, and databases such as Chilling Effects in communications to subscribers about takedown notices. *See* our forthcoming toolkits for samples. They can facilitate consumer satisfaction by disclosing their procedures, including whether substantive review is done, and how "takedown" and "putback" are implemented.
- Small commercial service providers and their subscribers, as well as rightsholders, would profit from development of a toolkit of form notices and responses, including basic information about § 512. Such a toolkit could be distributed via bar associations, trade associations, and the Internet. In particular, small commercial service providers need to understand that (a) in order to access the § 512 safe harbor, they must register an agent with the U.S. Copyright Office, and develop and reasonably implement a policy for terminating repeat infringers; and (b) § 512 does not require removal; it merely encourages removal of material that is hosted within the meaning of § 512(c), or linked to within the meaning of 512(d), by offering a safe harbor from *potential* liability for that material.
- Econometric research on the effects of copyright enforcement on small and mid-sized businesses is indicated. In particular, does the § 512scheme act as a market-entry barrier, or disproportionately affect the competitiveness of small- and mid-sized independent businesses?

IV. CONCLUSION: HOW WELL IS THE TAKEDOWN PROCESS WORKING?

Our conversations with service providers suggest that while the immunity offered by § 230 and the safe harbor regulatory scheme of § 512 are useful, § 512, in particular, is not working very well, and solves few of the problems it was intended to solve.

Complaints from individual rightsholders are a small fraction of total complaints. By contrast, machine-generated complaints about P2P filesharing services continue to arrive in significant numbers, especially for large service providers and educational institutions. These complaints are burdensome to service providers, and the processes and technologies they adopt to handle mass quantities of notices threaten to chill free expression. The merits of individual filesharing complaints are almost entirely disregarded, a cost perhaps not regarded as significant by notice senders or even service providers. However, it is not an insignificant cost, and it is not one that was approved by Congress. Removal of access to the Internet is removal of access to the premier information resource and speech platform of our

day, as well as an essential public utility for business, education, and communications. Significant procedural safeguards should be implemented to protect users from bearing this cost unnecessarily or wrongfully.

The process also causes collateral damage to targets of non-filesharing complaints, who are forced to try to defend their rights in a system set up by service providers to process mass volumes of filesharing complaints, rather than in a system set up to protect the users as customers or respect their free expression or academic freedom interests. Simple efficiencies of process encourage small and medium-sized service providers, and service providers that offer mixed services—Internet access as well as hosting—to implement a single, one-size-fits-all "takedown" process even for complaints for which they are granted the straightforward 512(a) safe harbor. Educational service providers similarly find it simpler to implement a one-size-fits-all procedure, and are under substantial political pressure to do so.

The filtering and monitoring of user expression, in response to P2P filesharing, is a cost that has not even been calculated, but it threatens to undermine the academic and intellectual missions of our educational institutions.

The opportunity costs imposed by the system must also be counted. The spam economics of mass numbers of machine-generated filesharing complaints undermine service providers' ability to fight actual spam, a cost every Internet user is paying. The money our educational institutions are pouring into "copyright compliance," at the behest of the rightsholder industry and elected officials, costs both their students and the taxpaying public.

While small service providers appear to fly under the radar of the "takedown spam," the overall copyright environment threatens their competitiveness, and forces them into a catch-22 of risking ruinous litigation costs and copyright damages, or removing user content with little procedural protection. Small providers should not be forced to choose between restricting their users' speech on the one hand, and operating a successful business on the other. Small service providers' lack of access to informed counsel and model policies and practices can be addressed, which will help to minimize their confusion and protect them from unnecessary liability, while protecting free expression and being responsive to rightsholders. More study is needed, as well, to understand how copyright costs affect small and independent businesses.

While the costs are high, and in some cases not yet calculated, the benefits are not equivalent. Certainly, the copyright industries have not gotten what they wanted from § 512—an effective way to address distribution of copyrighted material over the Internet, distribution that has largely moved to the P2P filesharing networks. Ordinary rightsholders, who might prefer expeditious removal for defamatory

or private communications, are stymied by § 230's broad protections; those who can fit their complaints into § 512 do so, with none of the free expression reviews ordinarily applied to defamation or privacy complaints.

In crafting § 512(c), Congress attempted to balance the risk of massive distribution of commercially copyrighted content against the risks of mistaken identity, wrongful claims, and other errors. While the law does favor rightsholders with "expeditious" takedown, it injects some balance with procedures for putting back speech, and remedies for mistaken targets. To the extent that § 512(c) is, admittedly, unbalanced in favor of rightsholders, this was arguably justified by the threat of massive copyright infringement on hosted websites.

However, the sorts of infringing activities that are, for the most part, being addressed under § 512(c) do not justify the lopsided remedy that it creates. Not all copyright matters are appropriate for the simple and, in practice, largely unreviewed processing of § 512. Many "copyright infringement" issues, moreover, fall well outside the paradigmatic situation, but nevertheless provide complainants with the same "expeditious" takedown, with no judicial review and little recourse for targeted users. Service providers reported problems that don't fit well within § 512, and pose real difficulties for any substantive analysis, raising legal issues beyond copyright infringement. The use of copyright law to enforce rapid takedown in ownership and contract disputes, as well as the plethora of other non-copyright uses such as privacy, was almost certainly unintended by Congress.

Unfortunately, those remedies that offer some balance on the free expression side have turned out to be narrow, cumbersome, and little used. Legislative and judicial reforms have been proposed elsewhere,[83] and many of these reforms would be very helpful. In particular, removing the *ex ante* takedown procedure, while eliminating the benefit of rapid takedown, would reset the default in copyright infringement to something closer to the standard enjoyed for other speech issues. Strengthening the user protection provisions of § 512(f)-(g) would also be a significant reform. Finally, limiting the scope of § 512 to the less complicated claims of copyright infringement—reproduction and distribution of an entire work—would significantly help to avoid the problems posed by encouraging "expeditious" and unreviewed takedown of disputed material raising complex questions of fact and law, while still addressing the majority of concerns of copyright holders.

[83] *See, e.g.*, Takedown Notices Study, *supra* note 13, 22 *Santa Clara Comp. & High Tech L.J.* 652, 688-92 (summarizing various legislative reform proposals, and offering additional proposals).

Even without legislative reform, however, individual institutions and service providers can adopt some of the best practices we have highlighted in this report, to protect their own legal and business interests, while responsibly addressing their subscribers' and copyright holder rights. Following this report, we will release "toolkits" of the best practices we observed, along with sample policies, notices, and resource lists. Educational institutions and other service providers, as well as their subscribers and third party copyright holders, will benefit from service providers making their policies and procedures transparent; following the law closely and not extending it in ways that unfairly penalize users and subscribers; and helping users, subscribers and copyright holders better educate themselves.

Appendix
List and Affiliations of People Interviewed

- Andrea Almeida, General Counsel, ThePlanet.
- Jonathan Bailey, Consultant
- Scott Beale, Founder, Laughing Squid
- Adam Bruce, President and Co-Founder, Vidiac
- DMCA Compliance Technician, Blogger
- Jacqueline Craig, Director of Policy, University of California Office of the President
- Jeff Campbell, Communications Director, DreamHost
- Jeffrey Diehl, Webmaster, 10 Zen Monkeys
- Will Doherty, Founder and former Executive Director, Online Policy Group
- Andy Dorman, Network Manager, Hiwaay Internet Services
- Brent Emerson, Worker-Owner/CFO, Electric Embers Cooperative
- Karen Eft, IT Policy Manager, University of California, Berkeley
- Daniel Kahn Gillmor, Technology Advisor; Interactivist.net; Openflows; May First/People Link
- Eric Goldhagen, Collective Member, Openflows; WWW Artists' Coalition
- DMCA Compliance Coordinator, Google Inc.
- Georgia Harper, Scholarly Communications Advisor, University of Texas
- Ardoth Hassler, Associate Vice President for University Information Services, Georgetown University
- Merri Beth Lavagnino, Chief Information Technology Policy Officer, Indiana University
- Mark Libkuman, Interactivist.net; Advocacy Developers
- Clifford Lynch, Director, Coalition for Networked Information
- Jamie McClelland, Co-Director, May First/People Link
- Tracy Mitrano, Director of IT Policy, Cornell University
- Chuck Munson, Collective Member, Infoshop News
- Benny Ng, Director of Marketing, Hurricane Electric
- George Poletes, former General Counsel, ThePlanet
- Gary Schlickeiser, Director, Technology Infrastructure Services, Reed College
- Lauren Schoenthaler, Senior University Counsel, Stanford University
- Devin Theriot-Orr, Counsel, Riseup.net
- Michal Wallace, Founder & Proprietor, Cornerhost
- Keith Watson, Systems Support Specialist, Georgia Institute of Technology
- Robert Whitt, DMCA Compliance Technician, Indiana University