DIGITAL RIGHTS MANAGEMENT

Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345 (2004)

In the traditional economics of deterrence, raising the sanction is a simple matter of increasing the legislated or judicially imposed penalty for a particular offense. With digital copyright infringement, things are a bit different. Copyright law already includes substantial supracompensatory sanctions in both civil and criminal law. Any copyright infringer—even one who acts innocently—can be held liable for statutory damages in lieu of actual damages at the plaintiff's sole election. Those statutory damages normally range from $750 to $30,000 per work copied at the factfinder's discretion. The court has the discretion to lower the amount to $200 per work for innocent infringers and to raise it to $150,000 per work for willful infringers.

These damage amounts reflect recent increases by Congress and dealing with large-scale infringement over p2p networks offers no reason to raise these damage amounts further. Because the most likely targets of a civil lawsuit in the p2p context are the "keystone" uploaders, who often have several hundred different songs on their computer, existing statutory damages can easily run into the tens of millions of dollars per individual. This is likely to be an ample deterrent for the individuals who most often hold keystone positions on p2p networks. Indeed, it's arguably far too high already to do much good. College students do not have tens of millions of dollars to lose, and conversely those who do have that kind of money do not tend to spend their time trading music files on p2p networks. But civil suits with potentially enormous statutory damages may deter uploading because college students (or more likely the parents of teenagers) will fear bankruptcy. Indeed, the RIAA may have been able to eliminate some file sharing merely by threatening to sue some p2p users, and more when it actually filed a few hundred suits. But if so, existing statutory damages will be more than sufficient to achieve that deterrence.

College students are perhaps even more likely to be deterred by the prospect of going to jail. Copyright law includes rather substantial criminal penalties, including prison time, for willful copyright infringement. Under the 1976 Act as originally enacted, copyright infringement was a criminal offense only if the defendant acted willfully and for purposes of commercial advantage or financial gain. Congress expanded criminal penalties rather substantially in the No Electronic Theft Act of 1997, however. The law now provides that willful infringers are criminally liable either if they act for financial gain, a term now defined to include the expectation that others will reciprocate by providing copies of other works, or if they reproduce or distribute works worth more than $1000 retail value in any six-month period. This latter provision is likely to reach most keystone uploaders on a p2p network, so long as they act willfully. As with civil penalties, it doesn't seem that the existing criminal penalties need to be augmented.

The reason the already substantial civil and criminal penalties have only begun to have a deterrent effect is that for the most part they have not yet seriously been pursued against alleged direct infringers on p2p networks. As Stuart Green put it, "if the state is serious about enforcing intellectual property laws, it cannot simply expect to impose harsh criminal sanctions, stand back, and wait for compliance." Only in September 2003 did sound recording copyright owners begin to pursue civil infringement suits against individual p2p uploaders. In this subpart, therefore, we consider whether a small number of high-profile civil suits against, or criminal prosecutions of, file traders could substantially reduce widespread online infringement.

The prospect of spending several years in prison or owing millions of dollars in damages is likely to serve as a substantial deterrent to digital copyright infringement by end users. The more difficult empirical question is how many people the government must prosecute, or copyright owners must sue, in order to create a credible deterrent to illegal activity. We think the number of cases may actually be

relatively small, and indeed the empirical evidence to date offers some support for that view. There are several reasons for this.

First, while the number of users of p2p networks such as Morpheus and (before the injunction) Napster is massive, the overwhelming majority of those users engage only in downloading. Indeed, by one estimate, 3% of the users of a p2p network upload 97% of the files on that network. These high-volume uploaders also seem to be the users most likely engaged in uploading illegal content, rather than providing access to legal files. They are easy to identify, both because they will repeatedly appear in content searches and because many run so-called "supernodes" that facilitate fast downloads. Reducing infringement on a p2p network doesn't require targeting downloaders, who may in any event have a legitimate reason for downloading some copyrighted content. It just requires targeting uploaders, and in particular the much smaller number of high-volume uploaders. If there are 3 million users logged onto Morpheus at any one time, perhaps 90,000 of them are high-volume uploaders.

Second, many high-volume uploaders are likely to be easily deterred. They are not paid for uploading files and indeed contribute substantial bandwidth and perhaps time on a voluntary basis in order to make files available to others. They are persuaded to do so in part because the p2p community inculcates a "norm" of sharing, though the fact that most people do not upload indicates that that norm is not a particularly strong one in the community at large. But it is possible to participate in the p2p system without uploading, and the threat of bankrupting civil suits or criminal prosecution may induce a substantial number of high-volume uploaders to become passive downloaders instead. This is particularly true with criminal prosecution because the sort of individuals who tend to be high-volume uploaders seem likely to fear jail more than the average criminal. Willful digital copyright infringement over p2p networks is a crime apparently committed in significantly higher proportion than many other crimes by college students: young, educated members of society with a bright future ahead of them. The prospect of going to prison—and the attendant consequences, such as being kicked out of school—may worry a college student more than it would those inclined to commit other kinds of crime, such as burglary. The college student may feel she has more to lose and less to gain from this particular criminal activity than does the burglar. And since she has no strong stake in being an uploader, she may simply decide to quit. While it is only a guess, it might be reasonable to say that a five percent chance of criminal prosecution and punishment for uploading files in any given year would be enough to deter the majority of uploaders. Similarly, the parents of teenagers—another significant group of uploaders—may fear the prospect of a bankrupting multimillion dollar damage award more than other potential defendants in other types of unlawful activity, such that the same five percent chance of owing such an award might be enough to deter most uploaders. This means that if we must deter 90,000 people, we need only successfully prosecute or sue, and impose severe sanctions on, 4500. These numbers are only the roughest of estimates, but they suggest that the numbers involved may be more realistic than would otherwise seem the case from the large absolute numbers of people who participate in p2p networks.

Even this number might overstate the number of suits or prosecutions needed to significantly reduce widespread p2p infringement. While it is possible that deterrence occurs only after a threshold—that is, that no one will be deterred by the threat of legal action until the chance of prosecution reaches five percent—we think it more likely that deterrence is at least partially linear, because some high-volume uploaders are more risk-averse than others. Prosecuting fewer than 4500 people—say, 1500—might deter some but not all uploading of illegal content. Partial deterrence will not only reduce the infringement on p2p networks by eliminating the deterred users as sources of infringing files, but will also increase the burden on the remaining high-volume uploaders, as the mass of downloaders in a network shifts to the remaining uploaders. The result may be a cascade effect, in which causing some uploaders to stop providing illegal content (and deterring others from starting to provide such content) imposes technical burdens that in turn cause more uploaders to drop off the network, further increasing the technical burden (and the percentage risk of prosecution) for the remaining uploaders.

We can foresee at least four main objections to the use of criminal or severe civil sanctions to enforce the law against large-scale infringement in the p2p context. First, imposing such liability,

especially criminal liability, on a few individuals in order to deter thousands of others may seem unfair to those who are singled out for prosecution. This unfairness may have no formal legal consequence; selective prosecution occurs in a variety of fields and courts have consistently rejected constitutional challenges to the arbitrariness of making examples of a few defendants, at least where racial animus is not at issue. But it does put the burden of reducing infringement squarely on the backs of a few uploaders, rather than distributing it more evenly among the population of infringers, and many people might find that morally objectionable. And the level of sanction imposed on those select few against whom enforcement is vigorously pursued may well seem "radically disproportionate to the wrong they committed."

Second, the downside of effective deterrence is the risk of overdeterrence. Criminal penalties are particularly likely in white collar cases to deter legal conduct that is near the borderline of illegality and may be wrongly perceived as illegal. In this case, however, we think the risk of overdeterrence is minimal. We are describing criminal prosecution or civil suits for significant monetary damages focused entirely on high-volume uploaders—say, those who upload more than 500 copyrighted songs. It is highly unlikely that these high-volume uploaders are in fact engaged in legal conduct. If virtually all high-volume uploaders are acting illegally, and if it is clear how to avoid being in that category, overdeterrence doesn't seem a significant problem.

Third, as with any criminal law, mistaken prosecutions will impose significant costs on those wrongfully targeted. Similarly, mistaken civil suits will impose significant litigation expenses and related costs. Mistakes will certainly be made, though the straightforward nature of the case and the detailed electronic trails that file transfers create may actually make the risk of mistaken prosecution rather small. It is somewhat more likely that courts will err by punishing high-volume uploaders who are not in fact willfully infringing copyright, but who instead genuinely believe that their conduct is legal. This would be a miscarriage of justice, since willfulness is an element of criminal copyright infringement and of enhanced statutory damages, and the danger of such mistaken verdicts, given the potentially severe sanctions, may be a significant cost of pursuing criminal penalties or enhanced statutory damages against high-volume uploaders.

Finally, criminal prosecution requires the initiative of U.S. Attorneys, and they may find the prospect of prosecuting college students for uploading music politically unpalatable. And imposing criminal penalties is likely to cause defendants to fight back harder. To date, many file sharers sued civilly have settled for relatively low sums of money. Threaten to put them in jail, though, and many will plead not guilty and go to court. This raises the costs, both financial and political, of any given prosecution, though it may be a good rather than a bad thing for society to have these issues vetted in open court. Similarly, while the RIAA has proven willing to file civil suits, none have yet gone to trial, and it may be that jurors will prove sympathetic to file-sharing defendants regardless of what the law provides. This isn't really an objection to liability as much as skepticism that severe civil or criminal sanctions will really be enforced. It is true that a large number of people participate in p2p file sharing, and it is possible that they would protest criminal prosecutions, making the person who brought those prosecutions unpopular, or that they would serve on juries and return nullifying verdicts. On the other hand, some of the most powerful lobbying groups in the world are behind stronger criminal copyright enforcement. They managed to persuade Congress to pass the NET Act, strengthening criminal penalties and expanding the definition of criminal copyright infringement. More recently, a number of Congressional representatives have on two different occasions taken the Justice Department to task for not enforcing the NET Act, suggesting that there might be substantial political will in favor of criminal prosecution.

Still other objections to criminal prosecution or severe civil penalties stem from broader objections to the enforcement of copyright law in the digital environment. If you believe copyright law in the digital environment in general is a bad idea, or that p2p file sharing should be legal, it follows that you wouldn't want to see criminal prosecutions of, or substantial monetary penalties for, uploaders. From the perspective of those who both believe in the copyright system and believe that large-scale file sharing is

illegal, however, criminal prosecutions or very large statutory damage awards offer the advantage of dealing with infringement without unduly hampering technological innovation.

They have disadvantages too, however, as noted above. Most notably, it seems unfair and disproportionate to impose the burden of enforcing copyright so heavily on a few unlucky defendants. This is particularly true if the sanction is severe—we put up with random enforcement of traffic offenses because the sanction is so minor, but we might feel differently if speeders had to spend a year in jail. A perception of unfairness and disproportionality may be particularly likely in regard to p2p users, since the unlucky defendants may be particularly sympathetic: high school or college students who aren't engaged in more obviously antisocial types of conduct. Because of these shortcomings, in the Part that follows we examine alternative methods of targeting enforcement at direct infringers rather than at intermediaries.

RIAA v. Verizon Internet Services, 351 F.3d 1229 (D.C. Cir. 2003)

GINSBURG, *Chief Judge*: This case concerns the Recording Industry Association of America's use of the subpoena provision of the Digital Millennium Copyright Act to identify internet users the RIAA believes are infringing the copyrights of its members. The RIAA served two subpoenas upon Verizon Internet Services in order to discover the names of two Verizon subscribers who appeared to be trading large numbers of .mp3 files of copyrighted music via "peer-to-peer" (P2P) file sharing programs, such as KaZaA. Verizon refused to comply with the subpoenas on various legal grounds.

The district court rejected Verizon's statutory and constitutional challenges to § 512(h) and ordered the internet service provider (ISP) to disclose to the RIAA the names of the two subscribers. On appeal Verizon presents three alternative arguments for reversing the orders of the district court: (1) § 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications the content of which is determined by others; if the statute does authorize such a subpoena, then the statute is unconstitutional because (2) the district court lacked Article III jurisdiction to issue a subpoena with no underlying "case or controversy" pending before the court; and (3) § 512(h) violates the *First Amendment* because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously. Because we agree with Verizon's interpretation of the statute, we reverse the orders of the district court enforcing the subpoenas and do not reach either of Verizon's constitutional arguments.

I. Background

Individuals with a personal computer and access to the internet began to offer digital copies of recordings for download by other users, an activity known as file sharing, in the late 1990's using a program called Napster. Although recording companies and music publishers successfully obtained an injunction against Napster's facilitating the sharing of files containing copyrighted recordings, millions of people in the United States and around the world continue to share digital .mp3 files of copyrighted recordings using P2P computer programs such as KaZaA, Morpheus, Grokster, and eDonkey. Unlike Napster, which relied upon a centralized communication architecture to identify the .mp3 files available for download, the current generation of P2P file sharing programs allow an internet user to search directly the .mp3 file libraries of other users; no web site is involved. To date, owners of copyrights have not been able to stop the use of these decentralized programs.

The RIAA now has begun to direct its anti-infringement efforts against individual users of P2P file sharing programs. In order to pursue apparent infringers the RIAA needs to be able to identify the individuals who are sharing and trading files using P2P programs. The RIAA can readily obtain the screen name of an individual user, and using the Internet Protocol (IP) address associated with that screen name, can trace the user to his ISP. Only the ISP, however, can link the IP address used to access a P2P

program with the name and address of a person—the ISP's customer—who can then be contacted or, if need be, sued by the RIAA.

The RIAA has used the subpoena provisions of § 512(h) of the Digital Millennium Copyright Act (DMCA) to compel ISPs to disclose the names of subscribers whom the RIAA has reason to believe are infringing its members' copyrights. Some ISPs have complied with the RIAA's § 512(h) subpoenas and identified the names of the subscribers sought by the RIAA. The RIAA has sent letters to and filed lawsuits against several hundred such individuals, each of whom allegedly made available for download by other users hundreds or in some cases even thousands of .mp3 files of copyrighted recordings. Verizon refused to comply with and instead has challenged the validity of the two § 512(h) subpoenas it has received.

A copyright owner (or its agent, such as the RIAA) must file three items along with its request that the Clerk of a district court issue a subpoena: (1) a "notification of claimed infringement" identifying the copyrighted work(s) claimed to have been infringed and the infringing material or activity, and providing information reasonably sufficient for the ISP to locate the material, all as further specified in § 512(c)(3)(A); (2) the proposed subpoena directed to the ISP; and (3) a sworn declaration that the purpose of the subpoena is "to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting" rights under the copyright laws of the United States. If the copyright owner's request contains all three items, then the Clerk "shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the [ISP]." Upon receipt of the subpoena the ISP is "authorized and ordered" to disclose to the copyright owner the identity of the alleged infringer.

On July 24, 2002 the RIAA served Verizon with a subpoena issued pursuant to § 512(h), seeking the identity of a subscriber whom the RIAA believed to be engaged in infringing activity. The subpoena was for "information sufficient to identify the alleged infringer of the sound recordings described in the attached notification." The "notification of claimed infringement" identified the IP address of the subscriber and about 800 sound files he offered for trading; expressed the RIAA's "good faith belief" the file sharing activity of Verizon's subscriber constituted infringement of its members' copyrights; and asked for Verizon's "immediate assistance in stopping this unauthorized activity." "Specifically, we request that you remove or disable access to the infringing sound files via your system."

When Verizon refused to disclose the name of its subscriber, the RIAA filed a motion to compel production pursuant to Federal Rule of Civil Procedure 45(c)(2)(B) and § 512(h)(6) of the Act. In opposition to that motion, Verizon argued § 512(h) does not apply to an ISP acting merely as a conduit for an individual using a P2P file sharing program to exchange files. The district court rejected Verizon's argument based upon "the language and structure of the statute, as confirmed by the purpose and history of the legislation," and ordered Verizon to disclose to the RIAA the name of its subscriber.

The RIAA then obtained another § 512(h) subpoena directed to Verizon. This time Verizon moved to quash the subpoena, arguing that the district court, acting through the Clerk, lacked jurisdiction under Article III to issue the subpoena and in the alternative that § 512(h) violates the First Amendment. The district court rejected Verizon's constitutional arguments, denied the motion to quash, and again ordered Verizon to disclose the identity of its subscriber.

Verizon appealed both orders to this Court and we consolidated the two cases. As it did before the district court, the RIAA defends both the applicability of § 512(h) to an ISP acting as a conduit for P2P file sharing and the constitutionality of § 512(h). The United States has intervened solely to defend the constitutionality of the statute.

II. Analysis

The court ordinarily reviews a district court's grant of a motion to compel or denial of a motion to quash for abuse of discretion. Here, however, Verizon contends the orders of the district court were based

upon errors of law, specifically errors regarding the meaning of § 512(h). Our review is therefore plenary.

The issue is whether § 512(h) applies to an ISP acting only as a conduit for data transferred between two internet users, such as persons sending and receiving e-mail or, as in this case, sharing P2P files. Verizon contends § 512(h) does not authorize the issuance of a subpoena to an ISP that transmits infringing material but does not store any such material on its servers. The RIAA argues § 512(h) on its face authorizes the issuance of a subpoena to an "[internet] service provider" without regard to whether the ISP is acting as a conduit for user-directed communications. We conclude from both the terms of § 512(h) and the overall structure of § 512 that, as Verizon contends, a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.

A. Subsection 512(h) by its Terms

We begin our analysis, as always, with the text of the statute. Verizon's statutory arguments address the meaning of and interaction between §§ 512(h) and 512(a)-(d). Having already discussed the general requirements of § 512(h), we now introduce §§ 512(a)-(d).

Section 512 creates four safe harbors, each of which immunizes ISPs from liability for copyright infringement under certain highly specified conditions. Subsection 512(a), entitled "Transitory digital network communications," provides a safe harbor "for infringement of copyright by reason of the [ISP's] transmitting, routing, or providing connections for" infringing material, subject to certain conditions, including that the transmission is initiated and directed by an internet user. Subsection 512(b), "System caching," provides immunity from liability "for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the [ISP]," § 512(b)(1), as long as certain conditions regarding the transmission and retrieval of the material created by the ISP are met. Subsection 512(c), "Information residing on systems or networks at the direction of users," creates a safe harbor from liability "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider," as long as the ISP meets certain conditions regarding its lack of knowledge concerning, financial benefit from, and expeditious efforts to remove or deny access to, material that is infringing or that is claimed to be the subject of infringing activity. Finally,§ 512(d), "Information location tools," provides a safe harbor from liability "for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools" such as "a directory, index, reference, pointer, or hypertext link," subject to the same conditions as in §§ 512(c)(1)(A)-(C).

Notably present in §§ 512(b)-(d), and notably absent from § 512(a), is the so-called notice and take-down provision. It makes a condition of the ISP's protection from liability for copyright infringement that "upon notification of claimed infringement as described in [§ 512](c)(3)," the ISP "responds expeditiously to remove, or disable access to, the material that is claimed to be infringing."

Verizon argues that § 512(h) by its terms precludes the Clerk of Court from issuing a subpoena to an ISP acting as a conduit for P2P communications because a § 512(h) subpoena request cannot meet the requirement in § 512(h)(2)(A) that a proposed subpoena contain "a copy of a notification [of claimed infringement, as] described in [§ 512](c)(3)(A)." In particular, Verizon maintains the two subpoenas obtained by the RIAA fail to meet the requirements of § 512(c)(3)(A)(iii) in that they do not—because Verizon is not storing the infringing material on its server—and can not, identify material "to be removed or access to which is to be disabled" by Verizon. Here Verizon points out that § 512(h)(4) makes satisfaction of the notification requirement of § 512(c)(3)(A) a condition precedent to issuance of a subpoena: "If the notification filed satisfies the provisions of [§ 512](c)(3)(A)" and the other content requirements of § 512(h)(2) are met, then "the clerk shall expeditiously issue and sign the proposed subpoena . . . for delivery" to the ISP.

Infringing material obtained or distributed via P2P file sharing is located in the computer (or in an off-line storage device, such as a compact disc) of an individual user. No matter what information the copyright owner may provide, the ISP can neither "remove" nor "disable access to" the infringing material because that material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers.

The RIAA contends an ISP can indeed "disable access" to infringing material by terminating the offending subscriber's internet account. This argument is undone by the terms of the Act, however. As Verizon notes, the Congress considered disabling an individual's access to infringing material and disabling access to the internet to be different remedies for the protection of copyright owners, the former blocking access to the infringing material on the offender's computer and the latter more broadly blocking the offender's access to the internet (at least via his chosen ISP). "Where different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings." These distinct statutory remedies establish that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material resident on the subscriber's computer.

The RIAA points out that even if, with respect to an ISP functioning as a conduit for user-directed communications, a copyright owner cannot satisfy the requirement of § 512(c)(3)(A)(iii) by identifying material to be removed by the ISP, a notification is effective under § 512(c)(3)(A) if it "includes substantially" the required information; that standard is satisfied, the RIAA maintains, because the ISP can identify the infringer based upon the information provided by the copyright owner pursuant to §§ 512(c)(3)(A)(i)-(ii) and (iv)-(vi). According to the RIAA, the purpose of § 512(h) being to identify infringers, a notice should be deemed sufficient so long as the ISP can identify the infringer from the IP address in the subpoena.

Nothing in the Act itself says how we should determine whether a notification "includes substantially" all the required information; both the Senate and House Reports, however, state the term means only that "technical errors . . . such as misspelling a name" or "supplying an outdated area code" will not render ineffective an otherwise complete § 512(c)(3)(A) notification. Clearly, however, the defect in the RIAA's notification is not a mere technical error; nor could it be thought "insubstantial" even under a more forgiving standard. The RIAA's notification identifies absolutely no material Verizon could remove or access to which it could disable, which indicates to us that § 512(c)(3)(A) concerns means of infringement other than P2P file sharing.

Finally, the RIAA argues the definition of "[internet] service provider" in § 512(k)(1)(B) makes § 512(h) applicable to an ISP regardless what function it performs with respect to infringing material—transmitting it per § 512(a), caching it per § 512(b), hosting it per § 512(c), or locating it per § 512(d).

This argument borders upon the silly. The details of this argument need not burden the Federal Reporter, for the specific provisions of § 512(h), which we have just rehearsed, make clear that however broadly "[internet] service provider" is defined in § 512(k)(1)(B), a subpoena may issue to an ISP only under the prescribed conditions regarding notification. Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A). And as we have seen, any notice to an ISP concerning its activity as a mere conduit does not satisfy the condition of § 512(c)(3)(A)(iii) and is therefore ineffective.

In sum, we agree with Verizon that § 512(h) does not by its terms authorize the subpoenas issued here. A § 512(h) subpoena simply cannot meet the notice requirement of § 512(c)(3)(A)(iii).

B. Structure

Verizon also argues the subpoena provision, § 512(h), relates uniquely to the safe harbor in § 512(c) for ISPs engaged in storing copyrighted material and does not apply to the transmitting function addressed by the safe harbor in § 512(a). Verizon's claim is based upon the "three separate cross-references" in § 512(h) to the notification described in § 512(c)(3)(A). First, as we have seen, § 512(h)(2)(A) requires the copyright owner to file, along with its request for a subpoena, the notification described in § 512(c)(3)(A). Second, and again as we have seen, § 512(h)(4) requires that the notification satisfy "the provisions of [§ 512](c)(3)(A)" as a condition precedent to the Clerk's issuing the requested subpoena. Third, § 512(h)(5) conditions the ISP's obligation to identify the alleged infringer upon "receipt of a notification described in [§ 512](c)(3)(A)." We agree that the presence in § 512(h) of three separate references to § 512(c) and the absence of any reference to § 512(a) suggests the subpoena power of § 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.

As the RIAA points out in response, however, because §§ 512(b) and (d) also require a copyright owner to provide a "notification . . . as described in [§ 512](c)(3)," the cross-references to § 512(c)(3)(A) in § 512(h) can not confine the operation of § 512(h) solely to the functions described in § 512(c), but must also include, at a minimum, the functions described in §§ 512(b) and (d). Therefore, according to the RIAA, because Verizon is mistaken in stating that "the takedown notice described in [§ 512](c)(3)(A) . . . applies exclusively to the particular functions described in [§ 512](c) of the statute," the subpoena power in § 512(h) is not linked exclusively to § 512(c) but rather applies to all the ISP functions, wherever they may be described in §§ 512(a)-(d).

Although the RIAA's conclusion is a non-sequitur with respect to § 512(a), we agree with the RIAA that Verizon overreaches by claiming the notification described in § 512(c)(3)(A) applies only to the functions identified in § 512(c). As Verizon correctly notes, however, the ISP activities described in §§ 512(b) and (d) are storage functions. As such, they are, like the ISP activities described in § 512(c) and unlike the transmission functions listed in § 512(a), susceptible to the notice and take down regime of §§ 512(b)-(d), of which the subpoena power of § 512(h) is an integral part. We think it clear, therefore, that the cross-references to § 512(c)(3) in §§ 512(b)-(d) demonstrate that § 512(h) applies to an ISP storing infringing material on its servers in any capacity—whether as a temporary cache of a web page created by the ISP per § 512(b), as a web site stored on the ISP's server per § 512(c), or as an information locating tool hosted by the ISP per § 512(d)—and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber.

The storage activities described in the safe harbors of §§ 512(b)-(d) are subject to § 512(c)(3), including the notification described in § 512(c)(3)(A). By contrast, as we have already seen, an ISP performing a function described in § 512(a), such as transmitting e-mails, instant messages, or files sent by an internet user from his computer to that of another internet user, cannot be sent an effective § 512(c)(3)(A) notification. Therefore, the references to § 512(c)(3) in §§ 512(b) and (d) lead inexorably to the conclusion that § 512(h) is structurally linked to the storage functions of an ISP and not to its transmission functions, such as those listed in § 512(a).

C. Legislative History

In support of its claim that § 512(h) can—and should—be read to reach P2P technology, the RIAA points to congressional testimony and news articles available to the Congress prior to passage of the DMCA. These sources document the threat to copyright owners posed by bulletin board services (BBSs) and file transfer protocol (FTP) sites, which the RIAA says were precursors to P2P programs.

We need not, however, resort to investigating what the 105th Congress may have known because the text of § 512(h) and the overall structure of § 512 clearly establish, as we have seen, that § 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of

information sent by others. Legislative history can serve to inform the court's reading of an otherwise ambiguous text; it cannot lead the court to contradict the legislation itself.

In any event, not only is the statute clear (albeit complex), the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works. That is not surprising; P2P software was "not even a glimmer in anyone's eye when the DMCA was enacted." Furthermore, such testimony as was available to the Congress prior to passage of the DMCA concerned "hackers" who established unauthorized FTP or BBS sites on the servers of ISPs; rogue ISPs that posted FTP sites on their servers, thereby making files of copyrighted musical works available for download; and BBS subscribers using dial-up technology to connect to a BBS hosted by an ISP. The Congress had no reason to foresee the application of § 512(h) to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along. Had the Congress been aware of P2P technology, or anticipated its development, § 512(h) might have been drafted more generally. Be that as it may, contrary to the RIAA's claim, nothing in the legislative history supports the issuance of a § 512(h) subpoena to an ISP acting as a conduit for P2P file sharing.

D. Purpose of the DMCA

Finally, the RIAA argues Verizon's interpretation of the statute "would defeat the core objectives" of the Act. More specifically, according to the RIAA there is no policy justification for limiting the reach of § 512(h) to situations in which the ISP stores infringing material on its system, considering that many more acts of copyright infringement are committed in the P2P realm, in which the ISP merely transmits the material for others, and that the burden upon an ISP required to identify an infringing subscriber is minimal.

We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforseen [sic] internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology."

The stakes are large for the music, motion picture, and software industries and their role in fostering technological innovation and our popular culture. It is not surprising, therefore, that even as this case was being argued, committees of the Congress were considering how best to deal with the threat to copyrights posed by P2P file sharing schemes.

III. Conclusion

For the foregoing reasons, we remand this case to the district court to vacate its order enforcing the July 24 subpoena and to grant Verizon's motion to quash the February 4 subpoena.

So ordered.

Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006)

The Online Copyright Infringement Liability Limitation Act (OCILLA), codified at 17 USCA § 512, was passed in 1998 as a compromise between the nation's copyright and online service provider (OSP) industries. The legislation, passed as Title II of the Digital Millennium Copyright Act, created a process that was intended to help copyright owners ensure rapid removal of allegedly infringing material from the Internet while guaranteeing compliant OSPs a safe harbor from liability for Internet users' acts of copyright infringement. The U.S. copyright industry thus gained a new tool to combat the loss of billions of dollars (U.S.) annually from copyright infringement; OSPs, concerned about the direction of court decisions concerning their liability for their users' copyright infringement, received protection from potential secondary liability. To qualify, OSPs must "accommodate" technical protection measures employed by copyright holders and implement policies for terminating the accounts of repeat infringers. Further measures are also required of OSPs in some situations, including the takedown of online material in response to a copyright-holder notice—the subject of this Article.

In negotiating the § 512 compromise, copyright holders sought to ensure that OSPs had incentives to remove infringing material, and OSPs sought to avoid lawsuits and judgments based on secondary liability for users' acts of copyright infringement. The resulting § 512 safe harbor is granted to OSPs in exchange for the "expeditious" takedown, upon notice by the copyright holder, of allegedly infringing material. The alleged infringers are to be protected from mistaken takedowns and misuse of this rather remarkable extra-judicial process principally through a counternotice procedure, through which they can demand replacement of the material if the copyright owner fails to initiate a lawsuit.

Copyright-holders have had access to the easy-to-initiate takedown process afforded by 17 U.S.C. § 512 for nearly eight years, and a review of the law seems in order. Has this compromise between industries worked as planned? Has infringing material been removed from the Internet? How have Internet publishers fared, including businesses large and small, bloggers, critics, and the many other speakers who make use of the Internet? How, if at all, has the great democratization of expression afforded by the Internet been affected by a simple, expedient extra-judicial procedure for removing material? These questions are frustratingly difficult to answer, a difficulty exacerbated by the fact that § 512 takedown notices—a matter of private action like any other cease-and-desist letter—are not part of the public record.

But for nearly four years, the Chilling Effects project has attempted to fill some of the gaps in this knowledge by collecting and archiving cease-and-desist notices of all kinds. Chilling Effects has collected § 512 takedown notices from a variety of sources, including all notices received by Google Inc. For this Article, we analyzed nearly 900 of these notices along various axes in an attempt to begin answering some of these questions. Our research is ongoing, and presumably over time the data set will increase in depth and size. As such, this is a preliminary evaluation. Insofar as we have begun to answer some questions, we have also learned enough to raise more questions and establish directions for further research. Unfortunately, however, our findings comprise a rather negative snapshot of the ways in which the § 512 process is being used, and reveal little benefit to some of the constituencies it was intended to support.

. . . .

VI. Observations

A. General Observations

The overall set of 876 cease-and-desist notices includes 514 notices (59%) making a complaint only under § 512(d) (search engine index link); and 315 notices (36%) making a complaint only under § 512(c) (hosted material). In addition, 68 § 512(c)-like notices were sent to OSPs complaining of material residing on a user's computer. In other words, these notices ask for "takedown" in a situation where § 512(a)—the straight safe harbor for routing and communications—likely actually applies. A few notices (22, or 3%) included claims under more than one statutory section. Of the 514 § 512(d) search engine claims, only a few were sent to search engines other than Google. The vast majority of these notices were sent to Google solely, and a few were sent to multiple OSPs including Google. The high incidence of § 512(d) claims is, of course, due to the predominance of notices to Google in our data set. While Google submits all of its notices to Chilling Effects, two-thirds of its notices are for its search engine listings. Google-provided hosting services—including Blogger, UseNet and Google Groups archives—account for about a third of Google's total notices.

1. Google Notices: General Observations

We first note that there has been an increase over time in notices sent to Google, but that we cannot reliably tell from our data whether this represents a continuing upward trend. Section 512(c) and (d) notices both increased in the Google set from 2002 to 2005. In the somewhat more than three years' worth of data that we evaluated, the total number of § 512(c) and (d) notices submitted to the database increased from 70 in 2002 (March-December); to 151 notices in 2003; to 253 notices in 2004; to 245 in just the first seven months of 2005.

We had expected that some of the increase in total numbers of notices would have come through growth in visibility and awareness of the Chilling Effects project itself, but on examining the data it became apparent that most of the growth has come thus far from an increase in actual notices submitted to Google during the period in question. The number of notices actually sent and received by Google over almost the same period of time (April 2002—June 2005) has increased from an average of four per month in 2002 to eighteen per month for the first six months of 2005. However, it was impossible to confidently determine whether there is a forward trend in the data. (Though the chart visually appears to show an increasing trend, the R-squared values for the lines of best fit reveal (1) that the seeming increase is only weakly predictive for § 512(d) notices ($R2 = 0.60$); and (2) that we cannot predict with confidence whether the § 512(c) notices will increase over time, at all ($R2 = 0.33$).) Further, without a broader set of notices than we have, it is obviously impossible to determine whether use of the § 512 process generally is increasing or not.

The § 512(d) search engine notices do appear to have increased more dramatically than the § 512(c) hosted content notices sent to Google, and there is, overall, a much greater volume of § 512(d) notices in the set. This is true even though Google increased its § 512(c) offerings steadily during the study period. Of the increases in § 512 notices noted in the Google set and accordingly in the set of notices as a whole, it is plain that most are § 512(d) notices. The set of § 512(d) notices sent to Google has increased from an average of three notices per month in the second and third quarters of 2002, to an average of 21 per month in the second quarter of 2005.

Whether considered separately by OSP, section, or as a whole, the number of notices collected during any given month is small enough—5 to 45 notices—that a single spate of notices from an aggrieved user can cause a notable spike in the set. In February 2004, for instance, the American Poolplayers Association sent twenty notices to Google for UseNet archives, creating a visible spike in the § 512(c) collection. Likewise, just two months prior, in December of 2003, Mir Internet Marketing sent eighteen notices to Google, spiking the § 512(d) data set. . . .

The preliminary data from The Planet is not yet extensive enough to fully determine trends, or compare with the other notices. We note, however, that The Planet receives many more notices monthly than Google, and so will provide a rich sample of data to review for trends in future work, particularly over longer periods of time than we have yet been able to observe.

2. Self-reported Notices; General Observations

We also examined the self-reported set of notices. Here we note that nearly half the notices were sent in response to a situation where § 512(a) would likely apply—largely situations where alleged infringers are trading files across peer-to-peer networks. In fact, § 512(a) establishes a straightforward safe harbor for OSPs acting as conduits, with no notice-and-takedown procedure. Further, because complained-of files reside on user machines, the OSP cannot take down the material in the first place. In instances where the user is engaged in simple distribution of entire copyrighted works, we may presume that the underlying copyright complaint is strong, although defenses, such as the misidentification of the alleged infringer, may certainly apply. However, because § 512(a) does not authorize takedown notices, these notices raise other issues. We discuss this result further below.

B. Sender Characteristics

We examined the characteristics of those using the § 512 processes in our data set.

1. Corporate Senders

In our data set, corporations and business entities were the primary users of the § 512(c) (hosting) and § 512(d) (search) processes, and the primary senders of notices related to § 512(a) services (64 notices, 94%). Of Google § 512(c) notices, corporate and business senders made up 72% (171 notices) of the senders. Among self-reported § 512(c) notices, corporate and business senders made up 65% of notices. Among § 512(d) notices, the large majority, 409 (79%), were sent on behalf of corporate or business entities.

Beyond the general fact that business entities sent the large majority of notices, there were some interesting specifics. Section 512(c) and (d) senders in our data set are often small Internet businesses. A large percentage of Google search notices—55% of the Google § 512(d) notices—are competition-related. Entities send these notices to request the removal of links to their competitors. (This phenomenon is discussed further, below.) The software and game industries sent 23% of the § 512(c) notices (70 unique notices). These were largely related to circumvention of technological protection measures; a significant percentage included other claims of questionable relevance to the § 512 takedown procedures, including license restrictions, resales, game "cheats," and the like.

Perhaps surprisingly, neither § 512(d) search nor § 512(c) hosting notices in our data set show significant use by the movie and music industries. While . . . these industries anticipated and helped draft the notice and takedown provisions in § 512(c) and (d), our data show them only rarely using these provisions. Corporate and business entities are generally responsible for the lion's share of notices, but the movie and music industries combined were responsible for only 6% of the § 512(c) notices and only 3% of the § 512(d) notices. The lack of entertainment companies in our set may be, at least in part, because they choose not to send search engine complaints; however, we suspect that is not the entire story.

While we did not see nearly the number of § 512(c) or (d) notices we expected from it, the movie industry (followed by the computer software and games, and then music, industries) sent the vast majority of § 512(a) "takedown notices"—where takedown is neither required nor possible, but where complaints about an alleged infringer might convince the OSP to terminate the alleged infringer's service—in our data set. Our data do not reflect the very high numbers (in the tens of thousands annually) of notices

received by larger OSPs from the content industry, but the use of § 512(a) apparent in our very limited data has been anecdotally verified through a confidential interview discussing numbers from larger OSPs, among other sources. We look forward to examining this empirically with data from The Planet. If this § 512(a) effect is borne out, it seems likely that complaints about infringing movies and songs now focus on peer-to-peer networks, where the OSP acts only as a conduit. This change (unanticipated when the statute was drafted and passed) might help explain the relatively few copyright industry § 512(c) and (d) notices we collected. If true, this suggests that the copyright industry's concerns about piracy are currently not well-addressed by the notice-and-takedown process.

2. Individual Senders

Individuals constitute a significant minority of all senders in both the § 512(c) and § 512(d) contexts. Of Google § 512(c) notices, 20.7% of notices are apparently sent by, or on behalf of, individual rights-holders (49 of 236). Among non-Google § 512(c) notices, 17 (25%) were sent by or on behalf of apparent individuals. The situation is not markedly different among senders of § 512(d) notices. Google received 92 (17.9%) of its § 512(d) notices from, or on behalf of, individuals.

As might be expected, complaints sent on behalf of individuals vary considerably; it would be difficult to describe a "typical" complaint. For example, one individual complainant cited a blogger who had repeatedly re-posted entire posts without crediting the original author. Another individual wrote to request the removal of a book cover from a review site (the review, we note, was critical). Another complaint was apparently from a person unhappy with the use of his photograph on a website dedicated to criticizing his alleged disreputable character and dating habits.

3. Repeat Senders

A quarter of the senders in our database are repeat senders, and were responsible for more than half of all the notices. Of the 436 unique senders, 25% are repeat senders, and 329 (75%) sent only one notice. In all, 547 (62.4%) of the notices were sent by repeat senders. Within the 107 (25%) of repeat senders, 86 (20%) sent 2-5 notices; 10 (2%) sent 6 to 10 notices; six (1%) sent 11 to 20 notices; and five senders (1%) sent more than 20 notices—ranging from 21 to 54 notices.

The relatively few senders that sent large batches of notices are a significant presence in the dataset (the top 11 senders sent 29% of the overall notices in the data set) and any problems with their notices can affect the overall conclusions. We paid special attention, therefore, to issues with notices from those top senders. The American Poolplayers Association, which sent 21 notices, had a significant effect on the number of notices with questions about the copyrightability of the complained-of material. (APA's 21 notices comprise 57% of the 37 notices that presented obvious questions of copyrightability.) Microsoft's 21 notices all related to circumvention of software, of which 20 were § 512(c) notices, and one was apparently to a § 512(a) subscriber. ArticleInsider/Infosearch sent 23 notices, 7.2% of the literary properties in the § 512(d) set. Mir Internet Marketing's 50 notices almost entirely (48) related obviously to competitors. Star's Edge/Avatar's 54 notices were not counted as fair uses as a per se rule, but were not excluded from the count if something specific to the notice warranted its inclusion.

4. DMCA Enforcement Companies, Agents, Proxies & Rightsholders

We were interested in who executes the § 512 process for complainants, given the existence of private "rights enforcement" companies. The vast majority of all § 512(c) and (d) notices in our data set were sent by the rightsholders themselves, or their attorneys; far fewer notices were sent by agents, proxies or trade associations. Of § 512(c) notices, 94% were sent by or on behalf of the rightsholders directly. Of § 512(d) notices, 98.5% were sent by or on behalf of the rightsholders directly. Agents, enforcement agencies, and trade associations combined only account for 4.9% of all § 512(c) notices, and only 1.3% of § 512(d) notices. The picture is much more diverse in our § 512(a) notices, where

rightsholders sent 29% of the notices; enforcement companies sent 26.1% of the notices; and trade associations sent 30.4% of the 69 § 512(a) notices. Of § 512(a) notices sent on behalf of the large entertainment corporations, 18 notices were sent by DMCA enforcement companies, prominently including BayTSP, GrayZone and MediaForce.

Trade associations also show up as senders among our data, although they are a clear minority of users of the process. In total, 36 notices were sent by trade associations. Of the trade association notices, most represented corporate interests, such as the Business Software Association; only three represented individual interests, such as the Science Fiction Writers Association and the Creators Syndicate. We note that the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have only 9 notices in the § 512(c)-(d) sections, and that, to the extent that they used copyright enforcement agents such as MediaForce, they may appear under-represented. Only three notices were sent by traditional literary or licensing agents. In a few instances, celebrities or models' agencies and publishers collaborated to send notices.

C. Target Characteristics

Examining the characteristics of the targets of the notices—the alleged infringers—we found that 41% of all Google notice targets can be classed as competitors of the complainants. This is particularly significant for Google § 512(d) complaints regarding links in the index, where 55% of all notices relate to competitors. A significant percentage of the § 512(c) and (d) notices sent to Google—21%—target hobbyists, critics and educational users.

The "hobbyists" category includes many bloggers and fan sites. Notices sent to hobbyists are often from rival hobbyists or businesses in the field. Unauthorized use of photographs or graphics is a common theme in these notices, especially in the blog-related notices. The blogs may or may not be directly related to the topic of the copyrighted work; a use may be simply an illustration, linked to or grabbed from the Internet for its aesthetics rather than its original significance.

Comparison with the self-reported notices—including § 512(a) notices—shows that notices sent about competition are far more significant in the Google set than the self-reported set, and are particularly significant for search index complaints. This is unsurprising, given the fierce competition over search-result rank in Google's index. The hobbyists, critics and educational uses are higher in the self-reported set, also perhaps unsurprising given the self-selecting nature of that set.

D. Recipient OSP Characteristics

The data set of self-submitted notices is too small to afford any real quantitative analysis of recipient OSP characteristics. However, we do note that the notices represent many different kinds of OSPs. A wide variety of hosting providers are represented, including blog hosts (LiveJournal and Blogger, a Google subsidiary), and UseNet hosts (Google Groups submits posts). Section 512(a)-type hosts include many broadband providers of both DSL and cable access. We also have at least one notice to an upstream host of a webhost.

E. Subject Matter: Characteristics of the Allegedly Infringing Material

In this section, we delve into some more detailed characteristics of the notices we observed. For descriptive purposes, we sorted notices, and discuss them, according to loose subject matter categories, such as "text," "photographs" and "film." At some points, we use more detailed descriptors, such as "literary property." Although these categories can be, we think, useful in sketching a picture of the notices as a group, they are mainly descriptive, and we recognize that others may have sorted some notices differently.

1. § 512(c) (Hosted Material) Notices.

Out of all § 512(c) notices in either the Google or self-reported sets (303 in total), 10 relate to movies; 7 to music; 7 to games; 63 to software; 37 to photos; 8 to other graphics; 166 to text; 5 relate to whole websites; and 4 were undefinable.

Looking at the seven § 512(c) notices sent in reference to music more closely, we first note that all seven were self-submitted notices. Three of the seven requested takedown of music files being offered for download—one Faith Hill promotional song, another notice requesting takedown of multiple Faith Hill songs, and a third notice requesting takedown of some 88 songs by Ten Thousand Fists. The other notices were a grab-bag. One notice was a complaint about music files offered, but listed the number of such files available as "0." One notice requested takedown of guitar tabs, which are arguably fair uses; however, taking a fairly conservative approach, we did not code them as such. Two relate to celebrated cases of mashups or other claims of infringement of the derivative-works right: the Grey Album, or Beatallica. This is obviously far too small a sample to be statistically relevant, and almost certainly reflects selection bias relating to media coverage of the relevant subject matter. Increased media coverage may cause more people to download, and to host, the allegedly infringing material, both attracting cease-and-desist letters and also making it more likely that those letters will be submitted to Chilling Effects. For example, the Grey Album was the subject of a concerted "civil disobedience" day, which encouraged users to download and host the work, a mash-up of The Beatles' White Album and JayZ's Black Album. (Similarly, there was a concerted effort aimed at distributing and hosting the Diebold memos, a set of internal memos revealing practices that may have affected electronic voting machines.)

Of the ten § 512(c) notices sent by companies in the film industry, only two were sent to Google; the other eight were sent to other ISPs, and were included in the self-reported § 512(c) set. Of the two Google notices, one was a movie script, and the other cited trademark and copyright complaints about a Google blog, but without specifying any particular copyrighted or infringing works. Of the eight self-reported notices, we first note that two presented obvious defenses: one was a complaint about a screenshot and one was a misguided complaint about a public domain film archived at the Internet Archive. Three of the ten notices complained of illegal offerings of copyrighted content, all presumably popular TV shows. Although two notices were likely related to DeCSS claims, we did not include them in the anti-circumvention counts for lack of adequate confirming information. Finally, one notice was sent from IO/Titan Media to Sharman, notifying it that P2P users were using Sharman's software to distribute Titan's copyrighted films. Obviously, the self-submitted notices constitute a grab-bag of issues, and are likely not representative of all such § 512(c) notices.

As might be expected since the web is still heavily text-based in its offerings, text was by far the most-represented subject matter in the § 512(c) notices: 142 § 512(c) notices relating to text were sent to Google, and 24 § 512(c) notices relating to text were sent to self-reported OSPs and self-submitted by recipients. Of these notices, the majority were not easily classifiable beyond "text"—98 notices total, 16 self-reported OSPs, 82 Google notices. The text notices that were otherwise "unclassifiable" contained a mix of materials, or did not fit into the major categories of texts we had otherwise identified. For instance, we described the Diebold notices as unclassifiable text, because they included e-mails, internal correspondence and other materials. The Avatar/Star's Edge "lecture" materials were often included in "text," as were the Scientologist materials, a political site parodying the New York Times, and many others. Many "unclassifiable text" notices included text from websites. Of the "text" notices from which we could obtain more information, 21 related to systems or methods; 6 were obviously noncopyrightable data; 5 were e-mails posted by the recipient. Twenty-eight notices (or 16.8%) were related to traditional literary texts—18 articles, 7 stories and 3 books. Of the "literary texts," we note that a number of these texts were redistributions of religious, spiritual or Scientology-like materials, including the Avatar notices. Four notices resulted from the author's reconsideration of the publication of the original article.

Of the 37 photo-related § 512(c) notices, a small number (three) were personal photos that the subject wanted removed. Two were parents requesting takedown of photos of children, and one was an

individual requesting takedown of photos of himself from a critical website. Fifteen of the 37 photo-related § 512(c) notices were sent to OSPs other than Google; these included at least four identifiably pornography-related claims; seven from Leslie Kelly, plaintiff in *Kelly v. Arriba*; three personal photographs; and a celebrity photograph, possibly altered into pornography. Of the 22 photo-related § 512(c) notices sent to Google, at least seven were pornography-related claims, including some from Perfect10. The remainder included a variety of photographs, including professional, artistic and non-commercial photographs. We note that the allegedly infringing use of the works often seemed to incorporate the work into a larger work, such as an illustration of an article or a commentary. Further study on the derivative, transformative or substitutive use of photographic works, and the mix of personal, nonprofit or commercial uses, would be appropriate.

Of the 70 § 512(c) notices that were sent regarding software or computer games, 53 notices (76%) obviously or likely targeted anticircumvention devices rather than direct copyright infringement of the code. We discuss issues related to anticircumvention notices further below. Of the other claims included within the notices, nine related to distributions of the program or game, five to apparent resales and three to distributions of the source code. We have surprisingly few notices related to so-called "warez" sites—only 12.9% (nine notices) related to distributions of software, games or code. This may be an artifact of our data, which has few notices to small webhosts; perhaps our review of the notices from The Planet, which provides webhosting, will show a different picture.

2. § 512(d) (Information Location Tools) Notices

The § 512(d) set showed roughly similar composition of subject matter to the § 512(c) notices, with significantly more takedown requests complaining of links to text than any other kind of subject matter—329 of 521 notices (63.1%) asked for removal of links to text materials—unsurprisingly, mostly web-related content, as we discuss below.

Movie industry companies sent only 12 of the § 512(d) notices, and music industry companies sent only two. The software and games industries sent 56 § 512(d) notices requesting removal of links. Of the 56 total § 512(d) notices relating to software or computer games, 46% (26 notices) presented anticircumvention claims, and 54% (30 notices) presented only non-anticircumvention claims. Compared with § 512(c), more § 512(d) notices requested the removal of links offering downloads of works—48.3% of the software and game § 512(d) notices (28 notices). Some of the notices presented multiple claims, including complaints of reverse engineering, derivative works or resales of software.

Notices related to photographs comprised 13% (68 notices) of the § 512(d) notices, with other graphics at 4.6% (24 notices). As with the § 512(c) notices, some of the § 512(d) notices (eight) described what appeared to be personal photographs that the subject wanted de-linked; in only two of these eight notices was it clear that the sender understood that ownership of the copyright likely belongs to the photographer rather than to the subject. And again, as with the § 512(c) photograph notices, a few of these eight § 512(d) photograph notices presented obvious personal privacy issues. For example, one complainant explicitly stated that "the image on the above link has my photo. I do not want people to search my name and see my photo. I feel uncomfortable." The general composition of § 512(d) photographic notices was largely similar to the § 512(c) set: a mix of notices citing professional (including pornographic) works and amateur works on a wide variety of topics.

Looking more closely at the 329 § 512(d) notices complaining of links to text-based material, 50.5% (166) of the 329 notices cited web copy of some sort—some portion of a website, but not the entire website. Thirty-eight (11.6%) § 512(d) "text" notices complained of plain product descriptions. Reviews of individual notices show that in a number of additional notices the complaint related more broadly to descriptions of services or features—effectively, ad or brochure copy. At least half a dozen notices claimed copyright over meta-tags. Over and beyond the numerous notices requesting takedown of text-related webcopy, an additional 53 notices alleged copying of an entire website, and requested removal of

links to the entire site. This area begs study, as there is little caselaw delineating what aspects of a website are copyrightable expression and what are functional, ideas, or otherwise not protectable.

Of the 329 § 512(d) notices targeting text materials, 70 (21.2%) were based on literary properties of various sorts, including four notices citing books and 66 citing "articles" or "stories" (including blog postings). The infringement claims here seemed strong. Dissemination of short text articles in their entirety seems likely to be infringing and not a fair use, should such a complaint be litigated. Likewise, disseminations of entire short stories or poems seem likely to constitute infringement.

As with notices targeting photographs, some of the § 512(d) notices targeting text described various personal privacy or dignity concerns. Seven notices related to private e-mails posted publicly. At least 18 notices expressed a wish to de-index content because of embarrassment over the text. A few complainants expressed unhappiness over the circumstances of the current publication, rather than the publication per se.

3. Section 512(a) (ISP) Notices

We stress that our set of § 512(a) notices is statistically unreliable. There are only 68 such notices, and all were self-submitted. Nevertheless, we include this section to complete the picture of subject matter sent under the various sections in our data set.

As previously discussed, the movie industry sent the majority of these notices: 45 notices (66%). These were most typically form notices alleging peer-to-peer file sharing of commercially copyrighted films from major studios, although a few were apparently pornography. Nine notices made software-related claims, typically sent by BayTSP (a DMCA enforcement company) or the Business Software Association (BSA). Six notices were computer game-related, all sent by either the Interactive Digital Software Association (IDSA) or the Entertainment Software Association (ESA). Only four notices were from the music industry. The remaining notices were unclassifiable or multimedia, including one audiorecording of a book.

F. Enforceability, Substantive Legal Flaws and Process-Related Concerns

Perhaps most striking, we found that at least a third of notices contain at least one of the major categories of flaws we evaluated. These categories pose significant questions about the claim's enforceability in a court of law and/or invite serious concerns about the fairness of the process for targets. They are:

[] substantive legal questions related to the underlying copyright claim; and

[] significant technical noncompliance that renders the notice unusable according to the statute.

This figure does not include other questionable uses of the § 512 takedown process, such as sending notices where § 512(a) would apply, complaining of anticircumvention information, or sending notices when complicated questions of international law are relevant. We also did not count some categories of notices that are arguably fair use or otherwise defensible . . . . In this section, we describe the notices that comprise the "flawed one-third," as well as some other perhaps-problematic notices that we discovered but did not include in the count.

1. Issues with Underlying Copyright Claim.

We first examined significant questions related to the underlying copyright claim, including fair use defenses, other substantive defenses, very thin copyright, or non-copyrightable subject matter. Surprisingly, 31% of § 512(c) and (d) notices present claims that fall into this category. As a rule of thumb, we tried to capture notices where a genuine dispute related to copyright infringement or defenses would clearly arise. Examples range from the clearly problematic—for example, recipes, prices and

metatag information, which are unlikely to be covered by copyright—to instances of very thin copyright claims, such as very short product descriptions. We also included notices where the target was likely to have a fair use defense. A much smaller number of notices in this category were counted due to other substantive concerns, such as questions regarding the ownership of the copyright in question: for example, a small number of notices appear to be sent not by the copyright holder or a representative, but by a party with some other interest in the material, such as the subject of a photograph. Among § 512(c)-(d) notices sent to Google, at least one type of substantive, subject-matter flaw was apparent in 209 notices, or 29% of the Google set. Among the self-reported § 512(c)-(d) notices, 43 (59 %) of the self-reported notices had at least one substantive flaw.

One issue present in the § 512(c) and § 512(d) notice datasets is the problem of noncopyrightable subject matter. A total of 37 notices include claims for noncopyrightable subject matter, such as recipes, pricing information, forms and methods. The American Poolplayers Association sent takedown notices for posting its handicap formula. (Formulas are specifically excepted from copyright by 17 U.S.C. § 102(b).) Release of the handicap formula may present other claims, such as trade secrecy, but the notices were standard § 512 takedown notices, and made no additional allegations. Further, the notices we reviewed did not directly copy the formula from the manual, but instead described the formula, even paraphrasing and adding commentary. Recipes are likewise exempted from copyright as formulas or methods of operation. Although substantial literary expression in the form of surrounding text and photographs may be copyrightable, the base recipe is not. Yet several notices in the database claimed copyrights over recipes, and demanded takedown of copies. Pricing information is also largely factual, yet complainants targeted the release of pricing and sales information.

Questions of copyrightability were also raised by a variety of takedown notices relating to factual material in databases, product descriptions and photographs, and forms and templates. For instance, Yahoo! claimed a copyright on blog templates that emulate the Yahoo! look-and-feel. These templates were developed by blog users for personal use and submitted by their user-developers to Google's Blogger user template space. The copyrightable expression in Yahoo!'s template and layout is likely to be thin indeed; it seems a genuine dispute over infringement would arise. Many of these types of notices fall into a continuum of complaints that relate to websites being spidered and used for other purposes. The targets may be using the content for a variety of purposes: indexing product information, as in Google's Froogle service; generating search engine hits for "link farms"; referencing competitor's products; or emulating a competitor's website. While some such claims may be very sympathetic, such as complaints about URLs being used in a so-called link farm, they skirt the boundary of copyright protection. But the § 512 process admits no such gray areas; takedown removes any work alleged to infringe, regardless of the nature of the infringement.

Product information constitutes another problematic area for copyrightability. In complaints about product information, the copyrighted work may consist of a factual description of a product, accompanied by a very basic, "factual" photograph of the product. While there is no question that such product information in advertising can rise to high levels of artistry, few of the product information notices we reviewed demonstrated much originality. Rather, the product descriptions were often short and descriptive. Similarly, product photographs did not display any particular attention to lighting, background, angle, etc.; rather, they simply showed the described object. While the level of originality required for copyright protection is a mere quantum, at the least, it is likely to be difficult to distinguish between noncopyrightable facts and the copyrightable expression in short, factual, textual product descriptions and representative, non-artistic product photos. As such, we think that such notices require review before takedown, and counted them as problematic based on the very thin copyright claim, and the strong fair use claim that use of such thinly-copyrighted works often presented. These notices probably represent our least conservative coding practice; yet, we were careful to count only those where the copyright was thin, indeed, and expect that we undercounted them due to lack of detailed information in many notices.

Similar issues plague the large number of notices claiming infringement of website "layout" or design. Following our policy of conservatively coding notices for problems, we elected not to include this category of notices in our count of substantively flawed notices, because they present too many analytic challenges. Each such claim should be separately analyzed to determine its validity. In instances where an entire site is "mirrored" or copied, it is certainly likely that copyright infringement is occurring. However, some cursory examination of these claims reveals that some claims are not so strong, and may in fact be considerably weaker. Our brief analysis suggests that at least in some instances, the underlying copyright is again, thin, resting on, for instance, the hierarchical scheme of laying out pages of content; but we do not have enough information about many of these notices to place them in the "flawed" category. We do note that if a large proportion of the "website layout" claims rest on thin (or vanishing) copyright, this would be of particular concern, because many of these notices appear to be related to competitors seeking to de-list their competitors in the Google search engine.

2. Other Defenses

A small number of notices presented various other defenses. For instance, a small number of claims present obvious questions of ownership. In at least seven notices, for instance, the apparent subject, or parent of the subject, of a photograph wrote to request that the photograph be removed from the Internet. While the § 512 formalities were observed—the sender attests that they are the copyright owner or a representative—on reading the notice, it seems likely that the sender has misapprehended copyright law, and does not understand that the photographer is the likely copyright owner.

Two notices presented a different ownership question: software designers claimed that their client had failed to pay for a website design, and that they therefore owned the copyright. To even begin to evaluate the validity of such a claim would require analysis of the contract between the software designers and their clients, a task clearly unsuited for search engines and webhosts. These ownership-related issues between Web contractors and their clients also included a complaint that a former client had altered the website design by removing information about the website designer—the legality of which was centrally dependent on resolution of the ownership question. Another ownership-related dispute relied on a client's complaint that a former web-designer had maintained a copy of the website, which was achieving higher search rankings than the client's. Yet another notice claimed ownership over a work in the public domain. One notice was sent as part of an ongoing dispute among at least three different parties, all of whom claim ownership over a single work known as the "Footprints" poem. These vexing issues are also reflected in the limited available caselaw. In *Relate v. Jones*, an ownership dispute that apparently involved multiple cross-notices between the parties. One party ultimately obtained an injunction barring the other from filing DMCA notices with his ISP. Ownership of a copyright is handled, in the § 512 process, with a simple attestation of ownership. Yet these examples suggest that ownership of copyright—the threshold question before any claim can be made—is readily misunderstood.

One sender sent two claims, seeking to remove blogs that linked to allegedly copyright infringing materials—tertiary linking. Linking to material merely alleged to infringe *17 USC 106* is unlikely to be deemed even contributory infringement. Responsibility for hosting or indexing a site which links to a site that contains allegedly copyright infringing material seems clearly beyond the scope of responsibility of § 512 OSPs.

3. Statutory Flaws

Significant statutory flaws plagued one out of every eleven notices. By "significant" statutory flaws, we mean one of the four flaws that render a notice invalid according to the terms of the statute: failure to identify the allegedly-infringing work; failure to identify the allegedly-infringed work; failure to provide a way to locate the allegedly-infringing work; or failure to provide contact information for the

complainant. Other statutory flaws—the good faith and penalty of perjury statements, and the signature—do not exempt an OSP from responding to the notice, and notices exhibiting these flaws are not included in this figure. Takedowns based on notices with the significant flaws present significant burdens to the recipient OSPs and questions of fairness to the target. A complaint failing to identify the infringed or infringing works fails to make any genuine showing of a controversy, however limited the review of the merits of the controversy may be. Complaints that do not identify the location of the allegedly infringing work may result in over-or under-inclusive takedowns. The complainant contact information is important because alleged infringers have no way to respond with a counternotice if the OSP cannot reach the complainant.

4. Section 512(a) Notices

The non-Google data also show a high incidence of notices—48%, nearly half—where OSPs are actually acting merely as conduits, providing transmission and routing. At their most complete, the notices in the Chilling Effects database include a copy of the original complaint, accompanied by a warning or threat from the OSP to the user. The original complaint might include an "infringement activity report" citing an IP address, a network protocol, and a file alleged to have been distributed. Most complained-of material appeared to reside on users' machines, made available via broadband Internet access through a peer-to-peer network. As noted supra, transmission service falls under § 512(a), under which OSPs receive a safe harbor without taking any material "down." In fact, as the material resides on user computers rather than OSP servers, there is no way for the OSP to take material down, at all. We suspect that the advent of P2P has pushed some of § 512's intended beneficiaries—content providers—into sending notices where § 512(a) would apply. Notice in a § 512(a) context cannot result in "takedown," but it can result in a record of alleged infringers about whom multiple complaints are made. Given § 512's requirement that OSPs develop and promulgate a policy for determining "repeat infringers," it seems possible that those who send notices in a peer-to-peer context are hoping to create a record that will convince OSPs to terminate users who are the subject of complaints. Anecdotal evidence of correspondence from OSPs to their users in our database shows that some OSPs treat § 512(a) notices in this way.

The notices in the Chilling Effects database do not, however, uniformly include both OSP communications and complainant communications, so it is difficult to determine what the standard of the field is. A detailed survey of OSPs regarding their practices would be helpful to better map practices in this area.

5. International Targets

One surprising result was the large number of notices targeting material that appeared to reside outside the United States, particularly for Google notices (253, or 34%, of the Google notices). Further, a small number of notices (6) were sent to foreign OSPs. While the underlying claim might be strong in the United States, foreign targets may have local defenses; at the very least, foreign governments may look askance at the ex ante takedown process of § 512. Of course, foreign-owned material may be hosted on a United States ISP's server, subject to United States laws. However, the vast majority of these notices are related to Google search index results. For these notices, the material may well reside offshore; Google merely provides a link to the site. This situation raises complex questions related to U.S. jurisdiction over foreign actors who run afoul of United States copyright laws—questions that OSPs are almost certainly not in a position to answer when deciding whether to pull material out of an index.

6. Anti-Circumvention Notices

Finally, a number of notices—48 § 512(c) and 26 § 512(d) notices—specifically request removal of apparent "anticircumvention" devices, or links to anticircumvention devices, under § 512. (An

additional five notices did not specifically mention anticircumvention devices, but were possibly targeting them.) We did not add these notices to the count of "substantively flawed" notices. We elected to treat them separately, as they target acts that are likely illegal under 1201. However, these anticircumvention takedown notices are likely not proper subject matter for § 512 notices at all, and at the least they pose significant analytic difficulties under § 512.

Of the § 512(c) notices, 70 notices related to software or computer games, and of those, 48 (68.6%) specifically requested takedown of content based on an anticircumvention claim. Of the remaining 22 notices, five represented possible anticircumvention claims, including game "items" and game "cheats." Thus, of all software and computer game § 512(c) notices, a total of 53 notices (76%) were likely or definitely anticircumvention-related. The anticircumvention claims cited terms such as "cracked copies," "serial numbers or keys," "key generators" and other terms. We note that the term "cracked copies" is vague, and could describe any number of situations: a copy that has been reverse engineered to have the serial number request removed, or to have a serial number embedded in the software, or to have some other change made. Of the § 512(d) notices, 56 total notices presented software and games claims. Of those notices, 26 (46.4%) presented anticircumvention claims, and 30 (53.6%) presented no apparent anticircumvention claims. Some of the notices presented multiple kinds of claims, rendering analysis complex; for instance, claims of distributing works, distributing "hacked" works or various licensing violations (discussed below). Many such notices are form notices that list multiple possible acts, without specifying which is at issue in this instance. The acts may be described vaguely and might specifically reference several acts without specifying which is at issue, including distribution of reverse engineered software, key generator software, software "cheats" or serial numbers and access codes.

7. Claims Other than Copyright

A number of notices (193) appear to include claims in addition to, or instead of, copyright infringement—such as unfair competition, trademark-type claims, or privacy concerns. In some instances, a sender may have had a cognizable copyright claim, but they stated concerns beyond or in addition to copyright infringement. For example, . . . at least 26 notices reflect strong concerns or details relating to privacy issues.

Licensing restrictions have also been raised by senders unhappy with software resales. Three different senders sent a total of seven cease-and-desist notices to request removal of offers to sell software. Two of the notices sought to remove links to previously authorized resellers. The other five notices sought to remove links to offers to sell copies of the works; while these may have been illegal copies, the first two notices in the series explicitly reference the sender's "non-transferable license" and state that only the sender or its "authorized distributors or resellers" have the authority to "complete such license transactions or distribute these products." While some licensing restrictions may map to copyright claims, some will not, and most are likely to be enforced via contract law—an area of law not subject to § 512 takedown or safe harbor. Use of the takedown process to enforce privately-determined rights is a significant expansion, and one that elides the significant policy questions underlying shrink-and click-wrap license enforcement—questions which render an extrajudicial takedown procedure particularly inappropriate. Requests to remove reverse engineered or adapted software may likewise rely partially or entirely on restrictions imposed by license.

Because § 512 requires OSPs to develop a clear policy and establish a takedown procedure, it seems that senders sometimes shoehorn ill-fitting claims into a copyright complaint in order to obtain relief, a use that is troubling. Because of the small percentage of notices that reflect any one of these concerns, they are merely anecdotal, but again, add to the picture of how § 512 is being used.

G. Lack of Counter Notification

A final observation: though the ex ante takedown of questionable material would be troubling under any circumstances, concerns . . . about the number of flaws revealed in our data would be somewhat diminished if we had found evidence of counternotices and putback. Only seven counternotices are included in the Chilling Effects dataset, and very few documented cases of putback can be found. Confidential conversations with service providers again suggest that our data reflect the overall experience of OSPs, though we obviously cannot draw any conclusions based on the limited notices we have. Here again, further research with OSPs is needed. One possible reason for the low incidence of putbacks is that it is easier for some alleged infringers to move material to another hosting service or web site, rather than accept the 10-14 day takedown. Further, our result may be an artifact of our data, which are so dominated by search index notices. As a search provider has no obligation under § 512 (and generally, no ability) to notify the alleged infringer of takedown, there is little opportunity for targets to use the counternotice process, at all. Google does provide hosting services, and we have a substantial number of § 512(c) notices from it, but its hosting services are relatively new, and constitute a minority of notices from Google in our data set. Whether counternotices are more common in other hosting situations is a question for further research.

Of the self-reported § 512(c) notices, relatively few users (only ten) submitted correspondence from the OSP along with the original notice, so there is little opportunity at present to assess whether OSPs are informing their customers of the counternotice procedure. We note, however, that of the ten notices from § 512(c) providers to their customers, four did not provide any information about the counternotice option, four did, and two were ambiguous or confusing. We have an additional 52 notices where a § 512(a) provider forwarded information to its client. Many OSPs bolstered the notices with threats based on the user's obligations from their terms of service; fewer than half (21) presented a § 512(c)-like counternotice option. (We note, however, that of the six universities that were among these OSPs, five proffered counternotice options).

We expect that there is more to learn from our data set; further, we look forward to investigations into broader data sets, data that relate more closely to hosting services, and the like. Although more research would clearly be useful, we found this data set very helpful in developing a limited picture of § 512's use.