Edward Hernstadt
HERNSTADT ATLAS LLP
11 Broadway, Suite 615
New York, New York 10004
Tel: 212-809-2501
Fax: 212-214-0307
ed@heatlaw.com
www.heatlaw.com

Attorney for *Amici Curiae*

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CAPITOL RECORDS, INC., CAROLINE RECORDS, INC., EMI CHRISTIAN MUSIC GROUP INC., PRIORITY RECORDS LLC, VIRGIN RECORDS AMERICA, INC., BEECHWOOD MUSIC CORP., COLGEMS-EMI MUSIC INC., EMI APRIL MUSIC INC., EMI BLACKWOOD MUSIC, EMI FULL KEEL MUSIC, EMI GOLDEN TORCH MUSIC CORP., EMI LONGITUDE MUSIC, EMI VIRGIN MUSIC, INC., EMI VIRGIN SONGS, INC., EMI AL GALLICO MUSIC CORP., EMI ALGEE MUSIC CORP., EMI FEIST CATALOG, INC., EMI GOLD HORIZON CORP., EMI GROVE PARK MUSIC, INC., EMI HASTINGS CATALOG, INC., EMI MILLS MUSIC, INC., EMI MILLER CATALOG, INC., EMI ROBBINS CATALOG, INC., EMI U CATALOG, INC., EMI UNART CATALOG, INC., JOBETE MUSIC CO., INC., SCREEN GEMS-EMI MUSIC, INC., STONE AGATE MUSIC, and STONE DIAMOND MUSIC,	)	
Plaintiffs,	)	
	)	No. 07 Civ. 9931 (WHP)
	)	ECF Case
v.	)	
MP3TUNES, LLC, and MICHAEL ROBERTSON	)	
Defendants.	)	

BRIEF OF AMICI CURIAE PUBLIC KNOWLEDGE, ELECTRONIC FRONTIER FOUNDATION, CONSUMER ELECTRONICS ASSOCIATION, and HOME RECORDING RIGHTS COALITION IN SUPPORT OF DEFENDANTS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE HISTORY

TREATISES

OTHER AUTHORITIES

STATEMENTS OF INTEREST

Amici submit this brief pursuant to the accompanying motion for leave to file this brief *amicus curiae*.

Public Knowledge is a non-profit public interest organization devoted to protecting citizens' rights in the emerging digital information culture and focused on the intersection of intellectual property and technology. Public Knowledge seeks to guard the rights of consumers, innovators, and creators at all layers of our culture through legislative, administrative, grassroots, and legal efforts, including regular participation in copyright and other intellectual property cases that threaten consumers, trade, and innovation.

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization that has worked for over twenty years to protect consumer interests, innovation, and free expression in the digital world. EFF and its more than 14,000 dues-paying members have a strong interest in helping the courts and policy-makers ensure that copyright law serves public interest.

The Consumer Electronics Association (CEA) is the preeminent trade association of the U.S. consumer electronics industry. CEA members lead the consumer electronics industry in the development, manufacturing, and distribution of audio, video, mobile electronics, communications, information technology, multimedia and accessory products, as well as related services, that are sold through consumer channels. Its more than 2,200 corporate members contribute more than $173 billion to the U.S. economy.

The Home Recording Rights Coalition (HRRC) is a leading advocacy group for consumers' rights to use home electronics products for private, non-commercial purposes. HRRC represents the voice of consumers, retailers, manufacturers, and professional servicers of consumer electronics products. The HRRC was founded in 1981, in response to the Ninth Circuit's ruling in *Sony Corp. of America v. Universal City Studios*, later overturned by the

Supreme Court, that distribution of consumer video recorders constituted contributory copyright infringement.

These organizations have filed numerous *amicus curiae* briefs in matters involving interpretation of the safe harbor provisions of the Digital Millennium Copyright Act, including *Viacom Int'l Inc. v. YouTube, Inc.*, 07 Civ. 2103 (LLS), 2010 WL 2532404 (S.D.N.Y. June 23, 2010) and *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), and both organizations participated in an *amicus curiae* brief before the Second Circuit in the case of *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) ("*Cablevision*"), a leading case (along with *CoStar Group, Inc. v. Loopnet, Inc.*, 373 F.3d 544 (4th Cir. 2004)) addressing the level of volitional conduct required for a finding of direct copyright liability.

INTRODUCTION

Amici have moved to file this brief because we are concerned that the Court may be misled by certain arguments Plaintiffs have made in an effort to evict MP3tunes from the statutory "safe harbors" created by the Digital Millennium Copyright Act ("DMCA"). Plaintiffs also raise arguments regarding the public performance right that threaten the viability of both established and emerging computing technologies.

Plaintiffs ask this Court to thwart Congress's intent and turn back the clock on the DMCA. In effect, Plaintiffs' arguments would re-write section 512 so as to substitute their own judgment in the place of a court's in determining what constitutes a "reasonably implemented" policy for the termination of repeat infringers and to elevate "red flag" notice to render pointless the detailed "notice-and-takedown" regime laid out by Congress in section 512(c). Endorsement of Plaintiffs' views would reinstate a climate of legal uncertainty that would harm both innovative online services and the free expression they foster.

In addition, Plaintiffs have mischaracterized the scope and holding of the Second Circuit's decision in *Cablevision*, using the example of one intermediary following a particular practice to arbitrarily set a fictional minimum standard of behavior and technical design. Not only is this interpretation contrary to the holding of *Cablevision*, it asks this court to base liability on a straightforward engineering decision – the use of a typical, indeed standard, mechanism for data storage and management.

Amici urge the court to uphold the sound judgment of Congress and numerous courts and decline Plaintiffs' invitation to undermine the DMCA safe harbors, and the extraordinary innovation they have fostered. *Amici* also urge the court to reject Plaintiffs' incorrect interpretation of Cablevision and the volitional conduct standard, and adopt instead the sound adopted by numerous appellate courts, including the Second Circuit.

ARGUMENT

I. Congress Intended Section 512 to Reduce Legal Uncertainty for Service Providers

A. Congress's Intent Generally

Congress intended the DMCA to "facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education . . . ." S. Rep. No. 105-190, at 1-2 (1998). "[B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand." *Id.* at 8.

In order to accomplish these goals, Congress created a set of "safe harbors" designed to "provide '*greater certainty* to service providers concerning their legal exposure for infringements that may occur in the course of their activities.'" *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (*quoting* S. Rep. No. 105-190, at 20 (1998)) (emphasis added). Congress focused on creating a more predictable legal environment because it recognized that:

> [W]ithout clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability. For example, service providers must make innumerable electronic copies by simply transmitting information over the Internet. Certain electronic copies are made to speed up the delivery of information to users. Other electronic copies are made in order to host World Wide Web sites. Many service providers engage in directing users to sites in response to inquiries by users or they volunteer sites that users may find attractive. Some of these sites might contain infringing material. In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.

S. Rep. No. 105-190, at 8.

Thus, Congress correctly understood that the application of ambiguous copyright doctrines to new Internet technologies would put service providers in an impossible position. Service providers necessarily must make, manipulate, and transmit multiple copies of content at

several stages of their technical processes. These multiple copies might arguably infringe one or more of the display, performance, distribution, reproduction, or other rights in copyrighted content. During the Senate hearings preceding the DMCA, Roy Neel, President and Chief Executive of the United States Telecom Association stated the problem as follows:

> We have no way of knowing what those trillions of bits of information are flowing over our networks. We simply cannot do it, and to be held liable for those transmissions is simply nonsense and it will tie us up in court, create more litigation and more work for lawyers, but won't do anything to advance the construction and deployment of the Internet, nor will it protect copyright owners to any significant degree.

Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Committee on the Judiciary United States Senate on S. 1146, 105th Cong. 29 (1997); *see also* S. Rep. No. 105-190, at 30. In fact, by the time Congress took up the issue in 1997, online service providers had already been embroiled in copyright litigation over the activities of their users. Thus, Congress enacted safe harbors for secondary liability that were "absolutely necessary to the immediate survival of ISPs." *CoStar*, 373 F.3d at 555 (4th Cir. 2004).

B. Section 512's Structure

The structure of section 512 reflects Congress's desire to provide service providers with predictable rules in place of the murky, judge-made standards that characterize copyright's secondary liability doctrines. *See* 3 Melville B. Nimmer & David Nimmer, Nimmer On Copyright § 12B.01[A][1] (2005) (describing conflicting jurisprudence prior to 1998). The statute creates four safe harbors with detailed provisions setting out "rules of the road" for service providers. If their activities fall within one of the safe harbors, service providers may "opt in" to this alternate, more definite, set of rules by meeting specific statutory prerequisites. If the service provider chooses to comply with section 512 procedures, ordinary copyright liability rules will not apply, and vice versa. The statute also clarifies the limits of a service

provider's obligations – for example, by making it clear that a service provider need not monitor its service or affirmatively seek facts indicating infringing activity in order to enjoy the safe harbor. *See* 17 U.S.C. § 512 (m)(1).

In return, copyright owners were given several new remedies against infringers. The first of these is an expedited, extrajudicial "notice-and-takedown" procedure for obtaining redress against alleged infringement. *Id.* § 512(c)(1)(C). Second, copyright owners were given the power to issue pre-complaint subpoenas to service providers like MP3tunes in order to identify and locate infringing Internet users. *Id.* § 512(h).

This level of statutory detail stands in stark contrast to the ambiguous judge-made legal standards that would otherwise govern the activities of service providers. *Compare Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1170-75 (9th Cir. 2007) (discussing secondary liability principles applicable to online service providers) *with Perfect 10, Inc. v. VISA Int'l Serv. Ass'n*, 494 F.3d 788, 811-22 (9th Cir. 2007) (Kozinski, J., dissenting) (pointing out contradictions in secondary liability standards as applied to service providers).

Congress's desire to reduce legal uncertainty for service providers is also amply demonstrated in the legislative history – both in testimony before Congress regarding the legislation that would become the DMCA,[1] and in the legislative committee reports that accompanied the DMCA.[2]

---

[1] *See WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing Before the H. Subcomm. on Courts and Intellectual Property on H.R. 2281 and H.R. 2280*, 105th Cong. 123, 102 (1997) (statement of Representative Boucher about providing "stability in the law" and giving "the Internet service providers the assurances they need" to invest in the Internet).

[2] *See* H.R. Rep. No. 105-796, at 72 (1998) (Conf. Rep.) (Section 512 "provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities"); H.R. Rep. No. 105-551, Part II, at 49-50 (1998) (same); S. Rep. No. 105-190, at 20 (1998) (same); H.R. Rep. No. 105-551, Part I, at 11 (1998) ("[w]hile several

In short, the statutory language, structure, and legislative history all indicate that Congress intended section 512 to reduce the legal uncertainty that service providers would otherwise face in order to foster the growth of the Internet.

II. Plaintiffs' Interpretation of the DMCA Safe Harbors is Contrary to the Text and Intent of the Statute

A. Plaintiffs Would Require Repeat Infringer Policies to Meet Arbitrarily-Set Standards

Plaintiffs' narrow interpretation of section 512(i) would improperly exclude eligible service providers from the statutory immunities Congress created to protect the providers of innovative and value online services. Pl's. Mem. 29-30.

To qualify for the section 512 safe harbor, a service provider must: (1) adopt "a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers," (2) reasonably implement that policy, and (3) inform users of the policy. 17 U.S.C. § 512(i)(1)(A). Importantly, the statutory language of the repeat infringer provision is qualified; the statute only requires that the service provider's policy provide for the service termination of actual repeat infringers, and then only "*in appropriate circumstances*." *Id.* § 512(i)(1)(A) (2006) (emphasis added); *see Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1111 (9th Cir. 2007). As the court in *Veoh* emphasized, terminating a user's account is a serious and drastic action, and must be justified by reliable and verifiable information showing copyright infringement. 665 F. Supp. 2d at 1116.

A properly submitted DMCA takedown notice does *not* constitute evidence of copyright infringement. *Viacom*, 2010 WL 2532404 at *13 (S.D.N.Y. June 23, 2010). As courts have recognized, a good-faith allegation of infringement by a copyright owner may nevertheless be

---

judicially created doctrines currently address the question of when liability is appropriate, providers have sought greater certainty through legislation as to how these doctrines will apply in the digital environment").

wholly unmeritorious. *See Veoh*, 665 F. Supp. 2d at 1117; *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004). The allegations detailed in a takedown notice are exactly that: allegations, no more and no less. Accordingly, takedown notices cannot create an obligation upon the service provider to entirely terminate service for a user. This point is important because, as Congress noted when drafting the statute, the "reasonable implementation" requirement must not undermine the knowledge standard set out in section 512(c), which establishes a separate and distinct immunity based upon notice of alleged infringement. *See* H.R. Rep. No. 105-551 (II), at 61 (1998) ("[T]he Committee does not intend this provision to undermine the principles of new subsection (1) or the knowledge standard of new subsection (c) by suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing.").

Nor does section 512(i) require service providers to monitor or affirmatively seek evidence of infringement; in fact, courts are explicitly instructed not to read any such obligation into the statute. 17 U.S.C. § 512(m) (excepting accommodation of copyright owners' standard technical measures under section 512(i)(1)(B), which is not at issue here); *Viacom*, 2010 WL 2532404 at *13 (quoting *Veoh*, 665 F. Supp. 2d at 1116). Having no affirmative duty to police users, a service provider only loses section 512(i) eligibility if the copyright owner demonstrates that the provider failed to "terminate a user even though it ha[d] sufficient evidence to create actual knowledge of that user's blatant, repeat infringement of a willful and commercial nature." *Corbis Corp*, 351 F. Supp. 2d at 1104.

Repeat infringer policies may take a variety of forms. In *Viacom*, the court found reasonable YouTube's policy of counting as one "strike" against a user both (1) one DMCA takedown notice identifying multiple videos, and (2) multiple DMCA takedown notices received

within a two-hour period. 2010 WL 2532404. Similarly, the court in *Veoh* upheld Veoh's policy of waiting until the second warning to terminate users, even if the first warning resulted from multiple infringements. 665 F. Supp. 2d at 1116, 1118. Importantly, however, neither of these courts held the defendant's policy to be a minimum standard for section 512(i) eligibility, and in neither case was a mere allegation of infringement found to be enough to show actual infringement.

Finally, in their analysis of MP3tunes' repeat infringer policy, Plaintiffs assert that the "work-by-work notice mentality has long been rejected." Pl's. Mem. 32. This claim is both irrelevant and false. First, Plaintiffs conflate the repeat infringer policy requirement of section 512(i) with a notice-and-takedown scheme that service providers may utilize under section 512(c). Second, Plaintiffs' interpretation is incorrect on the merits. The most recent judicial opinion on this issue expressly found that a provider retains immunity even if it only removes the specific clips identified in the DMCA takedown notice. *Viacom*, 2010 WL 2532404 at *14.

Lacking case law on point, Plaintiffs rely instead on a series of inapposite holdings. For example, Plaintiffs point to *United States v. Texas*, 507 U.S. 529, 534 (1993), which concerns federal statutory abrogation of common law – an analysis that is markedly distinct from a situation in which both the source of liability and immunity from liability are explicitly established in federal statute. Plaintiffs also try to rely on *Fame Publishing Co. v. Alabama Custom Tape, Inc.*, a Fifth Circuit case concerned with compulsory licensing. 507 F.2d 667 (5th Cir. 1975). Contrary to Plaintiffs' claims, however, that case did not broadly proclaim that all exceptions to liability must be construed narrowly. *Id.* at 669-70. In fact, the court actually looked to the specific purpose of the compulsory licensing scheme under the 1909 Act, which it examined only after examining the statutory language. *Id.* By contrast, section 512 expressly

provides clear grants of immunity by its own language, and furthermore was enacted to create bright-line rules of immunity. *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (quoting S. Rep. No. 105-190, at 20 (1998)).

If courts undermine the certainty provided by section 512, they will in effect pull the rug out from underneath service providers that reasonably rely upon section 512 immunity to provide valuable, socially productive services to the public. Under clear standards for immunity, service providers may continue to innovate and bring exciting new services to consumers while knowing exactly their responsibilities under copyright law.

B. Plaintiffs' Interpretation of "Red Flag" Knowledge Impermissibly Expands the Knowledge Disqualifier

Plaintiffs' arguments regarding the "red flag" knowledge set forth in section 512(c)(1)(A)(ii) also cannot be squared with the language, structure, and purpose of the statute.

Section 512(c)(1)(A) grants the safe harbor to a service provider only so long as it:

> (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> (ii) in the absence of such actual knowledge, is not aware of facts and circumstances from which infringing activity is apparent [referred to in the legislative history as "red flags"]; or
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material . . .

17 U.S.C. § 512 (c)(1)(A).

Congress also enacted an "exclusionary rule" that clarifies the proper application of the knowledge provisions above: any allegations of infringement received from a copyright owner that fail to comply substantially with the detailed notice requirements set out in section 512(c)(3)(A) "shall not be considered . . . in determining whether a service provider has actual knowledge or is aware of facts and circumstances from which infringing activity is apparent." 17 U.S.C. § 512(c)(3)(B)(i); *see also* H.R. Rep. No. 105-551, Part II, at 56 (explaining this provision).

Thus, where the knowledge provisions of § 512(c)(1)(A) are concerned, the statutory scheme makes a distinction based on the *source* of the knowledge evidence. If the information *comes from the copyright owner*, it must substantially comply with the notice requirements of section 512(c)(3)(A), *e.g.*, by including information reasonably sufficient to permit the service provider to locate the infringing material. *See* 17 U.S.C. § 512(c)(3)(B). Upon receiving a compliant takedown notice, a service provider must respond "expeditiously" or forfeit the safe harbor. *Id.* § 512(c)(1)(C). Thus, the "actual knowledge" and "red flag" provisions effectively do not apply to infringement notices received *from copyright owners* – those notices either fail to substantially comply with § 512(c)(3)(A), in which case they are a nullity, or they meet those requirements, in which case the service provider must respond expeditiously. In short, there is no category of knowledge evidence received from copyright owners that reaches the "actual knowledge" or "red flag" provisions.

Consequently, the "actual knowledge" and "red flag" provisions in the statute apply only where knowledge evidence *comes from sources independent of the copyright owner*. At the same time, however, when a service provider learns about potentially infringing activity from sources other than the copyright owner, the statutory scheme does not require a service provider "to make discriminating judgments about potential copyright infringement." S. Rep. No. 105-190, at 49. Thus, "the 'flag' must be brightly red indeed – and be waving blatantly in the provider's face – to serve the statutory goal of making 'infringing activity . . . apparent.'" Nimmer, *supra*, at § 12B.04[A][1].

Here, among the purported "red flags" claimed by Plaintiffs were Plaintiffs' own notices – which should be disregarded for red flag purposes as discussed above – and the fact that other locker sites were common sources of sideloaded music files. Misstating both the law and facts,

Plaintiffs assert that other locker sites could "***never*** be a legitimate source of music sideloads." Pl's Mem. 10. This is demonstrably false: at a minimum, other locker sites would be a legitimate source for works that are in the public domain, or that have been authorized for widespread sharing. Examples of the latter abound, not merely in the viral marketing by Plaintiffs cited by MP3tunes (Def.'s Mem. 22), but also in many cases, with artists who explicitly grant permission for online sharing under Creative Commons licenses[3] or with other permissions for users to share their music.[4] Even if those locker sites are marketed to their users as serving to host personal files, nothing in the DMCA or any other statute prevents consumers from using those sites to share legitimate material over the Internet, and nothing creates any presumption that files so shared are *per se* illegal. Although Plaintiffs ask the Court to assume otherwise, external locker sites may be sources of legitimate music, and a service provider who provides links to those websites cannot be automatically subject to DMCA-disqualifying "red flag" knowledge.

Plaintiffs' characterization of some sites as having "reputations as havens for piracy" does not change the analysis. Mere awareness that some of the files linked to locker sites with unsavory reputations cannot constitute "red flag" knowledge. *See, e.g.*, *CCBill*, 488 F.3d at 1114 (providing services to websites named "illegal.net" and "stolencelebritypics.com" not enough to raise a "red flag" from which infringing activity is apparent). Indeed, even generalized knowledge that some infringement has occurred on Defendants' *own* site does not create "red

---

[3] Creative Commons licenses are granted by copyright holders to permit certain types of reproduction and distribution, including the sharing of music files online. Creative Commons, *About Licenses*, http://creativecommons.org/about/licenses/.

[4] Online music service Jamendo, for instance, lists over 268,000 tracks in its collection that have all been released with the artists' permission for the works to be shared online. Jamendo, http://jamendo.com. Many artists will also release albums for free online sharing directly. *See, e.g.*, *Calexico, Live in Nuremburg*, http://calexico.cashmusic.org/; Harvey Danger, *Why We're Releasing Our New Album for Free on the Internet*, http://www.harveydanger.com/press/why.php; Nine Inch Nails, *Ghosts: I-IV FAQ*, http://ghosts.nin.com/main/faq (2008).

flag" knowledge and disqualify them from DMCA safe harbors. *See, e.g.*, *Viacom*, 2010 WL 2532404, at *8–10.

By the same token, MP3tunes' alleged knowledge that some source websites are imperfectly scrubbed of infringing links does not raise red flag knowledge either. As the court observed in *Veoh*:

> No doubt it is common knowledge that most websites that allow users to contribute material contain infringing items. If such general awareness were enough to raise a "red flag," the DMCA safe harbor would not serve its purpose of "facilitat[ing] the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age," and "balanc[ing] the interests of content owners, on-line and other service providers, and information users in a way that will foster the continued development of electronic commerce and the growth of the Internet." S. Rep. 105-190, at 1-2 (1998); H.R. Rep. 105-551(II), at 21. See also Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 794 n.2 (9th Cir. 2007).

Veoh, 665 F. Supp. 2d at 1111. Indeed, any finding to the contrary would run directly counter to the Congressional impulse to minimize uncertainty and keep the burden of policing infringement where it belongs: with the copyright holder, who is best suited to determining whether copies of a work are authorized by license or law. Plaintiffs would not only have service providers police their own sites (a requirement explicitly and purposefully excluded from the safe harbors by Congress), but also assess the relative reputations of sites linked to or used as sources by their users. Congress clearly did not intend for the safe harbors to depend upon such a multiplicity of variables, determined not only by the behavior of a service provider's users, but also by the behavior of entirely unrelated parties in a chain of interactions of indeterminate length.

III. Service Providers Are Not Barred by the Public Performance Right From Using Standard Data Storage Models

Contrary to Plaintiffs' suggestion, *Cartoon Network, LP v. CSC Holdings, Inc.* ("*Cablevision*") does not decide their public performance claim. 536 F.3d 121 (2d Cir. 2008). First, the *Cablevision* decision did not address secondary liability or the DMCA safe harbors.

Second, Cablevision's decision to use a deliberately inefficient system to reduce its potential liability does not mean that others must do the same or risk copyright liability, and nothing in the Second Circuit's holding suggests otherwise.

Taken in context, however, *Amici* believe Cablevision can provide valuable guidance. *Cablevision* involved the cable provider's creation of a service called the RS-DVR, a system that allowed its customers to store television programs they had recorded off the air onto servers owned, housed, and serviced by Cablevision on its property. *Id.* at 123–25. The Second Circuit found Cablevision not liable, for three separate reasons. With respect to the allegation that Cablevision was making infringing reproductions when television programs were stored at users' command, the Second Circuit found that the volitional act (and therefore the potentially infringing behavior) was on the part of the user, and not the operator of the automated system. *Id.* at 133. On the claim that Cablevision was making infringing public performances of the recorded works when they were played back, the Second Circuit analyzed the factors necessary to deem a transmission a public performance and found that at least one of those factors was not met. *Id.* at 139–40. Finally, rejecting the assertion that Cablevision was making infringing reproductions when it buffered the entire incoming signal stream, the Second Circuit found that the fleeting buffer copies at issue, necessary for the functioning of so many systems, were too transitory to meet the definition of a "copy" and thus did not impinge upon a section 106 right. *Id.* at 130.

All three components of the Second Circuit's decision – and the legal precedents that informed it – are relevant here. Like Cablevision, MP3tunes does not itself volitionally create copies, but rather automatically processes the selection and copying of files by users. Furthermore, transmissions from MP3tunes' servers to users are not being made to the public. Moreover, the basic process of de-duplicating data, like making transient buffer copies, does not

impinge a copyright holder's exclusive section 106 rights.

A. Direct Liability for Public Performance Requires Volitional Conduct by Defendants

The Second Circuit determined that Cablevision's RS-DVR system did not infringe copyright holders' reproduction rights in television programs because Cablevision itself did not make the copies at issue, but rather implemented automatically the choices and desires of its individual customers. Because the copies were not made at Cablevision's instigation, Cablevision could not be found directly liable for them; instead, the proper defendant for any direct infringement would have been the customer. The Second Circuit noted that the same analysis might be applied to the public performance question, although it did not examine the issue, ruling instead on other grounds. *Id.* at 134. Nevertheless, the Second Circuit's analysis of volition is instructive, and parallels a line of cases dealing with the question of volition that spans the various section 106 rights.

The requirements for direct infringement in a case involving remotely provided services were stated by the Fourth Circuit in *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004) – a leading case on which *Cablevision* extensively relied. The Fourth Circuit explained in *CoStar* that:

> [T]o establish direct liability . . . something more must be shown than mere ownership of a machine used by others to make illegal copies. There must be actual infringing conduct with a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner himself trespassed on the exclusive domain of the copyright owner.

Id. at 550. Therefore, a service provider "who owns an electronic facility that responds automatically to users' input is not a direct infringer." *Id.* This rule is consistent with the traditional requirements for direct infringement and the holdings of other courts, and it is correct.

Until the late 20th century, engaging in "conduct with a nexus sufficient close and causal to the illegal copying," *id.*, was almost invariably a matter of physically performing the infringing activity. Today, however, copying instructions can be delivered via wired or wireless communications to a remote network server, personal computer, or other digital device located off of the copier's premises, and usually maintained by a third party. In response to this physical and legal separation between the party who controls the copying decision and the party who controls the copying equipment, courts have clarified that direct liability attaches, if at all, only to the party who controls the decision to copy.[5] A party whose role is limited to providing the means by which copies are made is not liable for direct infringement.

In one of the first of the network-oriented cases, *Religious Technology Center v. Netcom On-line Communication Services*, 907 F. Supp. 1361 (N.D. Cal. 1995), an Internet service provider was accused of direct copyright infringement based on a customer's posting of copyrighted material to the service provider's computer servers. *See id.* at 1367-68. The court rejected the direct infringement claim, holding that direct infringement requires "some element of *volition or causation* which is lacking where a defendant's system is merely used to create a copy by a third party." *Id.* at 1370 (emphasis added). Volitional control over the copying is necessary for direct infringement, the court explained, because any other "theory would create many separate acts of infringement and carried to its natural extreme, would lead to unreasonable liability." *Id.* at 1369.

In *CoStar*, the Fourth Circuit built upon *Netcom*. CoStar owned copyrighted photographs of commercial real estate. It brought a direct infringement claim against an Internet service

[5] This is not inconsistent with the description of copyright infringement as a strict liability tort. Strict liability in this context means that intent is not an element of the prima facie case; strict liability does not replace the need for actual, direct conduct.

provider, LoopNet, which provided a Web hosting service for real estate listings. LoopNet's customers were loading CoStar's copyrighted photographs onto LoopNet's computers for display on the LoopNet website. *See CoStar*, 373 F.3d at 546-47. The Fourth Circuit held that because LoopNet only provided the means by which copyrights were being infringed and was not "an actual duplicator itself," LoopNet was "not *directly* liable for copyright infringement." *Id.* at 546. It explained that control of the decision to copy is required for direct infringement because "[w]ere this not so, the Supreme Court could not have held, as it did in *Sony,* that a manufacturer of copy machines, possessing constructive knowledge that purchasers of its machine may be using them to engage in copyright infringement, is not strictly liable for infringement." *CoStar*, 373 F.3d at 549.

Consistent with *CoStar*, the court in *Parker v. Google, Inc.*, 422 F. Supp. 2d 492, 497 (E.D. Pa. 2006), could not discern "the necessary volitional element to constitute direct copyright infringement" where Google's search engine "automatically archive[ed] [copyrighted] postings and excerpt[ed] website in its results to users' search queries," so as to not require any human interaction whatsoever. *Id.* In other words, Google had not chosen to make any specific copy on its system.

Similarly, in *Field v. Google Inc.*, 412 F. Supp. 2d 1106 (D. Nev. 2006), the plaintiff alleged that Google directly infringed when it showed users copies of copyrighted material that were "cached" on its computers. *See id.* at 1115. The court disagreed, holding that

> when a user requests a Web page contained in the Google cache by clicking on a 'Cached' link, it is the user, not Google, who creates and downloads a copy of the cached Web page. Google is passive in this process. Google's computers respond automatically to the user's request. Without the user's request, the copy would not be created and sent to the user, and the alleged infringement at issue in this case would not occur.

Id. Thus, the court in *Field* held that "[t]he automated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement under the Copyright Act." *Id.*

These cases all stand for the proposition that, as stated in *CoStar*, "[s]omething more must be shown than mere ownership of a machine" used by others to infringe copyrights. *CoStar*, 373 F.3d at 550; *accord Sony Corp. of Am v. Universal City Studios, Inc.*, 464 U.S. 417, 437 (1984) (rejecting argument "that supplying the 'means' to accomplish an infringing activity and encouraging that activity through advertisement are sufficient to establish liability for copyright infringement"); *MGM Studios, Inc. v. Grokster, Ltd*, 545 U.S. 913, 960 (2005) (Breyer, J., concurring) ("the producer of a technology which *permits* unlawful copying does not himself *engage* in unlawful copying – a fact that makes the attachment of copyright liability to the creation, production, or distribution of the technology an exceptional thing").

In *Cablevision*, the Second Circuit identified two volitional behaviors: the creation of the system as a whole by Cablevision, and the decision to record, made by the user when he enters the appropriate command on his remote control:

> In the case of a VCR, it seems clear—and we know of no case holding otherwise—that the operator of the VCR, the person who actually presses the button to make the recording, supplies the necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine. We do not believe that an RS-DVR customer is sufficiently distinguishable from a VCR user to impose liability as a direct infringer on a different party…

Cablevision, 536 F.3d at 131. The choice to press the "play" button on a VCR, or on the RS-DVR, is no less the customer's decision than the choice to press the "record" button. Accordingly, Cablevision did not engage in volitional conduct requisite for a finding of copyright liability.

While the Second Circuit did not reach the public performance right, all of these considerations can be applied to any of the traditional section 106 rights. The foundational case

of *Netcom*, for instance, found a service provider not liable on these grounds for the same acts that resulted in alleged infringements of a copyright holder's reproduction, distribution, and display rights. *Netcom*, 907 F. Supp. at 1369–72. Likewise, *CoStar*'s analysis of volition was undertaken without distinguishing between the various 106 rights. *See CoStar*, 373 F.3d at 549-551.

Finally, *Amici* note that the potential nexus between Cablevision's conduct and the allegedly infringing activities of its users was much closer than that between MP3tunes and its users. While Cablevision was simultaneously the source of the original works that were ultimately copied and transmitted, MP3tunes does not provide any content to its users before users decide to place it in their lockers. If the Second Circuit (properly) found that Cablevision had not committed a volitional act, MP3tunes should certainly not be found to have done so.

B. Public Performances Must Be Made "To the Public"

In *Cablevision*, the Second Circuit also held that there could not be an infringement of a copyright holder's public performance right when a transmission of a work was not made "to the public." In determining what constitutes a public performance, the Second Circuit looked to the statutory definition, which states that the actor must

> . . .transmit or otherwise communicate a performance…of the work to a place [open to the public] or to the public, by means of any device or process, whether the members of the public capable of receiving the performance. . . receive it in the same place or in separate places and at the same time or at different times.

17 U.S.C. § 101. Cablevision argued that, since each copy or transmission of a work was only available to any one subscriber, the transmission was not being made "to the public." The district court, however, interpreted the relevant group of recipients was the potential audience of the *work*, not the individual *transmission*. Overruling the district court, the Second Circuit held:

> We cannot reconcile the district court's approach with the language of the transmit clause. That clause speaks of people capable of receiving a particular "transmission" or

> "performance," and not of the potential audience of a particular "work." Indeed, such an approach would render the "to the public" language surplusage.

536 F.3d at 135-36.

Here, as in *Cablevision*, the potential audience for each transmission made by the MP3tunes servers is an audience of one user. The nature of the storage mechanism, though different from Cablevision's, does not change the fact that each transmission has an extraordinarily limited potential audience. Put another way, just as the plaintiffs in *Cablevision* blurred the distinction between the potential audience for a work and the potential audience for a transmission, Plaintiffs here blur the distinction between the potential audience for a copy of a work and the potential audience for a transmission of a work.

Even if the transmit clause *could* be read to create an equivalence between the audience for a copy of a work and the audience for a transmission or performance, the analysis does not end there. The underlying question raised by the statute is not whether more than one person has access to a given transmission, but whether a transmission is made to a group of people that can constitute "the public."

MP3tunes does not transmit music to the general public, nor to all of its subscribers. A particular work in a particular locker will only be transmitted to a user who has placed it there—in other words, after he or she has averred to MP3tunes that she either legally owns the file and have uploaded it to her locker, or that she has legal authorization to access the file on the Web and has sideloaded it into her locker. The subset of MP3tunes users who have uploaded or sideloaded any one particular track (and thus have stated to MP3tunes that they are authorized to do so) still falls far short of the "public" required by the transmit clause.

Plaintiffs state that "public" may be composed of individual subscribers and not the general public at large. Pl's Mem. 24. However, the case they cite for this proposition, *National Football*

League v. Primetime 24 Joint Venture, held only that a satellite uplink which led to a satellite broadcast that was received by all of its Canadian subscribers qualified as a public performance. 211 F.3d 10 (2d Cir. 2000). While *NFL* thus suggests that a population less than the general public at large can serve as "the public" for the purposes of the transmit clause, it provides no guidance as to whether that "public" could be taken to mean an individual subscriber, or how many recipients would necessarily constitute "the public." *Id.* at 13.

Cablevision provides a model far closer to the facts at issue. Cablevision's transmissions were only available to that subset of RS-DVR users who had in fact chosen to press the "record" button at the right time to have made the recording in the first place. In this way, Cablevision ensured that any eventual playback would only be by users who had subscribed to the particular channels they were recording and who were permissibly time-shifting. By the same token, MP3tunes only permits transmissions to users who have indeed confirmed that they already have (presumably authorized) access to the work already. The members of this potential audience are far smaller than a satellite service's general set of subscribers, the set of potential in-store video renters, or the potential guests of a hotel. *See Columbia Pictures Indus., Inc. v. Redd Horne, Inc.*, 749 F.2d 154, 158–59 (3d Cir. 1984); *On Command Video Corp. v. Columbia Pictures Indus.*, 777 F. Supp. 787, 789–90 (N.D. Cal. 1991).

C. Plaintiffs' Interpretation of the Public Performance Right Would Chill Innovation in Cloud Computing and Online Storage

While *Cablevision* can assist the court in determining the *legal principles* at play in this case, it should not be taken to dictate the *technological features* that will and will not be permitted to support a finding of public performance copyright liability. *Contra* Pl.'s Mem. 26. In analyzing *Cablevision*'s decision to implement a separate copy for each user's designated recording, the Second Circuit simply noted that "any factor that limits the *potential* audience of a

transmission is relevant." *Cablevision*, 536 F.3d at 137. However, the court did not hold that any particular factor was dispositive. *Id.* at 139. So while the court did attend to Cablevision's particular storage decisions, it did not create a presumption that use of a more efficient and logical storage system might create infringement liability.

Indeed, courts have wisely avoided establishing presumptions for or against liability based on particular technical features. For instance, this Court held in *United States v. ASCAP (In re Cellco Partnership)* that Verizon was not publicly performing musical works embodied in cell phone ringtones when users downloaded them. 663 F. Supp. 2d 363 (S.D.N.Y. 2009). In determining that the transmissions from Verizon's servers to individuals' phones were not public performances, this Court did not suggest that Verizon should have licensed and maintained a separate ringtone file for each customer's chosen ringtones in advance of the customer downloading the file. *Id.* at 371-74.

Moreover, application of the presumption Plaintiffs advocate to this case would be particularly dangerous, because it would target an essentially ubiquitous engineering practice. Virtually every modern computer and computer user takes advantage of techniques such as data compression and deduplication. Every PDF and Microsoft Office file is compressed.[6] Since the 1980s, ZIP files have allowed ordinary users to compress and deduplicate data.[7] Microsoft's NTFS file system and Apple's HFS+ file system both support "transparent compression,"[8] and

---

[6] PDF and MS Office: *See* Adobe Sys. Inc., *PDF Reference, sixth edition: Adobe Portable Document Format version 1.7*, § 2.2.2 (2006), http://www.adobe.com/content/dam/Adobe/en/devnet/pdf/pdfs/pdf_reference_1-7.pdf; Frank Rice, Microsoft Corp., *Introducing the Office (2007) Open XML File Formats* (May 2006), http://msdn.microsoft.com/en-us/library/aa338205(office.12).aspx

[7] *See Phillip Katz, Computer Software Pioneer, 37*, N.Y. Times, May 1, 2000, http://www.nytimes.com/2000/05/01/us/phillip-katz-computer-software-pioneer-37.html.

[8] *See* Microsoft Corp., *File Compression and Decompression* (Nov. 4, 2010), http://msdn.microsoft.com/en-us/library/Aa364219; Mac OS X Hints, *Compress files with HFS+*

online services like Amazon, eBay, and Facebook all use one form of data compression or another.[9] Internal corporate networks use data deduplication to conserve disk space—for instance, many internal email systems (such as Microsoft Exchange) use deduplication for email attachments that are sent to multiple users simultaneously.[10] Backup systems such as Apple's "Time Machine" use deduplication to increase storage efficiency and reduce bandwidth.[11] These ubiquitous techniques take place in the background, but improve the user experience by making it more efficient. These technical details should have no bearing on the outcome of a lawsuit. Below, *Amici* demonstrate that, if the court rules that some data storage methods infringe copyright, there will be consequences far beyond the particulars of this case.

1. Principles of Data Deduplication

Data compression allows computers to save scarce resources (such as bandwidth or hard drive space) by applying techniques that make communication and storage more efficient. Every modern computer system uses these techniques. While computers deploy various complex algorithms in this process,[12] it is easy to see how this can work with a simple example of how data compression saves space by eliminating redundancy: it is more efficient to write "100 x A" than to write "A" one hundred times.[13]

Compression (Sep. 17, 2009), http://hints.macworld.com/article.php?story=20090902223042255.

[9] *See, e.g.*, Curt Monash, *eBay's Two Enormous Data Warehouses*, DBMS2 (April 30, 2009), http://www.dbms2.com/2009/04/30/ebays-two-enormous-data-warehouses/; Curt Monash, *Facebook, Hadoop, and Hive*, DBMS2 (May 11, 2009), http://www.dbms2.com/2009/05/11/facebook-hadoop-and-hive/.

[10] *See, e.g.*, Microsoft Corp., *Exchange single-instance storage and its effect on stores when moving mailboxes* (Feb. 8, 2008), http://support.microsoft.com/kb/175481.

[11] *See* John Siracusa, *Mac OS X 10.5 Leopard: the Ars Technica Review*, Ars Technica (Oct. 28, 2007), http://arstechnica.com/apple/reviews/2007/10/mac-os-x-10-5.ars/14.

[12] *See, e.g.*, L. Peter Deutsch, Network Working Group, Request for Comments 1951: DEFLATE Compressed Data Format Specification version 1.3 (1996), http://tools.ietf.org/html/rfc1951.

[13] The savings from these techniques can be significant. For example, a text file of the King James Bible takes up 4.4 MB of disk space, but a zip file containing *two* copies of the King

A technology known as "data deduplication" is increasingly built directly into computer systems, where redundant data is automatically compressed behind the scenes.[14] Deduplication uses compression techniques as described above, and an even simpler technique: A computer file system can be described as an index of files that each contain a reference to the location where the data comprising the file is stored. On a deduplicating file system, if the same file is stored twice on the same system, the index entry for both files might point directly to the same data.[15]

2. Plaintiffs' Public Performance Argument Creates Undue Liability Exposure for Legal Remote Computing Services that Use Data Deduplication

Computer users increasingly access services "in the cloud," using applications and storing data on remote servers rather than locally (on their own computers).[16] Many people use web-based email services like Hotmail and Gmail, share photos online via Flickr, Picasa, or Facebook, and even use services like Google Documents rather than running an office suite locally. In each case, a user's own personal data, whether emails, photos, or documents, is being stored on servers owned and maintained by a remote service provider. If the Court rules that the use of modern storage techniques makes a service directly liable for infringing a copyright owner's right to publicly perform a work, it could unintentionally cast a shadow of legal peril over a large and growing sector of the economy.

Plaintiffs ask this court to bypass the DMCA and jeopardize the structure of the high-tech industry by ruling that an Internet company directly infringes copyright and "publicly performs"

James Bible takes up only 2.8 MB: a little more than half the size of a single file, and about 70 % smaller than two files. When compared with the non-compressed size of the two files of 8.8 MB.

[14] *See, e.g.*, Jeff Bonwick, *ZFS Deduplication* (Nov. 2, 2009), http://blogs.sun.com/bonwick/en_US/entry/zfs_dedup.

[15] This is nothing new. A similar result can be achieved via "hard linking," a decades-old technique.

[16] *See generally* Red Hat, Inc., *Cloud 101* (2010), http://www.redhat.com/f/pdf/cloud/101_whitepaper.pdf.

a work when it offers a service that allows different users to access copyrighted works they have privately placed into their own accounts, while using standard, accepted storage methods behind the scenes. Most modern Internet services use data efficiency techniques of one kind or another. Additionally, many web services and Internet users use third-party storage solutions, and may have no control or knowledge of whether their storage providers use single instance storage or similar technologies. If the Court sides with Plaintiffs on this matter, it places all of them at risk.

Plaintiffs' reasoning also bypasses the DMCA's safe harbor provisions. Today, a web host is not liable when its users upload infringing materials to their accounts, provided it complies with the DMCA. But under Plaintiffs' reasoning, if two users upload copies of the same infringing file, and the web host's system is configured to automatically deduplicate files, the web host automatically becomes a direct infringer of copyright that publicly performs a work to each visitor to either users' site.

3. MP3tunes' Use of Single Instance Storage Technology Does Not Transform a Lawful Activity into an Unlawful One, Because Each User Accesses a Distinct Legal "Copy" of Each Work

MP3tunes has not violated any copyright owner's exclusive right to publicly perform its works by using data compression and deduplication techniques.[17] Neither the law nor any sound policy rationale requires that companies use inefficient and obsolete storage systems, and the outcome of a lawsuit should not hinge on the exact method by which a computer stores data on a disk.[18] In general, the proper viewpoint is that of the user—courts should not have to delve into the workings of hard disks and the design of file systems to decide a case.

---

[17] See 22-24 in Plaintiff's brief, where it is referred to as "single master" storage.

[18] The consequences of adopting a "bit-centric" view of copyright law can be wide-ranging, and would force future courts to continue to engage in the sort of byzantine theoretical reasoning Plaintiffs urge this Court to adopt. For example, many computer systems use multiple hard disks as part of a single data store. If any one disk fails, its contents can be reconstituted mathematically by analyzing the "parity data" on each of the remaining disks in the array. *See*

Copyright law is written broadly and expressly encompasses all manner of formats, including technologies that had not been invented when the statute was written. A "copy" is a "material object[] ... in which a work is fixed *by any method now known or later developed*, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 101, (emphasis added)[19] The storage technologies MP3tunes uses are simply a new method to store copyrighted materials and allow a work to be perceived.

Plaintiffs assert that finding an infringement of the public performance right hinges upon the question of whether one copy of a work is served to one user or to several. Pl.'s Mem. 24-26. As *Amici* have argued above, this distinction is immaterial. However, *Amici* also note that data deduplication, even when applied to identical music tracks, still allows for separate, legally cognizable copies to exist for separate users.

Each MP3tunes user listens to a distinct legal "copy" (or phonorecord) of each work listed in his account. Because what MP3tunes' systems may do to save space is immaterial from a legal perspective, there is still no single "copy" of a work that has been publicly performed. Each MP3tunes user first uploads a lawful copy of a work to the MP3tunes server. Behind the scenes, and invisibly to the users, MP3tunes then sees if the file that the user had uploaded is

---

James S. Plank, *A Tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems*, University of Tennessee Technical Report CS-96-332, http://www.cs.utk.edu/~plank/plank/papers/CS-96-332.pdf. The same block of parity data can be used to reconstruct different files depending on what other parity data it is combined with. If this court rules there always must be a one-to-one correspondence between bits on a disk and one (and only one) copy of a single work, then does parity data change from being a copy of one file to being a copy of another file depending on which disk in the system fails?

[19] While "copies" are always embodied in material objects, the law does not require that a given material object (such as a hard drive, or isolated sectors of a hard drive) correspond to one and only one copy. Rather, with modern technology, a single material object can constitute multiple copies of a single work (or copies of multiple works).

identical to a file stored elsewhere in the system. If it is, MP3tunes deduplicates the redundant data. Under Plaintiffs' argument, if MP3tunes had used obsolete storage technology and skipped that last step, it would not be liable for publicly performing a work, but because it used more sophisticated technology, it becomes liable for publicly performing the work. However, this assumes, incorrectly, that only one copy exists when multiple file identities share storage resources. This need not be the case. There is no single "performance or display of the work" because each user's copy is legally distinct. (see 2 M. Nimmer § 8.14 [C][3], at 8.192.2 ("*if the same* copy (or phonorecord) of a given work is repeatedly played (*i.e.*, 'performed') by different members of the public, albeit at different times, this constitutes a 'public' performance.") Because in this case, each user accesses a different "copy" in the eyes of the law, there is no public performance.

CONCLUSION

Plaintiffs' arguments rely upon several misinterpretations of the DMCA that, if accepted, would undermine the statute's Congressionally-mandated purpose of establishing the legal certainty necessary for the flourishing of online innovation and expression. Furthermore, Plaintiffs' interpretation of Cablevision and related cases is simply incorrect. *Amici* urge this court to reject Plaintiffs' radical approach, lest copyright liability – including possible liability for standard design decisions – threaten once again to impede legitimate innovation.

DATED: November 16, 2010

Respectfully submitted,

By: __/s/_Edward Hernstad_____

Edward Hernstadt
HERNSTADT ATLAS LLP
11 Broadway, Suite 615
New York, New York 10004
Tel: (212) 809-2501
Fax: (212) 214-0307
ed@heatlaw.com

Attorney for Amici Curiae

Of Counsel:

Sherwin Siy
John Bergmayer
Attorneys,
Jodie Graham
Mart Kuhn,
Law Clerks for Amicus
PUBLIC KNOWLEDGE
1818 N St. NW, Suite 410
Washington, DC 20036
(202) 861-0020
ssiy@publicknowledge.org

Corynne McSherry
Attorney for Amicus
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
corynne@eff.org

Robert S. Schwartz
Attorney for Amicus
CONSUMER ELECTRONICS ASSOCIATION
HOME RECORDING RIGHTS COALITION
Constantine Cannon LLP
One Franklin Square
1301 K St. NW, Suite 1050 East
Washington, DC 20005
(202) 204-3500
rschwartz@constantinecannon.com