Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 21, *Issue* 2 2011 *Article* 9

VOLUME XXI BOOK 2

Copyright Enforcement in the Cloud

Marc Aaron Melzer*

*Fordham University School of Law

Copyright Enforcement in the Cloud

Marc Aaron Melzer*

INTRODUCTION

The increasing digitization of content has created numerous challenges to copyright enforcement over the last two decades, as copies became near-perfect and infringement became easy and inexpensive.[1] The spread of digital content shares a symbiotic relationship with the growth and development of the Internet as a tool for communication and commerce. Innovations in digitization technology have been spurred by the desire for efficient and high-quality methods of transmitting content via the Internet. This technology has evolved as Internet transmission technologies have

A PDF version of this Article is available online at http://iplj.net/blog/archives/volumexxi/book2. Visit http://iplj.net/blog/archives for access to the IPLJ archive.

* LL.M. in Intellectual Property and Information Technology Law, Fordham University School of Law, 2010; J.D., University of Pennsylvania Law School, 2005; A.B., Princeton University, 2002.

1 VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 52–62 (Princeton Univ. Press 2009) (discussing the development and implications of digitization).

improved, allowing more data—thus larger and higher-quality content files—to speed around the globe.[2]

In particular, the last several years have seen the growth of "cloud computing," allowing users to employ a variety of protocols, applications, and transmission techniques to store data and to harness the processing power of remote servers, often controlled by third-party providers.[3] The development of cloud computing, heralded by more-expansive and less-expensive broadband Internet connections, is poised to add a new challenge to copyright enforcement as more users take to the cloud to store, transmit, manipulate, and share content.

This Article will identify likely problem areas for copyright enforcement arising from this technological trend and, through an analysis of recent copyright jurisprudence involving cloud computing, describe the present and near-term viability of copyright enforcement in the cloud.[4] Part I will focus on cloud computing: what the term comprises and what its design and implementation suggest about the viability of copyright enforcement, including challenges posed by different types of cloud computing. Part II will set out the framework of copyright law relevant to this issue. Part III will review some recent cases involving copyright and different types or aspects of cloud computing to analyze the near-term viability of enforcement in the cloud.

I. DEFINING "CLOUD COMPUTING"

Cloud computing refers to a set of approaches to diffuse computing power across more than one physical computer.[5] These approaches are generally divided into three categories:

---

2 *Id.* at 80 (describing the rapid development and deployment of global high-speed data networks).

3 *See infra* Part I.

4 This Article will not discuss user liability or the viability of enforcement against individual infringers.

5 *See* Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. OF STANDARDS & TECH., INFO. TECH. LAB. (Oct. 7, 2009), http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc [hereinafter *NIST Definition*].

Infrastructure-as-a-Service ("IaaS"), Platform-as-a-Service ("PaaS"), and Software-as-a-Service ("SaaS").[6] Nearly all computer users today, and an even greater portion of Internet users, utilize some method of cloud computing in their day-to-day activities.[7] To illustrate this point, the top five websites by visits, accounting for nearly one-quarter of all website visits in a given week, consist of two search engines/portals and three sites that can readily be considered examples of SaaS cloud computing: Facebook, the social networking site and number one website by traffic; Yahoo! Mail, the number one webmail provider by accounts; and YouTube, a video sharing site that will be discussed in more detail below.[8]

By contrast, a user with no presence "in the cloud" would be restricted to use only software found on her own computer, use e-mail, if at all, that is hosted and operated on servers that she controls, and eschew any interactive Internet sites, including all social networking sites.[9] While there are certainly those who operate in this framework, it is neither the norm in practice nor the prevailing business model in the computing or broader technology markets.[10] This comparison implicitly identifies why cloud

---

6 *Id.*

7 John Horrigan, *Use of Cloud Computing Applications and Services*, PEW INTERNET (Sept. 12, 2008), http://www.pewInternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx.

8 *Top 20 Sites & Engines*, EXPERIAN HITWISE, http://www.hitwise.com/us/datacenter/main/dashboard-10133.html (last visited Oct. 2, 2010).

9 Pat Bitton, *Tech Beat: Cloud Computing—What Is It, and Why Should You Care?*, TIMES-STANDARD, Oct. 8, 2010, http://www.times-standard.com/business/ci_16286491 ("If you're using applications like Google Mail or Salesforce.com, you're already using cloud computing."); Michael Otey, *The Rise of Cloud Computing*, WINDOWSITPRO (Apr. 26, 2010), http://www.windowsitpro.com/article/cloud-computing2/The-Rise-of-Cloud-Computing/2.aspx ("Cloud-based services such as Gmail and Hotmail have been in widespread use for years. Social-media sites such as Facebook and MySpace are also cloud-based services that millions of consumers have adopted and even take for granted.").

10 *See, e.g.*, Brad Stone & Ashlee Vance, *Companies Slowly Join Cloud-Computing*, N.Y. TIMES, Apr. 18, 2010, http://www.nytimes.com/2010/04/19/technology/19cloud.html (describing the gradual adoption of cloud computing by companies in several industry sectors).

computing has been described as a new avenue of competition for the major players in the computer industry, such as Microsoft.[11]

Cloud computing relies on the technology of virtualization, which allows an application to create and manage non-permanent, virtual (software-based) servers on physical server hardware.[12] It is this virtualization that provides the seemingly endless elasticity that is essential to cloud computing: "Virtualization means that e-mail, Web, or file servers (or anything else) can be conjured up as soon as they are needed; when the need is gone, they can be wiped from existence, freeing the host computer to run a different virtual machine for another user."[13] Modern cloud computing is a matured version of the mainframe-terminal system that was in vogue in the 1960s and 1970s, where companies would provide employees with "dumb" terminals with which to access the "smart" mainframe.[14] The terminals would require only enough processing power to connect to the mainframe, where the real work

---

[11] *See* William H. Page, *Microsoft and the Limits of Antitrust*, 6 J. COMPETITION L. & ECON. 33, 49–50 (2010) (suggesting that nascent cloud computing implementations can challenge established players, like Microsoft, shifting the antitrust analysis). Page quotes a "florid" description of possible advantages to be found in the cloud:

> Cloud computing offers virtually unlimited, on-demand computing resources. Your applications now live in a new platform—a computing cloud. In the cloud, your applications take advantage of the seemingly limitless processor cycles, memory storage, and network bandwidth along with extensive software capabilities. Your applications only pay for what they use. Beyond basic computing resources, cloud computing offers a range of application services that form a new platform—an Internet operating system—suitable for cost effective, dynamic, and Internet-scale solutions. An Internet operating system offers the scale and services required to meet the requirements of a dynamic, global, software application.

Id. at 50 (quoting Dana Moore & John Hebeler, *Computing in the Clouds*, DR. DOBB'S (Feb. 3, 2009), http://www.drdobbs.com/architecture-and-design/213000642;jsessionid=UMKP$MKFRG4SNQE1GHPSKH WATM32JVN).

[12] *See* Erica Naone, *Conjuring Clouds: How Engineers Are Making On-Demand Computing a Reality*, TECH. REV., Jul.–Aug. 2009, at 54, *available at* http://www.technologyreview.com/computing/22606.

[13] *Id.*

[14] *Id.* ("'Cloud computing is a reincarnation of the computing utility of the 1960s but is substantially more flexible and larger scale than the [systems] of the past,' says Google executive and Internet pioneer Vint Cerf.").

was done.[15] Just as "time sharing" once did, modern cloud computing creates the illusion that a user's individual computer is more powerful than it actually is.[16] Today, readily-deployed virtualization allows this approach to computing to be employed dynamically on a global scale.

The National Institute of Standards and Technology ("NIST") has developed a series of definitions seeking to encompass key elements of the diverse field of cloud computing.[17] These definitions, consisting of "five essential characteristics, three service models, and four deployment models," provide helpful structure to this discussion.[18] The "essential characteristics" are: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[19]

For the discussion of copyright enforcement in the cloud, the first two of these—self-service and broad network access—are the most important. Briefly, broad network access suggests the basis of the "problem" from the perspective of copyright owners. It is the characteristic that allows users to access and share their, or other users', cloud-based files and systems from virtually anywhere with broadband connections. Self-service speaks to the resulting liability questions, at the heart of this Article; namely whether the user or the system is committing and thereby liable for infringement when it occurs. As NIST defines it, the on-demand self-service characteristic means that, "[a] consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically *without requiring human interaction with each service's provider*."[20] The need for

---

15 *See, e.g.*, Jeffrey Voas & Jia Zhang, *Cloud Computing: New Wine or Just a New Bottle?*, ITPRO, Mar.–Apr. 2009, at 15, *available at* http://www.cs.pitt.edu/~ezegarra/Grid_computing/papers/Cloud%20Computing%20New%20Wine%20or%20Just%20a%20New%20Bottle.pdf ("In Phase 1, people used terminals to connect to powerful mainframes shared by many users. Back then, terminals were basically little more than keyboards and monitors.").

16 *See, e.g.*, NELL DALE & JOHN LEWIS, COMPUTER SCIENCE ILLUMINATED 328 (2006) (describing mainframe time-sharing).

17 *See NIST Definition*, *supra* note 5.

18 *Id.*

19 *Id.*

20 *NIST Definition*, *supra* note 5 (emphasis added).

human oversight, or lack thereof, on the provider side can play a key role in the analysis of provider liability, as will be discussed more fully below.[21] While the Copyright Act is generally understood to be and is applied as a strict liability statute,[22] courts have found a distinction in recent years where the defendant's system is automatically making the potentially infringing copies.[23] The "self-service" characteristic of cloud computing speaks to this very question of volitional conduct.

Recent case law has increasingly suggested that copies created as a result of *user* conduct and choice will generally not devolve liability to the service provider, even where the system making the copies was created and is owned and maintained by a service provider.[24] Certainly the NIST definition cannot answer the question in a given scenario of whether a system was making copies at a user's behest, but the existence of the definition, as a guideline to system operators and developers, can serve to bolster

---

21 *See infra* notes 190–200 and accompanying text.

22 *See, e.g.*, Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 308 (2d Cir. 1963) ("While there have been some complaints concerning the harshness of the principle of strict liability in copyright law, courts have consistently refused to honor the defense of absence of knowledge or intention." (citation omitted)); Sony/ATV Music Publ'g LLC v. CAVS USA, Inc., No. 3:08-0265, 2009 WL 2177110, at *11 (M.D. Tenn. July 21, 2009) ("[C]opyright infringement is a strict liability offense in the sense that it does not require that Plaintiffs demonstrate Defendants' intent to infringe, or even knowledge of the infringement.").

23 *See, e.g.*, Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008) ("When there is a dispute as to the author of an allegedly infringing instance of reproduction, *Netcom* and its progeny direct our attention to the volitional conduct that causes the copy to be made." (discussing Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361 (N.D. Cal. 1995))); *see also* CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 549 (4th Cir. 2004) ("While the court in *Netcom* did point out the dramatic consequences of a decision that would hold ISPs strictly liable for transmitting copyrighted materials through their systems without knowledge of what was being transmitted, the court grounded its ruling principally on its interpretation of § 106 of the Copyright Act as implying a requirement of 'volition or causation' by the purported infringer. This construction is one for which we have already indicated our preference over the contrary decision described in [*Playboy*]." (comparing *Netcom* with Playboy Enters. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993))); Parker v. Yahoo!, Inc., No. 2:07-cv-02757-MAM, 2008 WL 4410095, at *1 (E.D. Pa. Sept. 25, 2008) ("Although copyright infringement generally operates under a theory of strict liability, various courts have required an additional element of 'volition or causation' to find direct infringement.").

24 *See infra* notes 190–200 and accompanying text.

an argument along these lines, potentially allowing the service provider to avoid liability.

The "broad network access" characteristic stresses network availability and the ability of the consumer to access the data or service through a variety of client platforms, including "mobile phones, laptops, and PDAs [personal digital assistants]."[25] The ability to broadly view and distribute content is at the heart of the copyright enforcement problem online, so its place on the list of essential characteristics makes clear the relevance of this discussion to ongoing enforcement efforts. Pre-digitization, copyright enforcement was still difficult, but usually due to lack of scale: individual bootleggers selling a small quantity of a limited selection of copied material.[26] Now, users want and expect all content to be accessible everywhere, all the time.[27] Though this Article is not addressing the issue of individual infringers, ubiquitous, high-speed connectivity has been a boon for this type of scofflaw.[28] As to our focus, legitimate, law-abiding users are rarely concerned with whether and how a back-end system makes copies of copyrighted content to ensure the broad access that they demand. Broad network access also involves more parties in the transmission of data, increasing the number of Internet service providers and other intermediaries who must handle and pass along the data, potentially creating automatic, short-lived (or other) copies as part of the process.[29]

The approaches listed earlier—IaaS, PaaS, and SaaS—are referred to in the NIST definition as the three "service models."[30] Software-as-a-Service is the model with which most people are

---

[25] *NIST Definition*, *supra* note 5.

[26] *See, e.g.*, Brett Lunceford & Shane Lunceford, *Meh. The Irrelevance of Copyright in the Public Mind*, 7 NW. J. TECH. & INTELL. PROP. 33 (describing pre-digital examples of copyright infringement).

[27] *See, e.g.*, TECHNOLOGY CONFERENCE AT SUPERCOMM 2009, FUTURE VISION OF MOBILE BROADBAND 12 (Oct. 21–22, 2009), http://www.atis.org/supercomm/Presentations/LTE%20Track/Future%20Vision%20of% 20Mobile%20Broadband.pdf.

[28] *See, e.g.*, William F. Adkinson, Jr., *Liability of P2P File-Sharing Systems for Copyright Infringement by their Users*, PERIODIC COMMENTS. ON THE POLICY DEBATE, 4–5 (2004), http://www.pff.org/issues-pubs/pops/pop11.7p2psystems.pdf.

[29] DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE 87 n.3 (2009) (describing the process by which ISPs relay messages across the Internet).

[30] *NIST Definition*, *supra* note 5.

likely familiar. The most common example is web-based e-mail, where the consumer is using the provider's infrastructure and application, with perhaps a limited ability to specify user preferences. Social networking sites—Facebook, LinkedIn, and others—function similarly, to the extent users are inputting and uploading content and making connections via the sites' respective interfaces. Even the now-taken-for-granted act of shopping online involves some interaction with SaaS cloud computing when the consumer enters her credit card number and the provider's server-side software, often controlled by a third party to the transaction, processes the order information. Given the "closed sandbox" nature of most SaaS applications (meaning that users' options and their ability to modify the application are strictly limited) copyright owners could argue that SaaS operators have a greater ability—and thus a greater duty—to police infringement on their systems. This will be discussed more below.

Platform-as-a-Service describes a system where the user can deploy her own applications, "created using programming languages and tools supported by the provider."[31] However, the consumer's control is limited to those applications and perhaps some control of the hosting environment configurations.[32] In this model, the consumer may benefit from the greater processing power or storage capacity of the provider's system, or may need access to the rapid elasticity listed as an essential characteristic above. Infrastructure-as-a-Service takes the Platform-as-a-Service model a step further and gives the user control over all fundamental computing resources, down to "operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."[33] Engaging with an IaaS provider is equivalent to outsourcing a user's full data center needs, retaining the ability to access the center's operations via the Internet.

Both PaaS and IaaS involve primarily the dedication of physical resources—servers, network connections, etc.—so the

---

31 *Id.*

32 *See id.*

33 *See id.*

level of control remaining with the cloud service provider is arguably lower than is found in SaaS. While copyright owners could demand that service providers police these systems, PaaS and IaaS providers could counter that argument by explaining that to inspect every byte that crosses a user's virtual server would cripple a predominantly legitimate business.[34] For example, Amazon.com, with its Amazon Web Services ("AWS") and Elastic Cloud Compute ("EC2") products, among others, is one of the largest providers of IaaS cloud computing services.[35] One of its featured case studies is Sorenson Media, "a provider of video solutions."[36] Amazon, as a provider of cloud computing services to Sorenson Media, would likely argue that it would be unreasonable to put it in the position of policing for copyright infringement the readily scalable server space that Sorenson provisions. Such server space includes storage, database servers, application servers and a content delivery network.[37]

NIST also describes four deployment models, detailing how cloud infrastructure can be operated and made available: private cloud, community cloud, public cloud, and hybrid cloud.[38] All four may be managed by third-party providers, but the availability of the infrastructure of private and community clouds is limited to a certain set of users: either a single organization (private) or a group of organizations (community).[39] A public cloud's infrastructure is made available to the general public and is owned

---

[34] *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984) (applying patent law's "substantial noninfringing use" standard to copyright).

[35] *What Is AWS?*, AMAZON WEB SERVS., http://aws.amazon.com/what-is-aws (last visited Oct. 13, 2010).

[36] *AWS Case Study: Sorenson Media*, AMAZON WEB SERVS., http://aws.amazon.com/solutions/case-studies/sorenson-media (last visited Oct. 13, 2010).

[37] *Id.* ("Today, the Sorenson 360 Video Delivery Network service is architected entirely on top of Amazon Web Services—including Amazon EC2, Amazon S3 and Amazon CloudFront. [Sorenson's Vice President of Engineering, Charles] Sismondo explains, 'At the most simple level, when a customer uploads a video it hits our EC2 app servers, creating a database entry, sitting inside an S3 bucket and then pushed to the cloud for Cloudfront deployment and consumption . . . . We've also added a service layer that includes UltraDNS, Scalr and Pingdom to facilitate optimum interaction, uptime and availability of these services.'").

[38] *NIST Definition*, *supra* note 5.

[39] *See id.*

by a company selling cloud services. A hybrid cloud combines two or more of these deployment models. Each model raises challenges for copyright enforcement, though private and community clouds somewhat mitigate the problem of identifying the primary infringer, which plagues enforcement on the open Internet.[40]

II. COPYRIGHT LAW IN THE CLOUD

Before further examining how cloud computing poses specific, and perhaps new or modified, challenges to copyright enforcement, this article now clarifies which elements of copyright law are under discussion. As noted above, this Article will not address the issue of copyright infringement by individual users, but rather will focus on the question of enforcement as regards network intermediaries: Internet service providers and site and service operators, who generally fall under the statutory definition of providers of "interactive computer service[s]"[41] or online service providers ("OSPs").[42] While this distinction will shift our focus towards secondary liability more than primary liability for infringement, both types of liability will be discussed below.[43]

A. Identifying Infringement

Copyright in the digital age faced initial challenges in defining what constituted copying, given the potentially transient nature of

---

40 *See id.*

41 *See, e.g.*, 47 U.S.C. § 230(f)(2) (2006) ("The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.").

42 17 U.S.C. § 512(k)(1)(A) ("the term 'service provider' means an entity offering the transmission, routing or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification of the content of the material as sent or received.").

43 Additionally, this Article will not discuss the first prong of copyright infringement analysis—whether the plaintiff owns a valid copyright for the work in question—as this is often assumed or uncontested in cases such as those discussed herein, and, even when contested, is part of the analysis regardless of the medium or method of the alleged infringement.

digitally stored content, compared to analog or hard-copy storage. Around the time that the Internet was becoming available to the public, the Ninth Circuit decided *MAI Systems Corp. v. Peak Computer, Inc.*,[44] a key case in digital copyright jurisprudence. *MAI Systems* addressed the question of whether RAM copies of computer software, created automatically by the software so that it could be run, constitute copying for the purposes of copyright infringement.[45] Peak was in the business of servicing computer systems, and MAI computers accounted for more than half of Peak's business.[46]

The Ninth Circuit, reviewing the district court's grant of an injunction against defendant Peak, looked to the definitions found in the Copyright Act.[47] The Copyright Act defines "copies" as:

> material objects, other than phonorecords, 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.[48]

The Copyright Act then explains:

> A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.[49]

Peak contested the district court's finding that the copies of MAI software that were created in the computers' memory ("RAM") while Peak was servicing MAI computers were "fixed," as defined in the Copyright Act.[50] Both the district court and the

---

44 991 F.2d 511 (9th Cir. 1993).

45 *Id.* at 517.

46 *Id.* at 513.

47 *Id.* at 517–18 (citations omitted); *see also* 17 U.S.C. § 101.

48 17 U.S.C. § 101.

49 *Id.*

50 MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993).

Ninth Circuit, however, held that the copy created in RAM satisfied the statutory definition of an impermissible copy.[51] Neither court fully engaged the question of what constitutes a "period of more than transitory duration,"[52] which is a key question for digital and online copyright enforcement, and is a point with which later courts have taken issue.[53]

The *MAI Systems* view of copying in the digital world was applied to the online world two years later in *Religious Technology Center v. Netcom On-Line Communication Services, Inc*.[54] Notably, *MAI Systems*, as a Ninth Circuit decision, was binding precedent on the *Netcom* court in California,[55] but it was also the dominant pronouncement at the time on the construction of copyright law as applied to computers and digital technology. In *Netcom*, owners of copyrights in the works of L. Ron Hubbard, science-fiction writer and founder of the Church of Scientology, sought a judgment of infringement against a former minister of Scientology, Dennis Erlich, who was posting materials to the alt.religion.scientology ("a.r.s.") Usenet newsgroup; the owner of the bulletin board system ("BBS") that hosted a.r.s., to which the minister was posting portions of the copyrighted works; and the Internet service providers used by the BBS operator to make his system accessible to Internet users.[56]

Relying on *MAI Systems*, the *Netcom* court held that, "there is no question . . . that 'copies' were created, as Erlich's act of sending a message to a.r.s. caused reproductions of portions of plaintiffs' works on both [BBS operator] Klemesrud's and [ISP] Netcom's storage devices."[57] Here, the issue was not whether the copies were sufficiently fixed—the court held that: "Even though the messages remained on their systems for at most eleven days,

---

51 *Id.*

52 *Id.*

53 *See, e.g.*, Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 127 (2d Cir. 2008) (discussing and distinguishing the *MAI Systems* court's analysis of the "fixation" issue).

54 907 F. Supp. 1361, 1365 (N.D. Cal. 1995) ("This case concerns an issue of first impression regarding intellectual property rights in cyberspace.").

55 *Id.* at 1368.

56 *Id.* at 1365–66.

57 *Id.* at 1368.

they were sufficiently 'fixed' to constitute recognizable copies under the Copyright Act"[58]—but rather whether the BBS and ISP were liable for the mere presence of copies "automatically made on their computers using their software as part of a process initiated by a third party."[59]

The court declined to adopt the plaintiffs' argument advocating liability for direct infringement on the part of the BBS and ISP: "[I]t does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet."[60] The court took a kinder view of the plaintiffs' arguments regarding secondary liability, both contributory and vicarious. Contributory "[l]iability for participation in the infringement will be established where the defendant, 'with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.'"[61] The court allowed for the possibility that the ISP could be liable for contributory infringement if the plaintiffs could prove that the ISP had timely knowledge of the infringement.[62]

The court also found that the plaintiffs had raised a genuine issue of fact in the first prong of the vicarious liability test: whether the defendant "has the right and ability to control the infringer's acts."[63] The dispute here concerned Netcom's alleged ability, or professed inability, to screen messages or curtail user activity in a sufficiently precise fashion so that such policing would only affect users violating Netcom's terms of use, which prohibited copyright infringement.[64] However, the court held that Netcom, as a fixed-

58 *Id.*

59 *Id.*

60 *Id.* at 1372.

61 *Id.* at 1373 (citation omitted).

62 *Id.* at 1374–75. The court did not reach the ultimate question of whether Netcom had knowledge of the infringement since the issue was before the court on motions for summary judgment. The court concluded that, "there may be a question of fact as to whether Netcom knew or should have known that such activities were infringing," and when it gained that knowledge. *Id.*

63 *Id.* at 1375.

64 *Id.* at 1375–76. As with the issue of Netcom's knowledge under the contributory liability test, the court here was limited in its ability to reach the ultimate question because the matter was before the court on motions for summary judgment.

fee service provider, failed to satisfy the second prong of the vicarious liability test because it did not enjoy a direct financial benefit from Erlich's infringement.[65]

The secondary liability tests discussed in *Netcom* set the stage for much of the online copyright enforcement jurisprudence that followed, and will be essential to our analysis of the copyright enforcement challenges posed by cloud computing as ISPs and other interactive computer systems providers become ever more important to the day-to-day operations of computing at all levels. In *Playboy Enterprises, Inc. v. Frena*,[66] the court held a defendant BBS operator directly liable for violating the plaintiff's exclusive rights "to distribute copies . . . of the copyrighted work to the public" and "in the case of . . . pictorial . . . works . . . to display the copyrighted work publicly,"[67] even though the defendant contended that he did not upload any of the infringing images to the system himself and did not necessarily know that they were available via his BBS.[68] Regarding the defendant's knowledge of the direct infringement, the court held that "[i]ntent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement . . . ."[69]

Relying on this language, the *Netcom* plaintiffs argued that Netcom, too, should be held liable for direct infringement despite its purported lack of knowledge.[70] However, the *Netcom* court held that the intent or knowledge rule stated in *Playboy* was limited to allegations of direct infringement of the distribution right, "where liability exists regardless of whether the defendant makes copies."[71] The *Netcom* plaintiffs only indirectly alleged a violation of their distribution rights, found in 17 U.S.C. § 106(3), that the court chose briefly to address.[72] The court held that

---

65 *Id.* at 1376–77.

66 839 F. Supp. 1552, 1555 (M.D. Fla. 1993).

67 *See id.* at 1555 (quoting 17 U.S.C. § 106(3), (5) (2006)).

68 *Id.* at 1559.

69 *Id.*

70 Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1370 (N.D. Cal. 1995).

71 *Id.*

72 *Id.* at 1370–71.

Playboy was "factually distinguishable" on this point because Netcom did not store files for distribution.[73] It concluded that:

> [f]inding such a service liable would involve an unreasonably broad construction of public distribution and display rights. No purpose would be served by holding liable those who have no ability to control the information to which their subscribers have access, even though they might be in some sense helping to achieve the Internet's automatic "public distribution" and the users' "public" display of files.[74]

The § 106(3) claim reappeared in later plaintiffs' allegations, but ultimately was superseded by the Digital Millennium Copyright Act,[75] ("DMCA") which "ruled out [liability] for passive, automatic acts engaged in through a technological process initiated by another . . ." thus "codif[ying] the result in . . . *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*"[76]

B. Fair Use

After defining the relevant terms and enumerating the bundle of rights conferred by ownership of a valid copyright, the Copyright Act lists a number of limitations and definitions of scope: cases where infringement can be proven, but in which the defendant will not be liable under the Act.[77] For the purposes of this discussion, the "fair use" exception found in 17 U.S.C. § 107 is the most relevant of these limitations, because it exempts apparent instances of infringement from being the basis for

---

[73] *Id.* at 1372.

[74] *Id.*

[75] Digital Millennium Copyright Act, Pub. L. 105–304, 112 Stat. 2860 (1998). The Digital Millennium Copyright Act also ruled out future *MAI Systems*-type claims. Title III, Computer Maintenance Competition Assurance Act, amended 17 U.S.C. § 117 to enable those repairing computers to make certain temporary, limited copies while working on a computer. *See* 17 U.S.C. § 117(c) (2006).

[76] ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 622 (4th Cir. 2001) (citing Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995)).

[77] *See* 17 U.S.C. §§ 107–22.

liability. The section defines the exception in arguably broad terms:

> Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work . . . , for purposes such as criticism, comment, news reporting, teaching . . . , scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—
> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (4) the effect of the use upon the potential market for or value of the copyrighted work.[78]

Both the purposes and factors enumerated in the statute have been judicially construed as illustrative and advisory, rather than exhaustive. "Section 107 contemplates that the question of whether a given use of copyrighted material is 'fair' requires a case-by-case analysis in which the statutory factors are not 'treated in isolation' but are 'weighed together, in light of the purposes of copyright.'"[79] For example, while quoting from a book for the purposes of a book review will generally be found to be a fair use of copyrighted material, publishing a lengthy quote from the most interesting part of a new, not-yet-released book probably will not.[80]

Though a commercial purpose, as contemplated by the first factor, weighs against a finding of fair use, such a determination is not dispositive. In analyzing whether a use can claim protection behind § 107, courts have looked to whether the challenged use is

---

[78] 17 U.S.C. § 107.

[79] A.V. v. iParadigms, LLC, 562 F.3d 630, 638 (4th Cir. 2009) (citation omitted).

[80] *See, e.g.*, Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 539–40 (1985).

"transformative," a concept triumphed by District Court Judge Pierre Leval in his highly-influential[81] 1990 article:

> I believe the answer to the question of justification turns primarily on whether, and to what extent, the challenged use is transformative. The use must be productive and must employ the quoted matter in a different manner or for a different purpose from the original. A quotation of copyrighted material that merely repackages or republishes the original is unlikely to pass the test; in Justice Story's words, it would merely "supersede the objects" of the original. If, on the other hand, the secondary use adds value to the original—if the quoted matter is used as raw material, transformed in the creation of new information, new aesthetics, new insights and understandings—this is the very type of activity that the fair use doctrine intends to protect for the enrichment of society.[82]

This idea has particular traction in the digital world, where all content can ultimately be reduced to bytes and the word "transformative" takes on a uniquely technological flair.[83]

Importantly, however, fair use operates only at the periphery of copyright enforcement in the cloud because it is an exception to the primary act of infringement, not a separate defense against allegations of secondary infringement. Accordingly, the intermediaries primarily discussed herein cannot make use of the fair use defense, except to the extent that they are confronted with direct infringement claims in addition to claims for secondary

---

[81] Ben Sheffner, *Sony v. Tenenbaum: There Are Limits to Fair Use Defense in Copyright Infringement Cases*, 18 WASH. LEGAL FOUND. No. 25 (Oct. 9, 2009), *available at* http://www.wlf.org/Upload/legalstudies/legalopinionletter/100909Sheffner_LOL.pdf.

[82] Pierre N. Leval, Commentary, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1111 (1990).

[83] *See, e.g.*, *iParadigms*, 562 F.3d at 640 (holding that defendant's digital archiving of plaintiffs' school papers for a software system designed to detect plagiarism was sufficiently transformative in purpose and use to constitute "fair use"). *But see* UMG Recordings, Inc. v. MP3.Com, Inc., 92 F. Supp. 2d 349, 351 (S.D.N.Y. 2000) (rejecting defendant's contention that it was effecting a transformative use of "space shifting" by eliminating users' needs for physical CD copies of their music collections).

infringement. Most of these latter claims, however, will be avoided under the Digital Millennium Copyright Act, as noted above.[84]

C. Digital Millennium Copyright Act

The DMCA, passed and signed into law in October 1998, codified two World Intellectual Property Organization ("WIPO") treaties into United States law. For purposes of this discussion, our focus is Title II, *Limitations on Liability Relating to Material Online*,[85] codified at 17 U.S.C. § 512. Section 512 limits liability for online service providers ("OSPs") in certain circumstances. It also includes procedures by which OSPs and ISPs can avail themselves of a "safe harbor" against liability for secondary copyright infringement.[86] Section 512 limits the liability of service providers in four situations, if certain conditions are met. Service providers are not liable:

> for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections.[87]

This immunity is contingent on the service provider interacting with the material only to the extent absolutely necessary for the transmission to occur, by request of a third party to that third party's designated recipients, and not storing copies of the material transmitted for longer than absolutely necessary.[88] For the purposes of § 512(a)—describing transitory digital network communications—"service provider" is defined as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified

---

84 *See supra* note 78 and accompanying text.

85 17 U.S.C. § 512 (2006).

86 *Id.*

87 *Id.* § 512(a).

88 *Id.* § 512(a)(1)–(5).

by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[89] This definition encompasses ISPs, such as America Online and Comcast, in their traditional role of relaying digital packets from one server on the Internet to another.[90]

For all other parts of § 512, a "service provider" is defined as "a provider of online services or network access, or the operator of facilities therefor" and includes all entities encompassed by the previous, narrower definition.[91] Applications to which this broader definition applies include:

> *System caching*: Service providers generally are not liable as a result of "intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider. . . ." [92] This is an essential function in the provision of most online services and network access, so § 512(b) is largely protecting behavior that is needed for the Internet to operate.
>
> *Information residing on systems or networks at direction of users (or, "Hosting" services[93])*: Service providers generally are not liable as a result 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 . . . ."[94] As will be discussed below, this subsection is of critical importance to Web 2.0 service providers whose business models rely on user-generated content.[95] These service providers must, however, be vigilant

89 *Id.* § 512(k)(1)(A).

90 *See, e.g.*, JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 42–44 (2005) (describing how packet-switched networks operate); *see also* POST, *supra* note 29, at 80–89.

91 17 U.S.C. § 512(k)(1)(B).

92 *Id.* § 512(b).

93 CRAIG JOYCE ET AL., COPYRIGHT LAW § 9.03, at 794 (6th ed. 2003).

94 17 U.S.C. § 512(c).

95 *See infra* Part III.

> in meeting the conditions set forth in § 512(c) and elsewhere in § 512 in order to avail themselves of the statutory safe harbor.
>
> *Information location tools*: Service providers generally are not liable for "referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link . . . ."[96] As with § 512(b), subsection (d) serves largely to immunize a fundamental behavior of the Internet, and certainly of the World Wide Web, which is built on a system of links and pointers.

Many of the recent cases in this area hinge on § 512 and service providers' fidelity to its protections and conditions.[97] As a threshold matter, none of the protections of § 512 are available to a service provider if it fails to comply with subsection (i):

> The limitations on liability established by this section shall apply to a service provider only if the service provider . . . has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, 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.[98]

While subsections (a) and (b) focus on purely technical behaviors and do not condition the immunity on lack of knowledge,[99] subsections (c) and (d) require that the service

---

96 17 U.S.C. § 512(d).

97 *See, e.g.*, Perfect 10, Inc. v. Google, Inc., No. CV 04-9484 AHM (SHx), 2010 U.S. Dist. LEXIS 75071 (C.D. Cal. July 26, 2010).

98 17 U.S.C. § 512(i).

99 *See Id.* § 512(a)–(b) (providing that liability limitations apply to service providers if certain acts/criteria are met ranging from the service provider not initiating the transmission to it not being involved with the selection of the transmission of infringing material, none of which expressly address immunity on the basis of lack of knowledge).

provider lack "actual knowledge" that the material or activity using the material is infringing.[100] Subsection (d) codifies a combination of the contributory and vicarious liability standards discussed above: the service provider must lack actual or constructive knowledge, and also must not receive a direct financial benefit from the infringing material.[101]

Subsection (c) features the more robust and better known "notice and takedown" procedures, with which service providers must comply to avail themselves of the "safe harbor." Addressing the operation of hosting services, subsection (c) requires that service providers designate an agent, who will receive all notifications of infringement directed to the service provider.[102] Failure to comply with this requirement in a timely fashion can cost a service provider its ability to rely on § 512 as a defense to secondary infringement liability.[103] To be effective, the notice must comply with § 512(c)(3), and the provider must respond to an effective notice according to its policy, as discussed above, pursuant to § 512(i).[104] The precise contours of these requirements and protections continue to play out in litigation, particularly where cloud computing services of one form or another are concerned.

III. RECENT COPYRIGHT JURISPRUDENCE IN THE CLOUD

Having established the context in which questions of copyright enforcement in cloud computing are presented, we will now examine some recent cases that have confronted these issues and derive from them what we can expect from courts and relevant parties in the future.

---

100 *See* 17 U.S.C. § 512(c)–(d) (expressly providing that service providers should not be liable if there is no actual knowledge or awareness of infringing material).

101 *Id.* § 512(d)(1)–(2).

102 *Id.* § 512(c)(2).

103 *See, e.g.*, Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., No. C07-03952, 2010 U.S. Dist. LEXIS 85266, at *23–24 (N.D. Cal. Mar. 19, 2010) (noting that "a service provider cannot be eligible for the safe harbor provisions of the DMCA until 'the service provider has designated an agent to receive notifications of claimed infringement'" (quoting 17 U.S.C. § 512(c)(2))).

104 *See* 17 U.S.C. § 512(i).

Service providers have been availing themselves of the DMCA safe harbor provisions, found in § 512(c), for more than a decade.[105] Some recent cases illustrate the current contours of the protection and the level of compliance necessary to take advantage of that protection. The almost-defunct[106] online video site, Veoh, recently won a trio of decisions upholding its § 512(c) defense against contributory infringement.[107] Veoh's service, which was substantially similar to Google's YouTube,[108] is effectively a video application using the SaaS model of cloud computing—users interact with the service through their web browser software, but the video processing all takes place on Veoh's computers, using Veoh's software.[109]

---

[105] *See, e.g.*, CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 556 (4th Cir. 2004); *see also* UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009).

[106] *See, e.g.*, Ty McMahan, *Veoh Lives On—Behind the Acquisition of the Video Site*, WSJ.COM DIGITS BLOG (Apr. 8, 2010, 9:06 A.M.), http://blogs.wsj.com/digits/2010/04/08/veoh-lives-on-behind-the-acquisition-of-the-video-site ("It wasn't technically Veoh Networks Inc.'s final hour, rather its final two hours, when a relatively unknown start-up with no revenue stepped in to acquire the heavily capitalized online video company."); *see also* Antony Bruno, *Veoh Closing Down, UMG Lawsuit Blamed*, BILLBOARD.BIZ (Feb. 11, 2010), http://www.billboard.biz/bbbiz/content_display/industry/e3i550e90cd48d89b8c0504928f5c1c244e ("Online video sharing site Veoh is going out of business. The AllThingsD blog says it cut the entire staff yesterday and a bankruptcy filing is expected soon."); Peter Kafka, *Universal Music Group Didn't Help Veoh, but it Didn't Kill it*, ALLTHINGSDIGITAL: MEDIA MEMO (Feb. 11, 2010, 4:25 P.M.), http://mediamemo.allthingsd.com/20100211/universal-music-group-didnt-help-veoh-but-it-didnt-kill-it ("The music label's suit made it very difficult for Veoh to climb out of the deep hole it found itself in last year. But it was the Web video start-up, not Universal, that dug that pit.").

[107] *UMG Recordings*, 665 F. Supp. 2d at 1118; UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1092 (C.D. Cal. 2008); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1155 (N.D. Cal. 2008).

[108] *See About YouTube*, YOUTUBE, http://www.youtube.com/t/about (last visited Oct. 14, 2010) ("Founded in February 2005, YouTube is the world's most popular online video community, allowing millions of people to discover, watch and share originally-created videos. YouTube provides a forum for people to connect, inform, and inspire others across the globe and acts as a distribution platform for original content creators and advertisers large and small.").

[109] *See Io Grp.*, 586 F. Supp. 2d at 1139–40 **(**describing the automated uploading process used by Veoh, where, after a user would submit a video on Veoh's website, Veoh's systems would convert each video into Flash format and perform other automated tasks to make them searchable and available to other users).

In the first of these three decisions, *Io Group v. Veoh*, the court found that Veoh complied with all of the requirements of § 512.[110] Io Group, an adult entertainment company, sought an infringement judgment against Veoh based on copyrighted adult videos that Veoh users had uploaded to the site.[111] Rather than following the "notice and takedown" provisions of the DMCA, and engaging Veoh's DMCA-compliant policy, Io Group provided Veoh with no notice of the infringing content prior to commencing its suit.[112] By the time the suit was filed, however, Veoh had independently decided to remove all adult video content from its site, coincidentally including any content that formed the basis for Io Group's infringement claims.[113]

The court reviewed Veoh's policies, both with respect to its user-facing terms of use and acceptable usage policy and with an eye towards DMCA compliance.[114] After a step-by-step review of § 512's requirements, the court concluded that Veoh qualified for the safe harbor protections, despite Io Group's attempts to chip away at Veoh's policies and practices.[115] The court also noted its displeasure with Io Group's avoidance of the "notice and takedown" process, given Veoh's apparent receptiveness to play within the DMCA's rules.[116]

The other decisions in Veoh's favor came in a case brought by UMG Recordings, whose sound recordings and music compositions could be heard in videos, including UMG-produced

---

110 *Id.* at 1141.

111 *Id.* at 1136.

112 *Id.* at 1137.

113 *Id.*

114 *Id.* at 1137–38.

115 *Id.* at 1141–55. The court considered and rejected Io Group's argument that Veoh should fall outside of the safe harbor because of the apparent ease with which rogue users can regain access to the service after expulsion for infringement, which is a current source of tension in ongoing policy debates about copyright reform. The court cited the Ninth Circuit's decision in *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1111 (9th Cir. 2007) for the proposition that the DMCA states, "A service provider reasonably implements its repeat infringer policy if it terminates users when 'appropriate.' Section 512(i) itself does not clarify when it is 'appropriate' for service providers to act. It only requires that a service provider terminate users who are 'repeat infringers.'" (internal citation omitted).

116 *Id.* at 1148–50.

music videos, uploaded by third-party users to the Veoh service.[117] Veoh asserted its DMCA safe harbor defense, on the same grounds as it did in *Io Group*.[118] In the first of the two relevant decisions in this case, UMG moved for summary judgment to block Veoh's assertion of its DMCA defense.[119] The court focused on the technical processes by which the videos were manipulated, stored and accessed using Veoh's system. In particular, the decision discussed four software functions, which UMG claimed pulled Veoh outside § 512's protections: "(1) the reproduction of works through the creation of Flash versions of uploaded videos; (2) the reproduction of works through the creation of 'chunked' copies of uploaded videos; (3) the public performance of works when users access videos via streaming; (4) the distribution of works when users access videos via downloading."[120]

The court ultimately held that the limitations on liability found in § 512(c) apply to these software functions when they are employed for the purpose of facilitating access to user-stored material.[121] The court accepted as correct Veoh's argument, based in the language of § 512(c), that the statute presupposes that service providers will facilitate users' access to the material and that the purpose of processing done by the service provider need not merely be storage.[122] While this decision did not discuss "volitional conduct" in those terms, the analysis proceeds along similar lines.[123] Veoh argued that § 512's protections are not limited only to those functions that constitute storage at the user's request, but also encompass those activities necessary to accomplish storage.[124] The court agreed, holding that "the infringing conduct must occur *as a result of the storage*."[125] While

[117] UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1082 (C.D. Cal. 2008).

[118] *Id.* at 1091.

[119] *Id.* at 1082.

[120] *Id.* at 1088.

[121] *Id.* at 1092 ("The four software functions that UMG challenges fall within the scope of § 512(c), because all of them are narrowly directed toward providing access to material stored at the direction of users.").

[122] *Id.* at 1088–89.

[123] *See* Page, *supra* note 11 and accompanying text; Naone, *supra* note 12.

[124] *UMG Recordings*, 620 F. Supp. 2d at 1088.

[125] *Id.*

this was a matter of statutory interpretation of the DMCA, rather than a broader reading of copyright, it follows that the distinction is whether Veoh's actions stem directly—and *automatically*—from the user's volitional conduct of either uploading a video for storage using Veoh's infrastructure or accessing the video to view on Veoh's system.[126]

Having lost in its attempt to block Veoh's DMCA safe harbor defense, UMG next tried to attack Veoh's compliance, in much the same way as Io Group did.[127] Indeed, the court here explicitly cited the *Io Group* holding, titling that section of its decision, "Prior Finding in *Io Group* that Veoh is entitled to the Section 512(c) Safe Harbor."[128] As in *Io Group*, the court here addressed each component of the safe harbor step by step, finding at each point that Veoh was in compliance to the extent required by law.[129]

However, in a recently filed appeal to the Ninth Circuit, UMG is challenging the district court's grant of summary judgment.[130] At the heart of the appeal is UMG's argument that "the copyright rules that apply to online content companies like Veoh aren't all that different from those that apply offline, regardless of what the DMCA says."[131] Much of the brief repeats the arguments rebuffed by Judge Matz in the district court and criticizes his decisions.[132] Additionally, UMG challenges the characterization of Veoh's

---

[126] The court said as much in its analysis:

> Common sense and widespread usage establish that "by reason of" means "as a result of" or "something that can be attributed to . . . ." So understood, when copyrighted content is displayed or distributed on Veoh it is "as a result of" or "attributable to" the fact that users uploaded the content to Veoh's servers to be accessed by other means.

Id. at 1089.

[127] *See id.* at 1107; Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1154 (N.D. Cal. 2008).

[128] *UMG Recordings*, 620 F. Supp. 2d at 1104.

[129] *Id.* at 1105–1118.

[130] Appellants' Brief at 1, UMG Recordings, Inc. v. Veoh Networks, Inc., No. 09-56777, (9th Cir. June 17, 2010), 2010 WL 3706518 [hereinafter UMG Brief].

[131] Joe Mullin, *Not Dead Yet: Veoh's Big Copyright Win Outlives Company*, CORP. COUNSEL (Apr. 30, 2010), http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202457430480; *see also* UMG Brief, *supra* note 130, at 45 ("The DMCA did not simply rewrite copyright law for the on-line world." (citation omitted)).

[132] *See generally* UMG Brief, *supra* note 130.

service as equivalent to a web hosting service.[133] UMG's brief tries to differentiate between a web host, via a browser request, serving material that it has stored at the direction of a user, and Veoh's serving a video stored at the direction of a user,[134] but does not appear to explain it in a way that actually distinguishes them. Veoh's reply brief approvingly reviews the district court's decision and works step by step through the DMCA safe harbor analysis.[135] This appeal deserves attention particularly because it is directed to the Ninth Circuit, headed by Chief Judge Alex Kozinski, who has been vocal on Internet and intellectual property law issues.[136]

The popular video-sharing site YouTube is in the midst of litigation[137] substantially similar to Veoh's ongoing dispute with UMG. Content creator Viacom, and related companies, sued YouTube for copyright infringement based on the presence of user-uploaded copyrighted videos on the YouTube site.[138] The parties recently engaged in a round of summary judgment motions focused on the DMCA safe harbor.[139] Unsurprisingly, YouTube cited approvingly to the *Veoh* decisions, arguing that "[a]n unbroken line of cases, including recent decisions involving a video hosting service just like YouTube, confirms that Section 512(c) bars such [infringement] claims."[140] Viacom criticized the *Veoh* decisions, but attempted to distinguish them nonetheless,

---

133 *See id.* at 43.

134 *See id.* at 43–44.

135 *See generally* Brief of Appellee, UMG Recordings, Inc. v. Veoh Networks, Inc., No. 09-56777, (9th Cir. June 19, 2010), 2010 WL 3706519.

136 *See* UMG Brief, *supra* note 130, at 45; *see also* Alex Kozinski & Josh Goldfoot, *A Declaration of the Dependence of Cyberspace*, 32 COLUM. J.L. & ARTS 365, 368 (2009) (discussing Ninth Circuit, and other, decisions regarding online copyright infringement).

137 Anne Broache & Greg Sandoval, *Viacom Sues Google over Youtube Clips*, CNET NEWS (Mar. 13, 2007, 2:14 PM), http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html.

138 *See id.*

139 *See, e.g.*, Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment on Liability and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. Mar. 18, 2010) (No. 07-cv-02103), 2010 WL 1004561 [hereinafter Viacom Brief]; Memorandum of Law in Support of Defendants' Motion for Summary Judgment, Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. Mar. 18, 2010) (No. 07-cv-02103), 2010 WL 1004562 [hereinafter YouTube Brief].

140 YouTube Brief, *supra* note 139, at 19.

arguing that YouTube itself committed the infringement, so that the "right and ability to control" the activity of users is not the dispositive issue.[141]

In a thirty-page decision issued in June 2010, Judge Louis Stanton granted summary judgment to YouTube as to all of Viacom's claims for direct and secondary infringement, finding that "they qualify for the protection of 17 U.S.C. § 512(c)."[142] Judge Stanton focused on the knowledge requirement found in § 512(c)(1)(A)(i) and (ii) and, reviewing the legislative history and recent intellectual property case law, concluded that YouTube did not have the requisite knowledge to void DMCA safe-harbor protection and that Viacom's assertion of culpability by knowledge of "red flags" was not compatible with the statute.[143] He also distinguished *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*[144] and held that peer-to-peer file-sharing networks are not covered by § 512(c), finding Viacom's reliance on *Grokster* and its progeny faulty.[145] Viacom has appealed and made public statements anticipating victory at the appellate level.[146] Progress in this case and in the *Veoh* appeal could set up a Supreme Court showdown in the near future, perhaps clarifying certain elements of the DMCA's safe harbor.

While the legal lessons of the *Veoh* decisions thus far make it clear that most service providers, at least those falling under § 512(k)(1)(B), can readily avoid liability by complying with § 512's requirements, the broader lesson may not be as clear. As a relatively small and non-essential service provider, Veoh was in a good position to manage its users and respond to takedown notices with the requisite speed and diligence to satisfy the safe harbor provisions. It seems unlikely that a § 512(k)(1)(A) service provider—a traditional ISP—could operate quite so nimbly. Perhaps these services can address most of their needs within §

141 Viacom Brief, *supra* note 139, at 57–61.

142 Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 529 (S.D.N.Y. 2010).

143 *See generally id.*

144 545 U.S. 913 (2005).

145 *Id.* at 525–27.

146 *Viacom-YouTube Litigation*, VIACOM, INC., http://news.viacom.com/news/Pages/youtubelitigation.aspx (last visited Nov. 16, 2010).

512(a), but many provide storage capabilities for their users, such as website hosting and backup file storage, opening them up to the protections, but also the requirements, of § 512(c). Traditional ISPs, such as Comcast and Verizon, must be cautious to comply with notice-and-takedown procedures with respect to their hosting features lest they find themselves the subjects of secondary infringement actions.[147]

A recent summary judgment decision[148] against the owner of several BitTorrent websites stands in marked contrast to Veoh's repeated victories.[149] Applying the *Grokster*[150] Court's holdings on inducement, the court in *Columbia Pictures Industries, Inc. v.*

---

[147] Comcast provides two gigabytes of storage to all high-speed Internet customers. *High Speed Internet*, COMCAST, http://security.comcast.net/constantguard (last visited Feb. 15, 2011). Additionally, Comcast advertises its service as the "easier way to back up and share your valuable files." *Id.* Verizon offers residential customers "personal Web space," with the ability to "build your own blog, business site or Web page." *Verizon High Speed Internet*, VERIZON, http://www22.verizon.com/Residential/HighSpeedInternet/Features/Features.htm (last visited Feb. 15, 2011).

[148] *See* Columbia Pictures Indus., Inc., v. Fung, No. CV 06-5578 SVW(JCx), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009).

[149] BitTorrent, as a protocol, provides its own challenges to copyright enforcement:

> BitTorrent is a protocol (a set of rules and description of how to do things) allowing you to download files quickly by allowing people downloading the file to upload (distribute) parts of it at the same time. BitTorrent is often used for distribution of very large files, very popular files and files available for free, as it is a lot cheaper, faster and more efficient to distribute files using BitTorrent than a regular download.

What is BitTorrent, BITTORRENT, http://www.bittorrent.com/btusers/what-is-bittorrent (last visited Oct. 9, 2010). A recent census of files shared via BitTorrent found that about 99% of files being shared were infringing copyrights. *See, e.g.*, Ed Felten, *Census of Files Available via BitTorrent*, FREEDOM TO TINKER (Jan. 29, 2010, 10:45 AM), http://www.freedom-to-tinker.com/blog/felten/census-files-available-bittorrent ("Overall, we classified ten of the 1021 files, or approximately 1%, as likely non-infringing, this result should be interpreted with caution, as we may have missed some non-infringing files, and our sample is of files available, not files actually downloaded. Still, the result suggests strongly that copyright infringement is widespread among BitTorrent users."); *see also* Jacqui Cheng, *BitTorrent Census: About 99% of Files Copyright Infringing*, ARS TECHNICA (Jan. 29, 2010, 1:08 PM), http://arstechnica.com/media/news/2010/01/bittorrent-census-about-99-of-files-copyright-infringing.ars ("[A]lthough there are caveats to his findings, they highlight the relationship DRM has with illegal file sharing. As in: the more DRM there is on the legit versions of the content, the more popular it is on P2P.").

[150] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

Fung[151] held that inducement to infringement would vitiate a § 512 safe harbor defense: "inducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory."[152] The court further held that Fung's inducement obviated the need for a full explication of the contributory and vicarious liability tests.[153] Here, the world of users was potentially larger and certainly more unruly than that which faced Veoh, but Fung's affirmative conduct to induce and assist copyright infringement took him well outside the intended use of § 512's safe harbors.[154]

The *Fung* court stepped through the *Grokster* analysis, beginning by distinguishing the underlying technology:

> In a BitTorrent network . . . the download process is unique from that of previous systems such as Napster and Grokster. Rather than downloading a file from an individual user, users of a bit-torrent network will select the file that they wish to download, and, at that point, the downloading will begin from a number of host computers that possess the file simultaneously.[155]

Another underlying distinction between Fung's sites and the Grokster system is that a user did not search Fung's sites for infringing files themselves, but rather for links to "dot-torrent" files that would then allow the user to begin downloading the sought-after file from multiple users.[156]

---

151 No. CV 06-5578 SVW(JCx), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009).

152 *Id.* at *18.

153 *See id.* at *15 ("Having determined that Defendants are liable under an inducement theory for their users' infringing activities, the Court refrains from addressing Plaintiff's Motion for Summary Judgment on the theories of material contributory infringement and vicarious infringement.").

154 *See id.* at *5.

155 *Id.* at *2.

156 *See id.* at *2–3.

> The advantage of BitTorrent technology is the cumulative nature of its downloading and economies of scale. As more users download a given file, there are more sources for the file pieces necessary for others. This process, whereby individuals [may] be uploading and/or downloading from many sources at any given time is known as a

Moving on to its analysis of the plaintiffs' claims, the court opted only to address the claim of inducement of copyright infringement, holding that "[d]efendants' inducement liability is overwhelmingly clear."[157] Noting that material contribution to copyright infringement and inducement are collectively referred to as "contributory liability,"[158] the court looked to *Grokster* to explain the distinction: "Generally, inducement requires that the defendant has undertaken purposeful acts aimed at assisting and encouraging others to infringe copyright,"[159] while material contribution requires that the defendant "has *actual* knowledge that *specific* infringing material is available using its system."[160]

The theory of inducement, articulated in Justice Souter's *Grokster* opinion, looks to both the intent and affirmative actions of the defendant to determine liability: "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[161] Further, specific acts of infringement need not be proven to have been induced if a defendant's overall objective is deemed "patently illegal" by a court.[162] There is no exclusive basis for such an inference by the court,[163] but rather the *Grokster* Court suggested several possible activities that could lead to this inference, including the classic instance of inducement by "advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations."[164]

> "swarm." This prevents a backlog of users waiting to download from one individual user with the source file.

Id.

157 *Id.* at *6.

158 *Id.* at *7 (citing Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 795 (9th Cir. 2007)).

159 *Fung*, 2009 WL 6355911, at *7 (citing Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 936–37 (2005)).

160 *Fung*, 2009 WL 6355911, at *7 (citation omitted).

161 *Grokster*, 545 U.S. at 936–37.

162 *Id.* at 941.

163 *Fung*, 2009 WL 6355911, at *10.

164 *Grokster*, 545 U.S. at 937.

The *Fung* court found that plaintiffs had demonstrated several categories of inducement by defendants.[165] Defendant Fung created a category and corresponding page on his IsoHunt site dedicated to "Box Office Movies," encouraging users to identify BitTorrent files that would allow other users illegally to upload copies of the twenty highest-grossing films then playing in the United States.[166] Defendants provided other browseable categories to ease the process for users looking for specific types of infringing content.[167] Defendants argued that these lists either originated from users or were the result of "automated processes that simply reflect user activity."[168] Taking a different view of the volitional conduct issue than the court in *Sony Corporation of America v. Universal City Studios, Inc.*,[169] or the Second Circuit in *Cartoon Network LP v. CSC Holdings*,[170] the *Fung* court held that:

> Defendants' assertions ignore the material fact that Defendants designed the websites and included a feature that collects users' most commonly searched-for titles. The fact that these lists almost exclusively contained copyrighted works and that Defendants never removed these lists is probative of Defendants' knowledge of ongoing infringement and failure to stop this infringement.[171]

This activity by defendants stands in stark contrast to the "substantial noninfringing uses" found in *Sony*[172] and *Cartoon Network*.[173] As in *Grokster*,[174] the *Fung* court found several

---

165 *Fung*, 2009 WL 6355911, at *11–15. These categories, enumerated as section headings, include: "Defendants' message to users," "Defendants' assistance to users engaging in infringement," "Defendants' implementation of technical features promoting copyright infringement," "Defendants' business model depends on massive infringing use," and Defendants' willful blindness ("[O]strich-like refusal to discover the extent to which its system was being used to infringe copyright"). *Id.* at *15.

166 *Id.* at *11.

167 *Id.*

168 *Id.*

169 464 U.S. 417, 437–38 (1984).

170 536 F.3d 121, 130–31 (2d Cir. 2008).

171 *Fung*, 2009 WL 6355911, at *11.

172 *Sony*, 464 U.S. at 442.

173 Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 133 (2d Cir. 2008).

instances of direct statements by Fung encouraging infringement, and attempting to justify it as a proper activity.[175] The court also accepted evidence that Fung directly assisted users when they had difficulty locating or accessing infringing material.[176] The defendants' sites, like those in *Grokster*, were funded primarily by advertising revenue, and the evidence introduced by the plaintiffs clearly showed that the search for and acquisition of infringing content was the dominant reason for users to visit the sites and view the advertising.[177]

The court then turned to the Fung defendants' asserted DMCA defenses, focusing on § 512(d)'s "information location tools" provision.[178] The court's introduction to this section, while it did not bode well for defendants, is a helpful articulation of the DMCA:

> In many ways, the Digital Millennium Copyright Act is simply a restatement of the legal standards establishing secondary copyright infringement—in many cases, if a defendant *is* liable for secondary infringement, the defendant *is not* entitled to Digital Millennium Copyright Act immunity; if a defendant *is not* liable for secondary infringement, the defendant *is* entitled to Digital Millennium Copyright Act immunity. The two sets of rules do not entirely overlap, but this framework is helpful

---

174 Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 937–40 (2005).

175 *Fung*, 2009 WL 6355911, at *12.

176 *Id.* The court also noted, briefly, that the statements themselves are not the prohibited activity, but rather serve as evidence of intent to induce. *Id.* at 13. That said, the court cites authority that such statements are not protected by the First Amendment: "The first amendment does not provide a defense to a criminal charge simply because the actor uses words to carry out his illegal purpose. Crimes . . . frequently involve the use of speech as part of the criminal transaction . . . ." *Id.* at *14 (quoting United States v. Barnett, 667 F.2d 835, 842 (9th Cir. 1982)).

177 *Id.* at *14–15. The court rejected defendant's contention that the lack of detail in plaintiffs' evidence regarding advertising revenue precluded the use of this evidence, holding that, "the present Motion involves *liability* not *damages*, so such detail is unnecessary." *Id.* at *15 n.25.

178 *Id.* at *15–18.

> for understanding the Act's statutory text and structure.[179]

In short, the DMCA will be of little help to a defendant once inducement, or another basis for secondary copyright infringement, has been sufficiently proven. As discussed above, a defendant's knowledge and affirmative activities negate each required element of the safe harbor test.

Summarizing its findings, the court held that the Fung defendants' attempts to distinguish their case from *Grokster* failed.[180] To the defendants' claim that BitTorrent is different from the technologies at issue in *Grokster*, the court held that BitTorrent "is nothing more than old wine in a new bottle."[181] Cloud computing providers and users should pay heed to this type of judicial pronouncement because it suggests that attempts to design a system intended to circumvent the hook of liability—primary or secondary—could be thwarted if the court views the underlying elements as substantially similar to existing, reviewed technology or as having the same improper aims.

Both sides in *Viacom v. YouTube* cited *Fung* in their summary judgment briefs for its discussion of inducement. Viacom uses *Fung* at various points to support its application of the *Grokster* standards on inducement, a standard requiring less evidence of affirmative inducement, as a matter of law.[182] YouTube makes a single reference to *Fung* as a narrative, factual example of prohibited conduct to illustrate the contrast with its own service.[183]

---

179 *Id.* at *15.

180 *Id.* at *19. I will not review the court's discussion of defendant's second and third arguments—(2) that its activities were protected by the First Amendment and (3) that its users are located around the world and not just in the United States. While I anticipate that many cloud computing defendants will appeal to the international nature of their user base, this argument is almost always undone by evidence of domestic infringement or domestic victims.

181 *Id.* To the extent it acknowledged a distinction in the technology, the court found BitTorrent more likely to result in liability. "Defendants' technologies appear to improve upon the previous technologies by permitting faster downloads of large files such as movies. Such an improvement quite obviously increases the potential for copyright infringement." *Id.*

182 Viacom Brief, *supra* note 139, at 25–26, 47–48, 50, 52, 55, 57, 62.

183 YouTube Brief, *supra* note 139, at 83.

YouTube continues by arguing that *Grokster* stands for the proposition that courts should "reject[] inducement claims against services that were not designed intentionally to encourage copyright infringement, even if the services could be used for infringing purposes."[184] Courts have shown, and litigants accept, that both intention in system creation and design and ongoing operating conduct factor into an analysis of the DMCA safe harbor's applicability.[185] Those engaged in copyright reform efforts should consider this issue—how these lines are to be drawn—as ripe for clarification. However, judicial application of these standards has been fairly consistent, as YouTube and Veoh have argued in court and in their briefs, thus far successfully.[186]

Carelessness can also doom a service provider's attempt to invoke the safe harbor defense. A recent case involving a website hosting company illustrates what the failure to consider § 512 in a timely fashion can do to a defense.[187] Defendant Akanoc failed to designate a § 512(c) agent until four months after the complaint in this case was filed, thus barring a safe harbor defense.[188] Additionally, though unsurprisingly, the court held that there was, at best, limited evidence of a DMCA compliance policy.[189] While here, as with Veoh, the world of users was limited and reasonable steps could be taken to prevent infringement (or at the very least comply with § 512) it is unclear that the rule illustrated in *Akanoc* is readily scalable to major web hosts. As policy discussions over copyright reform continue, a value judgment must be made at some level as to whether, and under what circumstances, copyright enforcement justifies stifling or disabling the functionality of key service providers.

Moving away from the DMCA, Cablevision's RS-DVR (remote storage-digital video recorder) provides an interesting look

---

184 *Id.*

185 *See* Viacom Int'l Inc. v. Youtube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010); Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

186 *See supra* note 168, at 28.

187 Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 97 U.S.P.Q.2d 1178 (N.D. Cal. 2010).

188 *Id.* at 1187.

189 *Id.*

at one deployment of cloud computing principles in a not-strictly-computing method. Cablevision was sued by television content owners for developing a system that allowed users to access television content stored remotely on centralized servers, operating as DVRs, owned and controlled by Cablevision. The content owners ultimately lost and the circuit court decision provides an important reading of some of the key questions in cloud computing copyright jurisprudence: namely, whether an infringing copy is created by all technical processes, who is making the copy and whether liability arises from creating the instrumentality for the copy.[190] Piggybacking off of the district court's description of the RS-DVR system, the court noted that:

> "[T]he RS-DVR is not a single piece of equipment," but rather "a complex system requiring numerous computers, processes, networks of cables, and facilities staffed by personnel twenty-four hours a day and seven days a week." To the customer, however, the processes of recording and playback on the RS-DVR are similar to that [sic] of a standard set-top DVR. Using a remote control, the customer can record programming by selecting a program in advance from an on-screen guide, or by pressing the record button while viewing a given program. A customer cannot, however, record the earlier portion of a program once it has begun.[191]

At issue was whether Cablevision engaged in impermissible copying to operate the RS-DVR system.[192]

The first question concerned the buffer data; to allow its subscribers to save programs to their respective RS-DVR accounts,

---

[190] Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 124 (2d Cir. 2008), *cert. denied sub nom*. Cable News Network, Inc. v. CSC Holdings, Inc., 129 S. Ct. 2890 (2009) ("Critically for our analysis here, plaintiffs alleged theories only of direct infringement, not contributory infringement, and defendants waived any defense based on fair use.").

[191] *Id*. at 125 (citations omitted).

[192] *Id*. at 124.

Cablevision directed part of its programming stream into a buffer system.[193]

> "No bit of data remains in any buffer for more than a fleeting 1.2 seconds. And unlike the data in cases like *MAI Systems*, which remained embodied in the computer's RAM memory until the user turned the computer off, each bit of data here is rapidly and automatically overwritten as soon as it is processed."[194]

Accordingly, the court held that the buffer data, while satisfying the embodiment prong of fixation under the Copyright Act, was not fixed for more than a transitory period, failing the duration requirement.[195] This language appears to be protective of a service provider's ability to conduct the underlying technical business of the Internet without fear of infringement liability, even where the claim is for direct infringement, not secondary. ISPs could likely make out strong cases that any copying they do, for the purposes of conveying material to a customer or conveying that material to storage at the behest of a customer, is sufficiently fleeting to satisfy a fixation analysis as seen in *Cartoon Network*. This is essential to the smooth functioning of the Internet generally and cloud computing systems specifically.

Addressing the issue of direct liability for the creation of playback copies, the court read *Netcom* as a proper gloss on § 106, rather than merely an expedient and/or outdated decision limited only to the Internet and ISP context.[196] The court focused the issue by noting that there is a dispute as to the author of the allegedly infringing copy: Cablevision or the user.[197] The court arrived at its answer by looking to the instances of volitional conduct that led to the creation of the copy: "There are only two instances of volitional conduct in this case: Cablevision's conduct in designing, housing, and maintaining a system that exists only to produce a copy, and a customer's conduct in ordering that system to produce

193 *Id.*
194 *Id.* at 129–30.
195 *Id.* at 130.
196 Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008).
197 *Id.*

a copy of a specific program."[198] Ultimately, the court analogized the RS-DVR to the VCR, holding that the customer's conduct was the relevant volitional conduct in creating the copy.[199]

This, too, is a green light for cloud computing service providers. To the extent that service providers may be pursued for direct infringement, the *Cartoon Network* decision, echoing *Netcom*[200] and *Sony Corporation of America v. Universal City Studios, Inc.*,[201] stands for the proposition that system design, though it may lead to infringement, does not expose the provider or system designer to a direct infringement claim.

IV. OUTLOOK

Recent case law paints a fairly sunny picture for service providers in the cloud computing area. So long as they operate responsibly, within the DMCA's safe harbors, and avoid actively inducing infringement, their roles as intermediaries should not subject them to liability for copyright infringement. Courts have applied this approach when reviewing the conduct of SaaS providers, such as *Veoh*, so the rule should apply all the more to PaaS and IaaS providers, who arguably have less direct interaction with and control over the content that their customers place on their systems, unless the provider induces infringement by its customers.[202]

Of course, the corollary is the dark storm clouds that face content owners as cloud computing expands and more people continue putting more content into the cloud. The DMCA and the case law interpreting it place the burden on the copyright owner to

198 *Id.*

199 *Id.*

200 Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

201 464 U.S. 417, 437–38 (1984) ("In such cases, as in other situations in which the imposition of vicarious liability is manifestly just, the 'contributory' infringer was in a position to control the use of copyrighted works by others and had authorized the use without permission from the copyright owner. This case, however, plainly does not fall in that category.").

202 *See* UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009).

identify and pursue infringement via the notice-and-takedown regime.[203] Content owners have described that effort as "ultimately Sisyphean: because [these sites are] dynamic and change[] day-to-day or hour-to-hour as users upload more material, the task of identifying and sending notifications requesting the removal of copyrighted works would create an unending [version the children's] game of 'Whack-A-Mole.'"[204] While judges, as individuals, may be sympathetic to this argument, current precedent and understanding of the DMCA suggests that this is the balance Congress knowingly struck.[205]

While there are few bright lines in this area, service providers have a solid understanding of what the law requires of them at this point, and are therefore able to comply with the DMCA's safe harbor provisions. Content owners remain dissatisfied with the existing system, but do not lack options to pursue legal action against those directly responsible for infringement.[206] That these options are unpopular with the industries' consumers is not a matter for copyright law, though it suggests an attitude towards copyright in the digital age that should factor into discussions of reform.

There are some possible changes on the horizon, in the form of proposed legislation and international agreements. News of the Anti-Counterfeiting Trade Agreement ("ACTA"), a multilateral

---

[203] *See, e.g.*, *supra* notes 98, 109, 113.

[204] UMG Brief, *supra* note 130, at 55.

[205] *See, e.g.*, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 523 (reviewing the legislative history of the DMCA and finding that, "[t]he tenor of the foregoing provisions is that the phrases 'actual knowledge that the material or an activity' is infringing, and 'facts or circumstances' indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough.").

[206] *See* Matt Richtel & Sharon Waxman, *The Media Business, Film Studios Prepare Suits on Illegal Sharing of Files*, N.Y. TIMES, Nov. 5, 2004, http://query.nytimes.com/gst/fullpage.html?res=9905E2D8143CF936A35752C1A9629C8B63 ("Hollywood's major movie studios said yesterday that they would begin filing lawsuits this month against people who make copyrighted films available for downloading over the Internet."); *Music Piracy Suit Against N.Y. Family Is Settled for $7,000*, N.Y. TIMES, Apr. 28, 2009, http://www.nytimes.com/2009/04/28/business/media/ 28piracy.html ("She was one of thousands of people sued in the Recording Industry Association of America's antipiracy campaign . . . .").

agreement that has been negotiated in secret over the last several years, started to leak to the public over the year,[207] leading to a public disclosure by the negotiating parties of a draft text.[208] During the secret negotiations, one controversial provision that leaked to the public was a "three strikes" or "graduated response" policy whereby ISPs would be required to terminate the accounts of repeat offenders or face liability themselves, a departure from the DMCA framework discussed above.[209]

The footnote containing this provision, supported by the United States and longed for by content owners and their representatives, is not present in the first publicly released draft, suggesting that it

---

[207] *See, e.g.*, Rob Pegoraro, *Copyright Overreach Goes on World Tour*, WASH. POST, Nov. 15, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/11/13/AR2009111300852.html ("An international copyright agreement, negotiated under unusual secrecy, could impose a further round of restrictions on our use of digital technology. This Anti-Counterfeiting Trade Agreement, or ACTA, represents an attempt by the United States and other countries to set common rules for violations of intellectual-property laws. The United States hopes to use ACTA to export its laws, but in the process it might have to import others."); Eric Pfanner, *Quietly, Nations Grapple With Steps to Quash Fake Goods*, N.Y. TIMES, Feb. 16, 2010, http://query.nytimes.com/gst/fullpage.html?res=9501E0DA1138F935A25751C0A9669D8B63 ("Behind a veil of secrecy, the United States, the European Union, Japan and other countries are forging ahead with plans to coordinate an international crackdown on illegally copied music, movies, designer bags and other goods that change hands in sidewalk souks and Internet bazaars.").

[208] CONSOLIDATED TEXT PREPARED FOR PUBLIC RELEASE, ANTI-COUNTERFEITING TRADE AGREEMENT, *available at* http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf; *see also* Nate Anderson, *ACTA Arrives (Still Bad, but a Tiny Bit Better)*, ARS TECHNICA (Apr. 21, 2010, 4:07 PM) http://arstechnica.com/tech-policy/news/2010/04/acta-is-here.ars [hereinafter *ACTA Arrives*] ("We've been covering the Anti-Counterfeiting Trade Agreement (ACTA) for two years now, and in that entire 24 month period no official text of the agreement has been released. Remarkable, really, given the intense scrutiny, but there you have it. Today, that all changed as the countries behind ACTA finally released a consolidated draft text of the agreement.").

[209] *See, e.g.*, David Kravets, *ACTA Draft: No Internet for Copyright Scofflaws*, WIRED (Mar. 24, 2010) (citation omitted), http://www.wired.com/threatlevel/2010/03/terminate-copyright-scofflaws ("The specific ISP policy suggested in a footnote 'is providing for the termination in appropriate circumstances of subscriptions and accounts on the service provider's system or network of repeat infringers.' This so-called 'three strikes' or 'graduated response' policy, is the holy grail of Internet-copyright enforcement, staunchly backed by the Motion Picture Association of America and the Recording Industry Association of America.").

is no longer being considered by the negotiators.[210] Shortly before the release of the draft, the European Parliament approved a resolution stating that it would not support ACTA if it contained this type of provision.[211] A provision like this, which called for "the termination in appropriate circumstances of subscriptions and accounts on the service provider's system or network of repeat infringers," would create another liability hook to be used against ISPs, as failure to terminate repeat offenders would be grounds for liability in itself.[212] The absence of such a provision suggests that, for the time being, the rules set out in *Veoh* and *Fung* regarding inducement and proper compliance with § 512 will continue to set the boundaries of the DMCA safe harbor. There is also some evidence that stricter policing of and by ISPs through the imposition of a three-strikes law will not be effective in reducing infringement.[213]

As a domestic matter, Congress created a new executive position, the United States Intellectual Property Enforcement Coordinator (IPEC) under the Office of Management and Budget, as part of the Prioritizing Resources and Organization for Intellectual Property Act of 2008.[214] The first IPEC, Victoria Espinel, was appointed in the fall of 2009, and is currently engaged in a public comment period on the issue of "Coordination and Strategic Planning of the Federal Effort Against Intellectual

---

[210] *ACTA Arrives*, *supra* note 207 ("An earlier footnote found in a leaked draft provided a single example of such a policy: 'Providing for termination in appropriate circumstances of subscriptions and accounts in the service provider's system or network of repeat infringers.' In other words, some variation of 'three strikes.' That footnote is now gone from the text entirely.").

[211] *See, e.g.*, David Kravets, *ACTA Backs Away from 3 Strikes*, WIRED (Apr. 21, 2010), http://www.wired.com/threatlevel/2010/04/acta-treaty.

[212] *Id.*

[213] Nate Anderson, *Piracy up in France After Tough Three-Strikes Law Passed*, ARS TECHNICA (Mar. 26, 2010), http://arstechnica.com/tech-policy/news/2010/03/piracy-up-in-france-after-tough-three-strikes-law-passed.ars ("According to a team of French researchers, online copyright infringement is down on P2P networks—but it's up in areas that the law doesn't cover, such as online streaming and one-click download services like Rapidshare.").

[214] *Office of the U.S. Intellectual Property Enforcement Coordinator*, WHITEHOUSE.GOV, http://www.whitehouse.gov/omb/intellectualproperty (last visited Oct. 4, 2010).

Property Infringement."[215] The Center for Democracy and Technology, an Internet civil liberties group, submitted comments with a partial focus on the issue of intermediary liability:

> Our comments also urge the IPEC to resist calls to enlist ISPs in online copyright enforcement. Congress—in the DMCA and Section 230—has expressly rejected the notion that ISPs should be responsible for policing user behavior. This policy has led to an explosion of innovative services, and it should not be undercut by—to name two increasingly popular examples—"three strikes" or filtering mandates.[216]

It is, at this point, unclear what will come out of the IPEC's public comment collection and what her next steps will be. As noted above, the removal of the "three-strikes" footnote from the ACTA draft, and the European Parliament's declared objection to it, suggests that this provision is probably dead for the time being. The IPEC could promote a revision of the DMCA that includes a version of this provision to operate only domestically, though there is no evidence to suggest that such a revision is likely. Cloud service providers should keep an eye on this process as it unfolds.

Another proposal under discussion is the Copyright Reform Act ("CRA"), championed by Public Knowledge, a "public interest organization that works to protect the rights of citizens and consumers to communicate and innovate in the digital age."[217] The CRA is being developed in five parts, the first of which, addressing fair use, was recently released.[218] Overall, the CRA aims to:

---

[215] Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement, 75 Fed. Reg. 8137 (Feb. 23, 2010).

[216] Andrew McDiarmid, *CDT Urges IP Czar to Focus on Bad Actors, Not Intermediaries*, CTR. FOR DEMOCRACY AND TECH. (Mar. 25, 2010, 1:31 PM), http://www.cdt.org/blogs/andrew-mcdiarmid/cdt-urges-ip-czar-focus-bad-actors-not-intermediaries.

[217] Jennifer M. Urban, REPORT 1 UPDATING FAIR USE FOR INNOVATORS AND CREATORS IN THE DIGITAL AGE: TWO TARGETED REFORMS, PUB. KNOWLEDGE 1 (Feb. 13, 2010), http://publicknowledge.org/pdf/fair-use-report-02132010.pdf.

[218] *Id.* Public Knowledge summarized its fair use proposal as proposing to "extend[] the list of explicitly favored uses in the preamble to section 107 of the Copyright Act to

> 1. strengthen fair use, including reforming outrageously high statutory damages, which deter innovation and creativity;
> 2. reform the DMCA to permit circumvention of digital locks for lawful purposes;
> 3. update the limitations and exceptions to copyright protection to better conform with how digital technologies work;
> 4. provide recourse for people and companies who are recklessly accused of copyright infringement and who are recklessly sent improper DMCA take-down notices; and
> 5. streamline arcane music licensing laws to encourage new and better business models for selling music.[219]

On the whole, the proposals of the CRA occupy the opposite end of the spectrum from ACTA: generally loosening copyright liability to better accommodate the actual, modern usage of technology and content. At present it is unclear whether the CRA and its advocates will play a direct role in the revision and adaptation of copyright laws in the near-term, or whether the CRA will merely occupy the time and attention of some members of the academy in coming years. Interestingly, the proposals in the CRA seek to redefine the scope of copyright itself, not to create an enforcement regime like § 512. Movement towards this type of reform would make policing more difficult for content owners because it would change the terms of what they own.

A present example can be seen in the role of "fair use" in current litigation involving YouTube. In a Summary Judgment memorandum, YouTube argues that:

> [b]ecause neither the fair use (nor the *de minimis* use) of a copyrighted work is an infringement, any

include incidental uses, non-consumptive uses, and uses that are both personal and non-commercial." Pan C. Lee, Daniel S. Park, Allen W. Wang & Jennifer M. Urban, INTRODUCTION TO THE COPYRIGHT REFORM ACT, PUB. KNOWLEDGE 8 (Feb. 13, 2010), http://publicknowledge.org/pdf/cra-introduction-02132010.pdf.

[219] *Public Knowledge Proposes New Copyright Reform Act*, PUB. KNOWLEDGE (Feb. 15, 2010), http://www.publicknowledge.org/node/2906 (internal citations omitted).

> clip for which there is even a *debatable* claim of fair use is not one that YouTube had any obligation under the DMCA to unilaterally remove. A service provider cannot lose its safe harbor simply because it might err in making what are often complex or difficult fair-use determinations.[220]

If content owners argue, as UMG and Viacom have, that service providers should police their services for infringing content, YouTube's argument—that fair use and *de minimis* copying obfuscate claims of infringement making unilateral determinations difficult if not impossible—effectively counters the implication of a duty. If the CRA successfully broadens the definition of fair use, or otherwise alters the scope of copyright, YouTube's argument is only bolstered by the increase in content that may, on its face, appear to be infringing, but, as a matter of law, is not.

None of these reform efforts fully engage the question of whether the relevant technology has changed sufficiently since 1998 to require a reexamination of the DMCA. One of the issues at the heart of both the *Veoh* and *YouTube* litigations is the characterization of the respective defendants' systems.[221] We can fairly say that in 1998 the prospect of a YouTube-style system would be unfamiliar to most people, and certainly to members of Congress. Accordingly, we have no assurance as to whether Congress might have drafted the DMCA differently if, as UMG argues, the safe harbor was only intended to protect websites, of the variety common in 1998, and not interactive sites such as YouTube.com.[222] More generally speaking, Web 2.0 services have operated entirely under the aegis of the DMCA's provisions, especially its safe harbor, and thus far courts have condoned DMCA-compliant behavior.[223]

The system designed by Cablevision, at issue in *Cartoon Network*, is another example of technological convergence that

---

220 YouTube Brief, *supra* note 139, at 53.

221 *See supra* notes 133–44 and accompanying text.

222 *See* UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2008).

223 *See, e.g.*, *id.* at 1083.

challenges the definitions drafted to support the DMCA.[224] Broadly, the prospect of full-quality television transmitted using the same Internet protocol that enabled the web was a foreign concept in 1998. While the trend of judicial decisions suggests that reevaluation and revision are not imminently needed, they raise the question of how long the underlying structure of the DMCA can last before it becomes as obsolete as the computers of the late 20th century.

CONCLUSION

With current reform efforts all in their early stages, we must look to existing statutes and judicial interpretations to assess the near-term viability of copyright enforcement in the cloud. Barring significant judicial departure from the rules applied in *Veoh*, *YouTube*, *Fung*, and *Cartoon Network*—rules based in large measure on *Grokster* and *Netcom*—the challenge lies with content owners to devise a means to better protect their rights. The situation is not as bleak as copyright owners make it out to be. The music industry has survived the creation of the mp3 format,[225] and has bested Napster and Grokster,[226] leading to greater innovation in the industry's business model. The movie industry is similarly poised to thrive, striking down the most egregious Internet pirates and using the same technology to advance its content delivery systems.[227] The last decade has shown us that those who play by the rules—those of copyright law generally and the DMCA in particular—on both sides of the field benefit. Those, like Fung, who blatantly violate rights, and aid and abet infringement by others will face the consequences, just as those, like UMG, who

---

[224] *See* Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 127–29 (2d Cir. 2008).

[225] *See* Steven Seidenberg, *The Record Business Blues*, A.B.A.J. (June 1, 2010, 4:20 AM), http://www.abajournal.com/magazine/article/the_record_business_blues.

[226] *See generally* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

[227] *See, e.g.*, *Grokster*, 545 U.S. at 913; *see also* Eric Pfanner, *Four Convicted in Sweden in Internet Piracy Case*, N.Y. TIMES, Apr. 17, 2009, http://www.nytimes.com/2009/04/18/business/global/18pirate.html.

flout the established system to pursue a more aggressive one may find themselves out in the cold.

Attempts to hook ISPs with greater liability and responsibility would disrupt the existing Internet ecosystem to a degree that could stifle overall progress for the sake of protecting mostly large-scale content owners, an effort that is unlikely to succeed in the long run. The CRA proposals may go too far towards attempting to codify the notion of Internet exceptionalism[228] in ways it has not previously been codified, but the CRA does benefit from being responsive to actual conditions, as compared with ACTA's behind-the-eight-ball attempts to over-police an area of control that has clearly slipped away from rights holders. While partisans on each side of this debate insist that a new system is necessary, the status quo regime, combining statutes and judicial precedent, has proven remarkably adaptable to the changes in the ways that Internet technologies are applied. Large-scale reforms, at present, appear both unnecessary and more likely to cause harm than to bring about improvements.

[228] Peter Margulies, *The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment*, 2004 UCLA J.L. & TECH. 4 (2004), *available at* http://www.lawtechjournal.com/articles/2004/04_041207_margulies.php ("Many prominent commentators embrace a view we can call 'Internet Exceptionalism,' which stresses distinctions between the Internet and earlier communications media such as books, newspapers, and broadcasts. Internet Exceptionalists cite a variety of the Internet's attributes, centering on the same simultaneity and absence of mediation that preoccupied courts and commentators with regard to previous technological innovations. For example, Internet Exceptionalists note how the Internet enhances consumers' ability to assemble an individualized collage of information from a variety of specialized and partisan sources, without the intercession of an intermediary, such as an editor, who may offer a broader perspective.").