Vanderbilt Journal of Entertainment & Technology Law

Volume 13
Issue 4 *Issue 4 - Summer 2011*

Article 1

2011

Is Online Copyright Enforcement Scalable?

Annemarie Bridy

ENTERTAINMENT AND TECHNOLOGY LAW

VOLUME 13 SUMMER 2011 NUMBER 4

Is Online Copyright Enforcement Scalable?

Annemarie Bridy[*]

> An algorithm, design, networking protocol, program, or other system is said to scale if it is suitably efficient and practical when applied to large situations . . . . If the design fails when the quantity increases then it does not scale. –Wikipedia

ABSTRACT

This Article examines P2P file sharing and the copyright enforcement problem it has created through the lens of scalability. Part I traces the evolution of peer-to-peer (P2P) networks from Napster to BitTorrent, with a focus on the relative scalability of successive architectures. Part II takes up the difficult question of the scale of P2P infringement and its harms, examining the strategic number-crunching that underlies industry data on piracy, the government's credulous acceptance of that data, and the risk of letting industry hyperbole drive copyright policy and law enforcement priorities. Part III evaluates the efficacy of the Digital Millennium Copyright Act (DMCA) as a policy mechanism for scaling up online copyright enforcement. I argue in Part III that the DMCA has proven to be remarkably scalable for enforcing copyrights in hosted content but has altogether failed to scale in the context of P2P file sharing, leading to the dysfunctional workaround of mass John Doe litigation. Part IV weighs the costs and benefits of more scalable alternatives to mass litigation, including a potential amendment of the DMCA's pre-litigation subpoena provision and a pair of administrative dispute resolution systems—one hypothetical, the other real—for streamlining adjudication of P2P infringement claims.

[*] © 2011 *Annemarie Bridy*. Associate Professor of Law, University of Idaho College of Law. The Author would like to thank Steve Hetcher, Daniel Gervais, and the staff of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW for organizing and hosting the Symposium for which this Article was prepared. I am also grateful to my fellow Symposium participants for their engaging presentations and to James Grimmelmann and David Post for their thoughtful comments on an earlier draft.

TABLE OF CONTENTS

In 1969, the computer network that would eventually become the Internet consisted of exactly four nodes—two on campuses in the University of California system, one at Stanford University, and one at the University of Utah.[1] By 1989, the total number of nodes on the Internet had increased to 130,000.[2] By 1999, that number had grown to 56,218,000, and by 2009 it had reached 681,064,561.[3] In the

[1] DAVID POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 30 (2009).

[2] *Internet Host Count History*, INTERNET SYSTEMS CONSORTIUM, http://www.isc.org/solutions/survey/history (last visited Feb. 22, 2011). The ISC counts hosts by counting the number of IP addresses that have been assigned a domain name. *See ISC Internet Domain Survey Background*, INTERNET SYSTEMS CONSORTIUM, http://www.isc.org/solutions/survey/background (last visited Feb. 22, 2011).

[3] *Internet Host Count History*, *supra* note 2.

roughly forty years since its inception, the Internet has doubled in size approximately every fourteen months.[4] It is now over 170 million times bigger than its original size—an astonishing growth rate by any metric. As David Post has observed, growing a network to such a size at such a rate is no easy feat: "Turning Small into Big," he explains, "can be a tricky proposition indeed, because scaling problems—the problems that arise solely as a consequence of increasing size or increasing numbers—can be profound, and profoundly difficult to solve."[5]

To make a long (and technically complicated) story short, the Internet's designers solved the problem of scale by decentralizing the transmission of data and distributing it in tiny packets throughout the entire network.[6] Because the routing function is parceled out to machines across the network, data transmission gets done much more efficiently than it would if all of the data were passing through a single, central hub.[7] As the saying goes, many hands make light work. Another key to the Internet's scalability is its capacity to grow from any point on the network. To quote Post again, "centralized networks grow radially—outward from the center, like a starfish; there's only so fast they can grow, because the center has to 'keep up' with the whole network."[8] The Internet, by contrast, "grows like a bush, each of whose terminal twigs can sprout new twigs, or like a coral reef; every machine already on the network . . . can serve as the point of attachment for a machine or machines joining the network."[9] Because the Internet can grow out from any node, "as the network grows, its ability to grow grows."[10] The bigger it gets, the bigger it can keep getting.[11]

Although its size (measured in terms of the aggregate number of nodes it interconnects) is certainly impressive, the true miracle of the Internet is its unprecedented capacity to move data fast, far, and

[4] POST, *supra* note 1, at 44.

[5] *Id.* at 60.

[6] *Id.* at 73.

[7] *Id.* at 75.

[8] *Id.* at 76.

[9] *Id.*

[10] *Id.* at 78.

[11] Despite its prodigious (and always increasing) size, though, the Internet is surprisingly navigable. In 1998, Albert-László Barabasi and two of his graduate students at Notre Dame set out to determine how many degrees of separation there were between any two documents on the World Wide Web. *See* ALBERT-LÁSZLÓ BARABASI, LINKED: THE NEW SCIENCE OF NETWORKS 34 (2002). They concluded that there was an average distance of only 19 "clicks" between any two randomly chosen URLs. *See id.* This high degree of connectivity means that the Internet, the world's largest network, is actually classifiable as a small-world network. *See id.* at 31.

wide. The trouble this capacity has caused for the owners of copyrights in digitally reproducible music and films is well known. In the process of solving one tricky problem of scale, it turns out, the Internet created another, commonly referred to in the court pleadings of copyright industry plaintiffs as "massive infringement."[12] How to approach solving *that* problem of scale, if indeed it can be solved, is the subject of this Article.

Part I traces the evolution of peer-to-peer (P2P) networks from Napster to BitTorrent, with a focus on the relative scalability of successive architectures. Part II takes up the difficult question of the scale of P2P infringement and its harms, examining the strategic number-crunching that underlies industry data on piracy, the government's credulous acceptance of that data, and the risk of letting industry hyperbole drive copyright policy and law enforcement priorities. Part III evaluates the efficacy of the Digital Millennium Copyright Act (DMCA) as a policy mechanism for scaling up online copyright enforcement without hampering the growth of Internet services and applications. I argue in Part III that the DMCA has proven remarkably scalable for enforcing copyrights in hosted content, but has altogether failed to scale in the context of P2P file sharing, leading to the dysfunctional workaround of mass John Doe litigation. Part IV weighs the costs and benefits of more scalable alternatives to mass litigation, including a potential amendment to the DMCA's pre-litigation subpoena provision and a pair of administrative dispute resolution systems—one hypothetical, the other real—for streamlining adjudication of P2P infringement claims.

I. THE SCALABILITY OF P2P NETWORKS

A. The Evolution of P2P Architectures: Both a Client and a Server Be

Like the Internet itself, P2P file-sharing networks scale well by eschewing centralization and distributing workload.[13] In a traditional

[12] *See, e.g.*, Zomba Recording LLC v. Chen, No. 5:08cv00698, 2009 U.S. Dist. LEXIS 33364, at *1-2 (N.D.N.Y Apr. 15, 2009) ("This case is one of many similar cases being litigated throughout the country, in which groups of record companies have sued individuals in an attempt to combat and deter what they perceive as massive copyright infringement over the [I]nternet."); Arista Records LLC v. Lime Group LLC, 532 F. Supp. 2d 556, 578 (S.D.N.Y. 2007) (describing LimeWire as "the operator of a peer-to-peer network that was and is, in each record company's respective judgment, a notorious vehicle for massive copyright infringement"); MGM Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 970 (C.D. Cal. 2006) ("The complaint alleged that Defendants' file sharing software contributed to massive infringement of copyrighted works owned by Plaintiffs.").

[13] *See* Yung-Ming Li et al., *Analysis of Scale Effects in Peer-to-Peer Networks*, 16 IEEE/ACM TRANSACTIONS ON NETWORKING 590, 590 (2008) ("P2P technologies have many

client-server network, the more demands there are on the server from individual clients, the fewer resources are available to the rest of the network.[14] If there is too much demand at any given time, the server will crash, and clients will no longer be able to obtain content at all.[15] P2P networks improve on the client-server model by decentralizing distribution, claiming bandwidth from edge nodes to transmit data, and thereby avoiding congestion at dedicated servers.[16] The more peer nodes there are on a P2P network at any given time, the greater the network's total capacity.[17]

The Napster file-sharing service, which launched the P2P phenomenon, maintained a central server for indexing purposes, but no files were actually stored on or transferred through it.[18] Queries were routed through the central server, which performed a matchmaking function between peers on the network, but the file transfers themselves were unmediated.[19] Subsequent file-sharing systems, including FastTrack (used by Grokster and KaZaA) and Gnutella (used by Morpheus and LimeWire), further decentralized their architectures by eliminating the central indexing server.[20] To

operational characteristics that make them appealing. First, they rely on peer nodes, not the central servers, to deliver content and therefore are more scalable."); Stephanos Androutsellis-Theotokis & Diomidis Spinellis, *A Survey of Peer-to-Peer Content Distribution Technologies*, 36 ACM COMPUTING SURVEYS 335, 336 (2004) ("[P2P] architectures are generally characterized by the direct sharing of computer resources (CPU cycles, storage, content) rather than requiring the intermediation of a centralized server . . . . Such architectures typically have as inherent characteristics scalability, resistance to censorship and centralized control, and increased access to resources.").

[14] *See, e.g.*, Shirshanka Das et al., *The Case for Servers in a Peer-to-Peer World*, 36 ACM COMPUTING SURVEYS 335 (2004), (pointing out that "[t]raditional client-server architectures are known to be ineffective in handling large correlated bursts of user demands"); Lei Liu, et al., *Experimental Investigation of a Peer-to-Peer-Based Architecture for Emerging Consumer Grid Applications*, 1 J. OPT. COMMUN. NETW. 57 (2009) (citing poor scalability and low efficiency with increasing numbers of users as negative attributes of client-server networks).

[15] Li et al., *supra* note 14, at 590–91 (describing the "flash crowd" effect, in which very large numbers of users all attempt to download a popular file at the same time, causing the server hosting the file to crash).

[16] *Id.* at 590.

[17] *Id.* (explaining that "the effective bandwidth [of a P2P network] is scalable with respect to the number of active users"). Note that the term "peer" in the technical literature on P2P file sharing refers not to the user of the networked computer, but rather to the computer itself.

[18] *See generally* A&M Records v. Napster, Inc., 239 F.3d 1004, 1012 (9th Cir. 2001) ("Software located on the Napster servers maintains a 'search index' of Napster's collective directory.").

[19] *See id.* at 1012 (describing the architecture of the Napster system).

[20] *See generally* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 921–922 (2005) (describing the architecture of the FastTrack and Gnutella networks and their relationship to defendants Grokster and Morpheus); Arista Records LLC v. Lime Group LLC, 715 F. Supp. 2d 481, 494 (S.D.N.Y. 2010) (explaining that LimeWire software provides access to the Gnutella P2P networks); UMG Recordings, Inc. v. Alburger, No. 07-3705, 2009 U.S. Dist. LEXIS 91585, at

improve search efficiency without creating a bottleneck at a central indexing server, FastTrack employed mini-indexing servers, called supernodes, dispersed throughout the network, which were responsible for indexing the contents of nodes connected to them.[21] Supernodes were designated as such for their greater bandwidth and processing power relative to other peers on the network.[22] Gnutella, which did not employ supernodes, was a truly distributed P2P system, routing queries through the network from one node to the next until a node storing the desired file could be located.[23] Gnutella's purely decentralized architecture entailed longer search and discovery times than FastTrack's hybrid architecture and was therefore less efficient.[24]

Although all of these P2P networks distributed the task of transferring data, enabling every peer to function as both a client and a server, they still suffered from inefficiencies and asymmetries created by free riding.[25] For example, one study of Gnutella found that 70 percent of nodes on the network downloaded content without ever uploading any.[26] From the point of view of scalability, free riding on a P2P network is doubly problematic: Not only does it decrease overall content availability, it also increases the workload for the nodes that *do* upload content.[27] Free riding thus produces a "tragedy of the digital commons" and effectively transforms a P2P network into a bastardized client-server network, in which some nodes decline to serve any content and act only as clients.[28] The network gets bigger without getting any richer, and its workload is poorly distributed.

B. BitTorrent: Better Scaling Through Enforced Sharing

The BitTorrent file-sharing protocol, first released in 2001, solved the problem of P2P free riding quite elegantly—by making it

*3 (E.D. Pa. Sept. 29, 2009) (explaining that KaZaA software provides access to the FastTrack P2P network).

[21] *See id.* at 921. Search bottlenecks, albeit less severe ones than occur at a central indexing server, also occur at supernodes in a hybrid P2P network. *See* Liu, et al., *supra* note 14, at 596. Li and his co-authors found that search congestion is the primary factor restricting the scalability of P2P networks. *See id.* at 600.

[22] Androutsellis-Theotokis & Spinellis, *supra* note 13, at 346.

[23] *See Grokster*, 545 U.S. at 922.

[24] Androutsellis-Theotokis & Spinellis, *supra* note 13, at 346.

[25] Liu et al., *supra* note 14, at 590.

[26] Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, FIRST MONDAY (Oct. 2, 2000), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/792/701.

[27] Liu et al., *supra* note 14, at 590.

[28] Adar & Huberman, *supra* note 26 (explaining that free-riding degrades the entire performance of the network and effectively transforms non-free-riding nodes into centralized servers).

architecturally impossible for any peer on the network to take without giving.[29] The architecture of BitTorrent, like that of FastTrack, is a hybrid P2P model.[30] File transfers occur strictly among peers, but the process requires occasional interaction with a server, called a tracker, which helps peers locate other peers offering desired content.[31] The collectivity of peers sharing a particular file at a given time according to instructions received from the tracker is called a torrent or swarm.[32] In each torrent, there are two types of peers—leechers and seeds.[33] A leecher is a peer in the process of acquiring a file.[34] A seed is a peer that already has a complete copy of the file and that remains in the torrent to serve the leechers.[35] Every torrent requires at least one seed.[36]

When a leecher requests a file, the tracker sends that peer a list of other peers, usually numbering about fifty, that are already active in the torrent transferring the requested file.[37] Of the fifty peers, the leecher adds about twenty to forty as its neighbors.[38] The leecher downloads fixed-size pieces of the requested file from these neighbors, as well as from the seed. Each leecher usually serves four neighboring peers at a time.[39] As a leecher acquires new content, it simultaneously shares its content with other leechers in the torrent.[40] Unlike a client-server network, which bogs down as traffic increases, as a torrent grows, the aggregate network bandwidth of the torrent also grows.[41] For each peer in the torrent, data transfer rates are much faster than they would be in a client-server environment.[42]

[29] *See* Christopher D. Carothers et al., A Case Study in Modeling Large-Scale Peer-to-Peer File sharing Networks Using Discrete-Event Simulation, *in* PROCEEDINGS OF THE 2006 MODELING AND SIMULATION SYMPOSIUM (2006), *available at* http://www.cs.rpi.edu/~chrisc/publications/carothers-emss-2006.pdf ("What makes BitTorrent so unique compared to past efforts is that it provides a built in mechanism to ensure the fair distribution of content and prevents selfishness on the part of peers using game theoretical 'tit-for-tat' piece distribution algorithms.").

[30] Raymond Lei Xia & Jogesh K. Muppala, *A Survey of BitTorrent Performance*, 12 IEEE COMMS. & TUTORIALS 140, 141 (2010).

[31] *Id.* at 141.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Carothers et al., *supra* note 29, at 1–2.

[41] *Id.*

[42] *Id.*

Moreover, there is no denial of service on the part of an overburdened central server, and no single source of content is overtaxed.[43]

To keep the torrent operating at maximum capacity, the BitTorrent protocol uses a process called pipelining.[44] Every active peer in a torrent maintains a continuously refreshed queue of requests for pieces, so that no connection is ever left idle after any one piece is downloaded.[45] Each peer keeps track of the download rate it gets from the other peers it serves and preferentially uploads to the peers giving it the best download rates.[46] Every ten seconds, a peer reassesses the download rates it gets from the peers to which it is connected, and if another neighboring peer offers a better download rate, it temporarily chokes off the stingy peer and opens up a connection to the more generous one.[47] This "tit for tat" mechanism ensures that peers offering little or nothing to the torrent will get little or nothing from it.[48]

Although BitTorrent's mandatory sharing functionality increases efficiency and scalability, the protocol is not without inefficiencies. One major problem in terms of optimizing network resources is that BitTorrent "neighbors" are neighbors in name only; the protocol selects them randomly rather than based on their proximity to the requesting user.[49] This location-unaware selection mechanism prolongs download times and over-consumes bandwidth.[50] While the former problem may represent little more than an inconvenience to users, the latter is a source of loud complaint from Internet Service Providers (ISPs), which have controversially resorted to bandwidth-shaping to limit the load of BitTorrent traffic on their networks.[51] For ISPs, then, as well as copyright owners, the scaling

[43] *Id.*

[44] Xia & Muppala, *supra* note 30, at 141.

[45] *See id.*

[46] *Id.* at 142.

[47] *Id.*

[48] *See id.* ("This mechanism is very important to encourage contributors and punish free-riders, thus preventing leechers from downloading without contributing anything."). *But see id.* at 145 (citing a study by Andrade et al., which concluded that although the tit-for-tat protocol discourages free-riding successfully, the mechanism may not work as well if there is a large number of seeds in the torrent).

[49] *See id.* at 140 (identifying BitTorrent's random neighbor selection mechanism as one of the most widely criticized aspects of the protocol).

[50] *Id. see also* Sixto Ortiz, Jr., *Proponents Try to Rehabilitate Peer-to-Peer Technology*, 41 IEEE COMPUTER 16, 17 (2008) ("Currently, P2P services don't generally calculate the best route to use to transmit data and thus sometimes use peers that are far from one another, increasing latency and bandwidth consumption.").

[51] *See generally* Annemarie Bridy, *Why Pirates (Still) Won't Behave: Regulating P2P in the Decade After Napster*, 40 RUTGERS L.J. 565, 598–600 (2009) [hereinafter Bridy, *Pirates*] (discussing the Comcast torrent throttling controversy). Although the FCC sanctioned Comcast

up of BitTorrent networks has come at a price, though lack of reliable data makes it difficult to know how high a price or exactly how high a proportion of overall network traffic P2P transfers represent.[52]

One study conducted from 2008 to 2009, which did not include ISPs in the United States, concluded that P2P traffic generated the highest percentage of overall network traffic in all regions studied, ranging from 43 percent in Northern Africa to 70 percent in Eastern Europe.[53] (These percentages were down from a previous study in 2007, but the absolute volume of P2P traffic did not decline.)[54] The same study found that BitTorrent dominated all other protocols, including HTTP, the protocol that carries ordinary web-browsing traffic.[55] A 2009 study of Digital Subscriber Line (DSL) traffic on a major European ISP found the percentage of P2P traffic to be much lower—roughly 14 percent.[56] The authors of the 2009 study also found, however, that P2P users have longer sessions than non-P2P users, and that a larger percentage of P2P users are always connected.[57] This pair of findings from the 2009 study suggests that P2P users are more demanding of resources than their non-P2P counterparts.

To make the BitTorrent protocol even more efficient and less bandwidth intensive, computer scientists have been working on design

for discriminating against traffic solely on the basis of protocol, the U.S. Court of Appeals for the D.C. Circuit subsequently overturned the sanction, holding that the FCC is without jurisdiction to regulate traffic management by cable broadband providers. *See* Comcast Corp. v. Fed. Commc'ns Comm'n, 600 F.3d 642, 650 (2010); Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81, 112–14 (2010) [hereinafter Bridy, *Response*] (discussing the regulatory state of play for wire line broadband providers following the D.C. Circuit's decision in Comcast).

[52] *See* Bridy, *Pirates*, *supra* note 51, at 597 n.171 (discussing the difficulty of ascertaining how much network congestion is caused by P2P traffic); *see also* Peter J. Sevcik, *Peer-to-Peer Traffic: Another Internet Myth is Born*, BUS. COMMS. REV., Nov. 1, 2005, at 2, *available at* http://www.netforecast.com/Articles/BCR%20C42%20Peer-to-Peer%20Traffic.pdf (trying to assess the validity of a claim that P2P transfers accounted for 60% of all ISP traffic and concluding that "there is enough conflicting data and confusion over how to measure and report the data that no general conclusions should be drawn.").

[53] HENDRIK SCHULZE & KLAUS MOCHALSKI, IPOQUE INTERNET STUDY 2008/2009, at 2 (2009), *available at* http://www.ipoque.com/userfiles/file/ipoque-Internet-Study-08-09.pdf. The authors found significant differences over the eight regions that were studied: Northern Africa, Southern Africa, Middle East, Southern Europe, Southwestern Europe, and Germany. *Id.* at 1.

[54] *Id.* at 2 (reporting the percentage decline from 2007); *id.* at 5 (explaining that the percentage decline was not matched by a decline in absolute volume, because other protocols experienced percentage increases over the same period).

[55] *Id.* at 5.

[56] Gregor Maier et al., On Dominant Characteristics of Residential Broadband Internet Traffic, *in* IMC '09: PROCEEDINGS OF THE 2009 ACM SIGCOMM INTERNET MEASUREMENT CONFERENCE (2009), *available at* http://www.icir.org/gregor/papers/imc09-residential-traffic.pdf (finding that HTTP traffic, not P2P traffic, dominates).

[57] *Id.* at 92.

modifications that localize peer selection and introduce other resource-saving mechanisms, including more efficient file location, into the architecture.[58] In addition, a consortium of major telecommunications providers and P2P companies—the P4P Working Group—was formed in 2007 to improve resource utilization on P2P networks by promoting real-time communication between P2P applications and the ISP infrastructures on which they run.[59] With improved communication between P2P applications and ISP networks, the need for ISPs to resort to extreme traffic management measures like throttling or protocol blocking can be diminished, and the legitimate commercial potential of P2P as a means of content distribution can be realized.

C. P2P Past Its Peak: The Recentralization of Online Infringement

While studies attempting to measure P2P traffic reach different conclusions on the numbers, they agree that recent traffic trends show more growth elsewhere, particularly in the HTTP protocol.[60] The resurgence of HTTP has several causes: The increased popularity of streaming media and video-on-demand sites (e.g., YouTube, Hulu, and Netflix); the explosion of social networking sites (e.g., Facebook, LinkedIn, Twitter); and the migration of users to online file-hosting services, known as cyberlockers or Direct Download Links (DDLs) (e.g., Megaupload and RapidShare).[61] A 2010 forecast by Cisco Systems predicts that although P2P traffic will continue to grow in volume at an annual rate of 16 percent through 2014, it will

[58] *See, e.g.*, Carothers et al., *supra* note 29, at 1 (reporting the creation of a highly scalable simulation model that requires 30 to 1000 times less memory per peer than operational BitTorrent software); Lu Liu et al., *Efficient and Scalable Search on Scale-Free P2P Networks*, 2 PEER-TO-PEER NETW. APPL. 98, 98 (2009) (reporting on the development of a P2P search protocol that improves on existing models by considering both the number of shared files and the connectivity of each neighboring node in the network); Xia & Muppala, *supra* note 30, at 151 (summarizing the results of studies in which researchers have sought to optimize peer selection in a variety of ways).

[59] P4P is an initiative of the Distributed Computing Industry Association (DCIA) and counts among its members broadband providers, including Verizon, Comcast, and AT&T, and P2P software distributors, including BitTorrent. *See P4P Working Group (P4PWG) Membership*, DISTRIBUTED COMPUTING INDUSTRY ASS'N, http://www.dcia.info/activities/p4pwg/membership.html (last visited Feb. 22, 2011). "P4P stands for proactive network provider participation for P2P, or provider portal for P2P. The objectives of P4P are to (1) facilitate network applications, in particular P2P applications, to achieve the best possible application performance under efficient and fair usage of network resources; and (2) allow network providers to achieve efficient and fair usage of their resources to satisfy application requirements, reduce cost, and increase revenue." HAIYONG XIE ET AL., P4P: EXPLICIT COMMUNICATIONS FOR COOPERATIVE CONTROL BETWEEN P2P AND NETWORK PROVIDERS 2 (2007), *available at* http://www.dcia.info/documents/P4P_Overview.pdf.

[60] *See* SCHULZE & MOCHALSKI, *supra* note 53, at 2–3; Maier et al., *supra* note 56, at 90.

[61] *See* SCHULZE & MOCHALSKI, *supra* note 53, at 11–12; Maier et al., *supra* note 56, at 96.

drop over the same period to only 17 percent of total consumer Internet traffic.[62] Traffic on file-hosting services, by comparison, is expected to grow about three times faster.[63] In a recent filing with the FCC, the Motion Picture Association of America (MPAA) described the proliferation of file-hosting sites as a manifestation of increasing fragmentation in the online market for infringing content.[64] The International Federation for the Phonographic Industry (IFPI) made a similar observation about fragmentation in its 2010 Digital Music Report, citing a U.K. study which found that although P2P remains the major platform for online piracy, illegal distribution through other channels, including Usenet groups and cyberlockers, grew significantly in 2009.[65]

Cyberlocker sites rely on a centralized architecture and thus seem to represent a step backwards in the evolution toward completely distributed networks.[66] This recentralization makes life easier for copyright owners, because centralized content distribution systems, unlike distributed ones, provide static and easily identifiable targets for litigation and other enforcement efforts.[67] When a system is as large, dynamic, and decentralized as a P2P network, trying to shut it down by targeting individual nodes is a losing proposition.[68] Some nodes will be more connected than others, and destruction of these highly connected nodes will be relatively more damaging to the network as a whole, but a very large distributed network will survive

[62] CISCO SYS., INC., CISCO VISUAL NETWORKING INDEX: FORECAST AND METHODOLOGY 2009–2014, at 2 (2010) [hereinafter CISCO FORECAST 2009–2014]. At the end of 2009, P2P traffic accounted for 39% of total consumer Internet traffic. *Id.* At the end of 2008, it accounted for 50%. CISCO SYS., INC., CISCO VISUAL NETWORKING INDEX: FORECAST AND METHODOLOGY 2008–2013, at 2 (2009).

[63] CISCO FORECAST 2009–2014, *supra* note 62, at 2 (projecting an annual growth rate of 47% in file sharing).

[64] MOTION PICTURE ASS'N OF AM., INC., REPLY COMMENTS IN THE MATTER OF PRESERVING THE OPEN INTERNET AND BROADBAND INDUSTRY PRACTICES 13–14 & n.32 (Apr. 26, 2010), *available at* http://www.mpaa.org/Resources/46ba617a-4dc9-4fdb-acce-9100ac274af4.pdf.

[65] INT'L FED'N OF THE PHONOGRAPHIC INDUS., IFPI DIGITAL MUSIC REPORT 6 (2010), *available at* http://www.ifpi.org/content/library/DMR2010.pdf.

[66] *See* J.A. Pouwelse et al., *Pirates and Samaritans: A Decade of Measurements on Peer Production and Their Implications for Net Neutrality and Copyright*, 32 TELECOMM. POL'Y 701, 706 (2008) (characterizing the development of post-P2P content-sharing systems that rely on centralized architecture—for example, YouTube—as an evolutionary step backwards).

[67] As Jonathan Zittrain has pointed out, "[t]hose seeking to block the illegal content must pressure the entity within the chain of data transfer whose selection maximizes the chances of both legal responsibility and successful enforcement." Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 658 (2003). This process becomes relatively easy when all of the illegal content resides in one place under the control of one entity.

[68] *See* Andrés Guadamuz González, *Scale-Free Law: Network Science and Copyright*, 70 ALB. L. REV. 1297, 1316 (2007) (explaining that scale-free networks, including P2P networks, are robust and stable, in part because most of the nodes are not hubs, so an attack on any one node is unlikely to have any impact on the network as a whole).

the targeting of individual nodes, and its connections will simply reroute around the failure.[69] A defining feature of distributed networks, including the Internet itself and the P2P networks that overlay it, is their resiliency in the face of failure or attack.[70] This resiliency is one key to their scalability.

II. THE SCALE OF P2P INFRINGEMENT AND ITS HARMS

A. *"Massive Infringement" as a Rhetorical Construct*

The use of adjectives denoting great scale (e.g., terms like "vast" and "massive") to describe the problem of P2P piracy has long been a rhetorical strategy of the copyright industries, which have thereby sought to impress upon legislatures and courts both the magnitude of the problem they face and the need for urgent and decisive action.[71] Although not particularly subtle, the strategy has been quite effective, judging from the number of court decisions that incorporate the industry's scale-conscious rhetoric. The cases against P2P software distributors going back to *A&M Records v. Napster* are strewn with references to the "massive" scale of P2P infringement.[72]

[69] *See id.* at 1316–18 (suggesting that targeting of supernodes or hubs might be more successful than random attacks).

[70] *See id.* at 1316.

[71] The IFPI's annual digital music reports provide a nice longitudinal sample of how this strategy has been deployed. *See* INT'L FED'N OF THE PHONOGRAPHIC INDUS., *supra* note 65, at 5 (referring to "the vast number of people who currently do not pay for music they consume"); INT'L FED'N OF THE PHONOGRAPHIC INDUS, IFPI, DIGITAL MUSIC REPORT 22 (2009) [hereinafter 2009 DIGITAL MUSIC REPORT], *available at* http://www.ifpi.org/content/library/dmr2009.pdf (arguing that "the vast scale of unauthorised music consumption is massively damaging investment in music and the careers of artists"); INT'L FED'N OF THE PHONOGRAPHIC INDUS, IFPI, DIGITAL MUSIC REPORT 21 (2008) [hereinafter 2008 DIGITAL MUSIC REPORT], *available at* http://ifpi.org/content/library/dmr2008.pdf (asserting the need for "a system for curbing mass copyright infringement"); *id.* at 22 (describing the "vast bulk" of P2P traffic as infringing); *id.* at 8 (lamenting "massive unauthorised distribution"); INT'L FED'N OF THE PHONOGRAPHIC INDUS, IFPI, DIGITAL MUSIC REPORT 18 (2007), *available at* http://ifpi.org/content/library/dmr2007.pdf (stating that "Limewire and BitTorrent continued to be massive carriers of copyright theft" in 2006); *id.* at 12 (warning that social networking sites should not use innovation "as an excuse . . . to practice massive copyright infringement"); INT'L FED'N OF THE PHONOGRAPHIC INDUS, IFPI, DIGITAL MUSIC REPORT 18 (2006), *available at* http://ifpi.org/content/library/digital-music-report-2006.pdf (warning that "P2P services cannot simply turn a blind eye . . . and profit from massive infringement"); INT'L FED'N OF THE PHONOGRAPHIC INDUS, IFPI, DIGITAL MUSIC REPORT 18 (2005), *available at* http://www.ifpi.org/content/library/digital-music-report-2005.pdf (describing P2P file sharers as "large-scale distributors of unauthorized files"); INT'L FED'N OF THE PHONOGRAPHIC INDUS, IFPI, DIGITAL MUSIC REPORT 8 (2004), *available at* http://ifpi.org/content/library/digital-music-report-2004.pdf (stating that the "vast bulk" of music consumed online is unlicensed).

[72] *See, e.g.,* Arista Records LLC v. Lime Group LLC, No. 06-cv-5936, 2010 WL 2291485, at *17 (S.D.N.Y. May 25, 2010) (holding that "[t]he massive scale of infringement committed by LimeWire users, and LW's knowledge of that infringement, supports a finding that

In *MGM Studios, Inc. v. Grokster, Ltd.*, Justice Souter wrote of the "gigantic scale" and "staggering" scope of the alleged infringement.[73] Similar language permeates the cases against individual file-sharers. In *Elektra Entertainment Group, Inc. v. Bryant*, for example, the court wrote that "the process [of P2P file sharing] is potentially exponential rather than linear, threatening virtually unstoppable infringement of the copyright."[74] In *Twentieth Century Fox Film Corp. v. Streeter*, the court described P2P technology as leaving the plaintiffs' works "vulnerable to massive, repeated, and worldwide infringement."[75] When it comes to online infringement, the industry's clarion message has been that scale changes everything: If the problem were smaller and more localized—if the potential losses were not so easily multiplied—the situation would be much less dire for industry plaintiffs, and the need for immediate relief less acute.

The copyright industries have targeted Congress, as well as the courts, with the message that size matters. Transcripts of legislative hearings on file sharing are full of scale-conscious language. In this context, members of the House Judiciary Committee have characterized file sharing as an "epidemic,"[76] citing dramatic statistics to prove its "devastating impact" on the entertainment industry.[77] In testimony before the Senate Judiciary Committee supporting passage of the Intentional Inducement of Copyright Infringements Act of 2004, Register of Copyrights Marybeth Peters accused P2P software distributors of using P2P technology to "create vast global networks of

LW intended to induce infringement"); MGM Studios, Inc. v. Grokster, Ltd., 518 F. Supp. 2d 1197, 1217 (C.D. Cal. 2007) (referring to "undisputed evidence at summary judgment of massive end-user infringement"); *id.* at 1224 (referring to a prior holding that "StreamCast's business model depended upon massive infringement"); *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 638 (N.D. Ill. 2002) (describing the Aimster service as one "whose very raison d'[ê]tre appears to be the facilitation of and contribution to copyright infringement on a massive scale"); *id.* at 649 (referring to "the ongoing, massive, and unauthorized distribution and copying of Plaintiffs' copyrighted works"); A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 901 (N.D. Cal. 2000) (referring to "the massive downloading of MP3 files by Napster users"); *id.* at 925 (finding that "the evidence establishes that unauthorized sharing of plaintiffs' copyrighted music occurred on a massive scale"); *id.* at 926 (citing "statistical evidence of massive, unauthorized downloading and uploading of plaintiffs' copyrighted works").

[73] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 940 (2005) (finding that MGM presented "evidence of infringement on a gigantic scale"); *id.* at 923 (concluding that "the probable scope of copyright infringement is staggering").

[74] No. CV 03-6381, 2004 WL 783123, at *7 (C.D.Cal. Feb. 13, 2004).

[75] 438 F. Supp. 2d 1065, 1073 (D. Ariz. 2006).

[76] *Reducing Peer-to-Peer (P2P) Piracy on University Campuses: A Progress Update: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Prop. of the H. Comm. on the Judiciary*, 109th Cong. 79 (2005) [hereinafter *Hearing*].

[77] *Id.* at 12–65. Rep. Howard Berman (CA) opened the hearing with the following statistics: "In March 2005 alone, 243 million songs were downloaded from illicit peer-to-peer services. It's estimated that approximately 400,000 films are illegally downloaded every day." *Id.*

copyright infringement."[78] Testifying a few years later before the House Judiciary Committee, Cary Sherman of the Recording Industry Association of America (RIAA) described file sharing on university campuses as a "massive assault."[79] Summing up his industry's losses, Sherman alleged harms at once calculably and incalculably great: "billions of dollars in lost sales, thousands of lost jobs, countless lost career opportunities."[80] This official message of titanic loss has been so consistent over time, and delivered so often to so many audiences, that it is now taken for granted from hearing rooms to court rooms to news rooms. There is garden variety infringement, the industries' logic goes, but then there is "massive infringement," for which the Internet is to blame and which differs so much in degree from what came before that it begs to be treated as different in kind.

B. The Challenge of Measuring Massive Infringement

As with estimates of P2P traffic as a proportion of total Internet traffic, estimates of infringing traffic as a proportion of total P2P traffic have varied over time and among sources. In the literature on P2P, much of it authored by trade groups representing corporate rights owners, a commonplace claim is that piracy accounts largely, if not overwhelmingly, for the traffic on P2P networks.[81] P2P plaintiffs have repeatedly made this claim, and courts have generally found it to be vindicated by credible evidence, including expert testimony. MGM's expert statistician in *Grokster* found that nearly 90 percent of the files available on the FastTrack system were copyrighted, and the Court was persuaded that the "vast majority" of downloads were, in fact, infringing.[82] More recently, the court in *Arista Records LLC v. Lime Group LLC* credited Arista's expert's testimony that 98.8 percent of the files requested for download on the LimeWire system were copyrighted and not authorized for free

[78] *Protecting Innovation and Art While Preventing Piracy: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. 5 (2004) (statement of the Hon. Marybeth Peters, Register of Copyrights).

[79] *An Update: Piracy on University Networks: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Prop. of the H. Comm. on the Judiciary*, 110th Cong. 9 (2007) [hereinafter *Hearing II*] (testimony of Cary Sherman, President, RIAA).

[80] *Id.*

[81] *See, e.g.*, DANIEL CASTRO ET AL., STEAL THESE POLICIES: STRATEGIES FOR REDUCING DIGITAL PIRACY 2 (2009) *available at* http://www.itif.org/files/2009-digital-piracy.pdf (asserting that unauthorized distribution of copyrighted content has become "the principal use of [P2P] technology, although such networks are occasionally used to distribute legal content"); 2009 DIGITAL MUSIC REPORT, *supra* note 65, at 22 (claiming that "file-swapping of copyrighted music and movies is widely acknowledged to account for a large part of P2P activity").

[82] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 922–23 (2005).

distribution.[83] In *Columbia Pictures v. Fung*, a case involving secondary infringement claims against the operators of the isoHunt and TorrentBox torrent tracker sites, Columbia's expert testified that over 90 percent of the downloads available through the sites were copyright protected.[84] In a decision granting Columbia's motion for summary judgment, the court found that the defendant, Fung, had failed to call the opposing expert's conclusions into doubt or to rebut the expert's statement that he relied on standard statistical sampling techniques to arrive at the numbers in his report.[85] Even if the percentages were not actually as high as the expert reported, the court said, there was no question that a substantial percentage of the available files were infringing—enough to prove the plaintiff's claims.[86]

Outside the context of expert testimony and industry white papers, data on the percentage of P2P traffic that is copyright infringing are difficult to locate, but the available data tend to corroborate industry assertions that the bulk of files available on P2P networks are infringing.[87] Australian researchers from the University of Ballarat reported in 2010 that 89 percent of all torrents—97.9 percent of all non-pornographic torrents—in a sample of over one million were infringing.[88] Of the torrents in the top three categories by volume—movies, TV shows, and music—there were no legal torrents in the study's sample.[89] To highlight the difficulty of finding truly independent statistics, it is worth noting that the study, though released under the auspices of the Internet Commerce Security Laboratory, was supported by a major Australian movie and DVD distributor.[90] In a smaller study, apparently without industry ties, a student researcher at Princeton University found that all of the movie, TV, and music torrents in a sample consisting of 1021 files were likely

[83] Arista Records LLC v. Lime Group LLC, No. 06-cv-5936, 2010 WL 2291485, at *51 (S.D.N.Y. May 25, 2010).

[84] Columbia Pictures Indus. v. Fung, No. CV06-5578, 2009 U.S. Dist. LEXIS 122661, at *17 (C.D. Cal. Dec. 21, 2009).

[85] *Id.*

[86] *Id.* at *18–19.

[87] *See, e.g.*, 2008 DIGITAL MUSIC REPORT, *supra* note 71, at 22 ("Independent estimates suggest up to 80 per cent of internet traffic is generated by P2P file distribution, the vast bulk of which is unauthorised [sic] use of copyrighted music and movies.").

[88] *See* ROBERT LAYTON & PAUL WATTERS, INVESTIGATION INTO THE EXTENT OF INFRINGING CONTENT ON BITTORRENT NETWORKS 1, 21 (2010), *available at* http://www.afact.org.au/research/bt_report_final.pdf.

[89] *Id.* at 1.

[90] The study was funded by Village Roadshow. *Id.* It is prominently featured on the home page of AFACT—the Australian Federation Against Copyright Theft. *See* AUSTRALIAN FED'N AGAINST COPYRIGHT THEFT, http://www.afact.org.au (last visited Feb. 23, 2011).

infringing.[91] Only 1 percent of the files in the sample, which also included video games, software, books, and pornography, were classified as likely non-infringing.[92]

C. The Challenge of Measuring Massive Infringement's Harms

Reliable and independent numbers are even more elusive when it comes to measuring file sharing's economic impact on the copyright industries and the U.S. economy as a whole. The claims made by industry representatives are, not surprisingly, quite dramatic. In comments to the FCC in 2010, the MPAA asserted that online infringement costs U.S. creative industries billions of dollars and hundreds of thousands of jobs annually.[93] A 2007 study often cited by industry trade groups estimated annual losses on the same order of magnitude: $58 billion in total output, over 370,000 jobs, and $2.6 billion in tax revenue.[94]

These estimates, the methodologies that produced them, and the assumptions on which they rely have been challenged on their merits[95] and countered by at least one major study whose authors attempted to look at the other side of the coin, assessing the value added to the economy by industries that rely on fair uses of copyrighted works.[96] As required by the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act), the General Accounting Office (GAO) examined existing research on the economic effects of counterfeiting and piracy.[97] In a report released in

[91] *See* 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 (summarizing the results of the study by Princeton senior Sauhard Sahi).

[92] *Id.*

[93] MOTION PICTURE ASS'N OF AM., INC., *supra* note 64, at 5–6.

[94] *See* STEPHEN E. SIWEK, INST. FOR POLICY INNOVATION, THE TRUE COST OF COPYRIGHT INDUSTRY PIRACY TO THE U.S. ECONOMY (2007), Siwek's data is from 2005. *Id.*

[95] *See* COMPUTER & COMMC'NS INDUS. ASS'N, COMMENTS ON THE JOINT STRATEGIC PLAN 6–36 (Mar. 24, 2010), *available at* http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000334/NC-CCIA_IPEC_Comments.pdf (arguing that industry estimates of piracy losses reflect nine different fallacies).

[96] *See* THOMAS ROGERS & ANDREW SZAMOSSZEGI, FAIR USE IN THE U.S. ECONOMY 9 (2010), *available at* http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000354/fair-use-study-final.pdf ("The fair use economy in 2007 accounted for $4.7 trillion in revenues and $2.2 trillion in value added, roughly one-sixth of total U.S. GDP. It employed more than 17 million people and supported a payroll of $1.2 trillion. Fair use companies generated $281 billion in exports and rapid productivity growth.").

[97] *See* Prioritizing Resources and Organization for Intellectual Property Act of 2008, Publ. L. No. 110-403, § 501, 122 Stat. 4256 (directing the GAO to "conduct a study to help determine how the Federal Government could better protect the intellectual property of manufacturers by quantification of the impacts of imported and domestic counterfeit goods on . . . the overall economy of the United States.").

2010, the GAO concluded that economic loss estimates widely cited by the government could not be substantiated due to the absence of underlying studies.[98] In attempting to discover the origin of the estimates, the GAO learned from government officials that the numbers came directly from industry;[99] they were neither independently reviewed nor supported by any disclosure of data or methodology.[100] To all appearances, corporate rights owners have been laundering their loss statistics to win support for their legislative and enforcement agendas: They submit estimates to government officials, who uncritically quote the estimates in government documents, which industry representatives then quote to the media as official proof of the losses piracy causes.[101] By means of this circuit, numbers based on questionable assumptions and emanating from sources with a vested interest in their inflation acquire a false air of objectivity and empirical soundness. Because policy and enforcement apparatuses informed by skewed statistics are bound to produce skewed priorities and initiatives, the GAO report should stand as a reminder to policy makers of the need for disinterested data gathering and assessment.

There is, however, some truth behind the hype. Notwithstanding the copyright industries' propensity to exaggerate their losses, or the fastness and looseness with which their statistics are (re)circulated by uncritical government officials and media outlets, there can be little question that P2P networks have facilitated large-scale infringement, or that the volume of files traded illegally by means of such networks has been, and remains, large and revenue-depleting. As the GAO concluded, without factitious precision, "the problem is sizeable."[102]

[98] GENERAL ACCOUNTING OFFICE, INTELLECTUAL PROPERTY: OBSERVATIONS ON EFFORTS TO QUANTIFY THE ECONOMIC EFFECTS OF COUNTERFEIT AND PIRATED GOODS 18 (2010), *available at* http://www.gao.gov/new.items/d10423.pdf.

[99] *Id.* at 16 ("Commerce and FBI officials told us they rely on industry statistics on counterfeit and pirated goods and do not conduct any original data gathering to assess the economic impact of counterfeit and pirated goods on the U.S. economy or domestic industries.").

[100] *Id.* (explaining that "industry associations do not always disclose their proprietary data sources and methods, making it difficult to verify their estimates.").

[101] *Id.* at 18 (explaining how the process worked with respect to a 2002 FBI press release).

[102] *Id.* at 15.

III. THE DMCA AND THE SCALABILITY OF ONLINE ENFORCEMENT

A. *"Scaling Up" Enforcement to Facilitate Growth*

The legislative history of the DMCA frames the statute as a means of ensuring the continued global growth of the Internet.[103] To facilitate that goal, the statute was crafted to minimize obstacles to growth for both content providers, who would not expand the digital distribution of their works without assurances that they would be protected from "massive piracy," and service providers,[104] who would not expand their sites and networks without assurances that they would be protected from massive liability for copyright infringement.[105] In light of the legislative history's focus on promoting Internet growth, the DMCA can be understood as a mechanism for simultaneously scaling up online copyright enforcement and scaling back online copyright liability—a unified solution designed to give rights owners the security necessary to expand content distribution and service providers the security necessary to expand applications and network infrastructure.

The DMCA scales up enforcement while scaling back liability through provisions in Title I that prohibit circumvention of technological protection measures[106] and provisions in Title II that create safe harbors for service providers, conditioned on their assisting rights owners in the expeditious resolution of online copyright infringement disputes.[107] There are two provisions from Title II on which copyright owners have relied heavily in their efforts to make enforcement scale for the digital environment: § 512(c), which establishes the notice-and-takedown framework for which the DMCA is most well-known,[108] and § 512(h), which allows rights owners to

[103] *See* S. REP. NO.105-190, at 1–2 (1998) ("The 'Digital Millennium Copyright Act of 1998' is designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.").

[104] In the statute, the term "service provider" is defined broadly to include both providers of Internet access (ISPs) and providers of online services. *See* 17 U.S.C. § 512(k) (2006).

[105] *See* S. REP. NO.105-190, at 8 ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy. . . . At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet.").

[106] *See* 17 U.S.C. § 1201.

[107] *See* 17 U.S.C. § 512(a)–(d). As Edward Lee has noted, Title I expands copyright liability, while Title II contracts it. Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 233 (2009).

[108] *See* 17 U.S.C. § 512(c); *see also* Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices under Section 512 of the Digital Millennium Copyright*

serve subpoenas on service providers outside of litigation to obtain the identities of alleged infringers.[109] Tacitly premised on the reality that litigation is not an efficient means of resolving the voluminous infringement claims that arise in the context of online services, § 512(c) and § 512(h) require service providers to act cooperatively with rights owners, without intervention from a court, to remove allegedly infringing content from their services and to identify those ostensibly responsible for its distribution.

B. The DMCA's Scalability for Hosted Content

Notwithstanding initial resistance from both camps, service providers and rights owners have adapted quite well over the last decade to doing business within the parameters defined by the DMCA's notice-and-takedown system.[110] On YouTube, for example, the § 512(c) notice process is fully automated for both individual and corporate rights owners.[111] Facebook also offers a standardized online notice form,[112] and Scribd provides DMCA-compliant templates for both notices and counter-notices.[113] On these popular content-sharing sites, the notice-and-takedown system has come to operate as a well-oiled, always-on copyright enforcement machine.

Notwithstanding this fact, corporate rights owners have argued since the DMCA's enactment, and more loudly since the dawn of Web 2.0 and the user-generated content (UGC) revolution, that the notice-and-takedown machinery in the DMCA is inadequate to protect their

Act, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 624–31 (2006) (giving a detailed explanation of the mechanics of notice and takedown under the DMCA).

[109] *See* 17 U.S.C. § 512(h) ("A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer . . . . The request may be made by filing with the clerk . . . a copy of a notification described in subsection (c)(3)(A); a proposed subpoena; and a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.").

[110] *See* Jerome H. Reichman, Graeme B. Dinwoodie, & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 994 (2007) (concluding that "the past decade of experience with the DMCA notice and takedown regime suggests that a relatively balanced and workable solution to this particular dual-use technology problem has been found.").

[111] *See Content Management*, YOUTUBE, http://www.youtube.com/t/dmca_policy (last visited Oct. 5, 2010).

[112] *See DMCA Notice of Copyright Infringement*, FACEBOOK, https://www.facebook.com/legal/copyright.php?copyright_notice=1 (last visited Feb. 22, 2011).

[113] *See DMCA Copyright Infringement Takedown Notification Template*, SCRIBD http://support.scribd.com/forums/33563/entries/22980 (last visited Oct. 19, 2010); *DMCA Counter-Notification Template*, SCRIBD, http://support.scribd.com/forums/33563/entries/22993 (last visited Oct. 19, 2010).

rights.[114] Viacom has pressed this argument, so far unsuccessfully, in its closely watched lawsuit against YouTube.[115] In an opinion granting YouTube's motion for summary judgment based on the company's consistent compliance with the terms of the DMCA's safe harbor provisions, the court rejected Viacom's contention that the notice-and-takedown system is an enforcement failure.[116] On the contrary, the court concluded, evidence in the record suggested that the system is both functional and efficient: "Indeed, the present case shows that the DMCA notification regime works efficiently: When Viacom over a period of months accumulated some 100,000 videos and then sent one mass take-down notice on February 2, 2007, by the next business day YouTube had removed virtually all of them."[117]

Viacom's power to eliminate 100,000 instances of alleged infringement overnight, with a single notice, is a testament to the DMCA's success in making online enforcement scalable without creating growth-inhibiting burdens for online services like YouTube, whose business models are founded on content sharing. Although copyright owners continue to advocate a judicial interpretation of the DMCA that would require sites like YouTube to be more proactive in their efforts to enforce third-party copyrights, the DMCA is quite clear that active monitoring for infringing content is not a burden that

[114] *See, e.g.*, Anthony Bruno, *RIAA to Google: Help Us Fight Piracy*, BILLBOARD.BIZ, Aug. 19, 2010, http://www.billboard.biz/bbbiz/content_display/industry/e3if6a7faa5026473498f596f5a73238fa5 (reproducing the text of a letter from the RIAA and other industry groups to Google CEO Eric Schmidt, in which the senders state that "[t]he current legal and regulatory regime is not working for America's creators"); Declan McCullagh, *RIAA: U.S. Copyright Law 'Isn't Working,'* CNET NEWS (Aug. 23, 2010), http://news.cnet.com/8301-13578_3-20014468-38.html (quoting RIAA president Cary Sherman).

[115] Viacom Int'l. Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 524 (S.D.N.Y. 2010) (granting summary judgment to YouTube). In its complaint, Viacom accused Google of "shift[ing] the burden entirely onto copyright owners to monitor the YouTube site on a daily or hourly basis to detect infringing videos and send notices to YouTube demanding that it 'take down' the infringing works." Complaint for Declaratory and Injunctive Relief and Damages at ¶ 6, *Viacom*, 718 F. Supp. 2d 514 (No. 1:07CV02103). In reality, the law puts that burden squarely on rights owners like Viacom; the DMCA expressly does not condition eligibility for safe harbor on a service provider's monitoring its service for infringing content. *See* 17 U.S.C. § 512(m) (2006) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity . . . ."). Viacom thus asked the court to hold YouTube liable for a sin of omission that the law does not recognize as a sin at all. *See* Complaint for Declaratory and Injunctive Relief and Damages, *supra*. It is interesting to note that Viacom's complaint is full of the scale-conscious rhetoric discussed in Part II above. For example, Viacom alleged that "YouTube has harnessed technology to willfully infringe copyrights on a huge scale," *id.* ¶ 2, that "YouTube appropriates the value of creative content on a massive scale," *id.* ¶ 2, that "a vast amount" of the content available on YouTube is infringing," *id.* ¶ 3, and that YouTube has "done little or nothing to prevent this massive infringement," *id.* ¶ 5.

[116] *Viacom*, 718 F. Supp. 2d at 524.

[117] *Id.*

Congress saw fit to allocate to service providers when it balanced the need to make the Internet safe for copyright owners against the need to promote growth and innovation in online services.[118]

C. The Costs of Scalable Enforcement

There are, of course, downsides to a system designed to avoid the delay and expense of litigation by facilitating the overnight removal of 100,000 allegedly infringing files. Along with such efficiency comes the potential for abuse by copyright owners. For example, notices of infringement have been used to censor speech that copyright owners find offensive and to suppress unlicensed uses of copyrighted works that are colorably fair;[119] similarly, DMCA pre-litigation subpoenas have been used as a pretext for identifying constitutionally protected anonymous speakers.[120] While the DMCA does contain provisions designed to protect users from notices sent in bad faith[121] and to enable the restoration of wrongfully removed material,[122] it is unclear whether these safeguards are as protective of users' rights in practice as they are in theory.[123] Forced to choose between protecting themselves from liability and protecting the

[118] *See supra* note 115 and accompanying text. Although it is not required to do so by the DMCA, YouTube maintains an automated audio and video identification system by means of which infringing content can be blocked, tracked, or monetized, as the copyright owner prefers. *See Audio ID and Video ID*, YOUTUBE, http://www.youtube.com/t/contentid (last visited Feb. 22, 2011).

[119] *See* Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 367–68 (2003) (arguing that "piracy surveillance techniques . . . fail to consider two significant costs to non-offenders: overdeterrence of speech and evisceration of fair use."); Seth K. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 32–33 (2006) (giving examples of speech-censoring abuses of the DMCA); Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1888–89 (2000) (discussing the troubling First Amendment implications of the DMCA's notice-and-takedown framework); Jacqui Cheng, *Five Examples of Lame DMCA Takedowns*, ARS TECHNICA (May 16, 2010), http://arstechnica.com/tech-policy/news/2010/05/five-examples-of-lame-dmca-takedowns.ars.

[120] *See, e.g.*, *In re* Subpoena Issued Pursuant to the Digital Millennium Copyright Act to: 43SB.Com, LLC, 86 U.S.P.Q.2D (BNA) 1505 (D. Idaho 2007) (quashing a § 512(h) subpoena intended to identify a pseudonymous blog commenter based on the blog operator's posting of a copyrighted cease and desist letter, which alleged that the commenter's statements were defamatory).

[121] *See* 17 U.S.C. § 512(f) (providing for remedies in cases of knowing material misrepresentation that material is infringing).

[122] *See id.* § 512(g) (providing for the replacement of removed material).

[123] *See* Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1003 (2008) (pointing out that most users who receive notices of infringement do not attempt to have removed material restored); Urban & Quilter, *supra* note 108, at 636 (questioning whether the procedural protections in § 512 are sufficient to provide adequate recourse for users).

expressive rights of their users, service providers are much more likely to err on the side of caution.[124] In this regard, the DMCA's mechanisms for streamlining dispute resolution are not without costs. Rights owners like Viacom focus exclusively on the costs of under-enforcement, but over-enforcement is an equally problematic artifact of § 512's workable-though-imperfect design for making online copyright enforcement scalable for hosted content.

D. The DMCA's Failure to Scale for P2P

It is not the end of the story, however, to say that the DMCA's enforcement machinery has proven to be scalable with respect to service providers that host content for users. The DMCA has not scaled well for enforcing copyrights infringed by means of P2P file-sharing networks, because the statute was designed primarily to address infringements that occur when users upload copyrighted material to a provider's servers or link to infringing content posted by others.[125] When it enacted the DMCA, Congress did not anticipate the distributed nature of P2P networks or the correspondingly distributed nature of the infringement they would enable. High-volume infringement is relatively easy to detect and combat when the content in question is fixed on the servers of easily identifiable intermediaries with duly designated DMCA agents;[126] it becomes much harder to detect and combat when that content is in transit across a distributed network whose membership is anonymous and dynamic.

The safe harbor provisions of § 512 cover four types of service provider functions: transitory digital network communications (i.e., routing and transmission), system caching, storage on behalf of users,

[124] This tendency is encouraged by the DMCA's absolution of ISPs for good faith removal of material that is ultimately found to be non-infringing. *See* 17 U.S.C. § 512(g)(1). As Seth Kreimer has explained, "if it is costly to distinguish protected from unprotected speech, the proxy censor is likely to abandon the effort to avoid errors and adopt a conscious policy of prophylactic self-censorship that blocks any content that could precipitate the threat of sanctions." Kreimer, *supra* note 119, at 28. *See* also Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 115 (2007) ("Notice and takedown therefore rewards overzealous copyright owners who use the DMCA mechanism to rid the Web even of legitimate content, secure in the expectation that ISPs will take everything down rather than risk their eligibility for the safe harbor.").

[125] *See* Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 41 (2006) ("[The DMCA] was designed to address a mainly centralized architecture . . . . Peer-to-peer architecture, by contrast, is decentralized and allows users to search for files stored in the libraries of other users.").

[126] *See* 17 U.S.C. § 512(c)(2) (requiring designation of an agent to receive notifications of claimed infringement).

and information location.[127] Service providers performing each of these functions, with the significant exception of routing and transmission, are required to comply with the notice-and-takedown framework in § 512(c).[128] The DMCA's primary focus on user-uploaded material residing on the systems of service providers reflects the then-current state of the art in network architecture.[129] Before P2P file-sharing applications came onto the scene, the most copyright-relevant function an online service provider performed was storage on behalf of users—the function covered by the safe harbor in § 512(c).[130] In P2P networks, however, files are not uploaded to a provider's server; they remain instead on the users' own systems, from which other users directly retrieve them.[131] In this architecture, the most copyright-relevant functions a service provider performs are routing and transmission—the functions covered by the safe harbor in § 512(a).[132] Because the DMCA was designed to deal with providers serving a centralized file-storage function, it has proven a poor fit in cases involving P2P, where the service provider functions only as a pass-through or conduit for the transfer of infringing material.[133]

The DMCA's exemption of providers of routing and transmission services (a.k.a. "mere conduits") from the notice-and-takedown requirements in § 512(c) is entirely consistent with the fact that such providers do not store or control user content.[134] Nevertheless, the exemption has operated in the context of P2P file sharing to negate the scalable enforcement mechanism that notice and takedown provides. Inasmuch as P2P file sharing shifts the locus of infringing activity from the storage function to the transmission function, it places such activity beyond the knowledge and control of

[127] *See id.* § 512(a)–(d).

[128] For providers of system caching, the requirement is found at § 512(b)(2)(E). For providers of storage on behalf of users, the requirement is found at § 512(c)(1)(C). For providers of information location tools, the requirement is found at § 512(d)(3). There is no corresponding requirement for providers of routing and transmission services.

[129] *See* Elkin-Koren, *supra* note 125, at 41.

[130] Bridy, *Response, supra* note 51, at 97.

[131] *Id.* (citing A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001) (explaining how a P2P system works)).

[132] *Id.*

[133] *Id.*; *see also* Lemley, *supra* note 124, at 113 (remarking on the obsolescence of the DMCA's safe harbors in light of P2P technology).

[134] *See* Recording Indus. Assoc. of Am. v. Charter Commc'ns, Inc., 393 F.3d 771, 776 (8th Cir. 2005) (explaining that the absence of the notification and remove-or-disable-access provisions from § 512(a) "makes sense where an ISP merely acts as a conduit for infringing material . . . because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material").

the ISP and thus beyond the reach of the enforcement scheme created by § 512(c).[135]

As a consequence of the exemption of conduit providers from the notice and takedown requirements of § 512(c), the expedited subpoena provision in the DMCA—§ 512(h)—has also been held inapplicable to these providers.[136] This is because the application for a subpoena under § 512(h) must include a copy of the notice described in § 512(c)(3)(A).[137] The notice described in § 512(c)(3)(A) must identify, among other things, "the material that is claimed to be infringing . . . and that is to be removed or access to which is to be disabled" by the service provider.[138] In reaching the conclusion that the subpoena power in § 512(h) cannot be held to extend to providers covered by § 512(a), the Courts of Appeals for the D.C. and Eighth Circuits found it dispositive that § 512(c)'s notice-and-takedown requirements do not apply on the face of the statute to providers that act simply as conduits for information.[139] After all, how can § 512(h), which expressly requires an applicant to submit a copy of a notice compliant with § 512(c), apply to providers that are not subject to § 512(c) in the first place?[140] It makes more sense to conclude, as these Circuits did, that the references to § 512(c) in § 512(h) restrict the applicability of § 512(h) to providers that are able to remove or disable access to specific material.[141] In short, courts have held, there is an assumption

[135] Although in-network filtering and blocking technologies have greatly evolved since the passage of the DMCA, and broadband providers actively manage network traffic in ways that were not then possible, the statute presupposes a passive transit model; § 512(a) requires that material be transmitted through the qualifying provider's system "through an automatic technical process and without selection of the material by the service provider." 17 U.S.C. § 512(a)(2) (2006).

[136] *See Charter Commc'ns, Inc.*, 393 F.3d at 777; Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., 351 F.3d 1229, 1238 (D.C. Cir. 2003).

[137] *See* 17 U.S.C. § 512(h)(2)(A).

[138] 17 U.S.C. § 512(c)(3)(A).

[139] *See Charter Commc'ns, Inc.*, 393 F.3d at 776 (explaining that each safe harbor that covers a function allowing the ISP to remove or disable access to infringing material (i.e., storage, system caching, or linking) contains a remove-or-disable access provision); *Verizon Internet Servs., Inc.*, 351 F.3d at 1236–37 ("We agree that the presence in § 512(h) of three separate references to § 512(c) and the absence of any reference to § 512(a) suggests the subpoena power of § 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.").

[140] *Verizon Internet Servs., Inc.*, 351 F.3d at 1236–37. I have argued elsewhere that judicial interpretations of § 512(i)—the DMCA's repeat infringer provision, which applies to all types of providers seeking safe harbor under § 512—have potentially created a "back door" requirement for conduit providers to have in place a system for receiving and responding to notices of infringement sent by rights owners. *See* Bridy, *Response*, *supra* note 51, at 98.

[141] *See Charter Commc'ns, Inc.*, 393 F.3d 771; *Verizon Internet Servs.*, 351 F.3d 1229. *But see* Lateef Mtima, *Whom the Gods Would Destroy: Why Congress Prioritized Copyright Protection Over Internet Privacy in Passing the Digital Millennium Copyright Act*, 61 RUTGERS L. REV. 627, 673 (2009).

underlying § 512(h) that a subpoena recipient will actually be in a position to take down material identified as infringing.

It is possible, perhaps even probable, that § 512(h) would have been written differently if P2P technology had existed at the time of the DMCA's drafting.[142] In light of that possibility, rights owners have persuaded some judges that the subpoena provision should be held to apply to service providers covered by §512(a), despite the assumption underlying § 512(h) that subpoena recipients can remove or disable access to specific material.[143] In the face of unanticipated technological developments, these judges look past the letter of the DMCA to make it scale for P2P file sharing. Such recuperative acts are plainly beyond the judiciary's competence, however, as the D.C. Circuit said in *Recording Industry Association of America, Inc. v. Verizon Internet Services*:

> It is not the province of the courts . . . to rewrite the DMCA in order to make it fit a new and unfor[e]seen [I]nternet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress . . . .[144]

In the absence of Congressional action to bring P2P file sharing and the providers whose networks are used for it within the scope of §§ 512(c) and (h) of the DMCA, rights owners cannot avail themselves of the statute's mechanisms for making online copyright enforcement scalable by allowing it to operate outside of litigation. When it comes to P2P file sharers, rights owners must sue to enforce their copyrights and, for that matter, even to figure out whom to sue.

E. A Perverse Consequence of the DMCA's Failure to Scale for P2P

In her dissent in *Charter Communications*, the Eighth Circuit case that interpreted § 512(h) to exclude § 512(a) providers, Judge Murphy emphasized the negative implications of the majority's holding for the DMCA's goal of making online copyright enforcement scalable:

[142] *See Verizon Internet Servs.*, 351 F.3d at 1238 ("Had the Congress been aware of P2P technology, or anticipated its development, § 512(h) might have been drafted more generally.").

[143] *See Charter Commc'ns, Inc.*, 393 F.3d at 778 (Murphy, J., dissenting) (asserting that § 512(h) should apply to conduit providers); Recording Indus. Ass'n of Am. v. Verizon Internet Servs., 240 F. Supp. 2d 24, 30 (D.D.C. 2003) (holding that § 512(h) applies to conduit providers seeking safe harbor under § 512(a)), *rev'd*, 351 F.3d 1229.

[144] *Verizon Internet Servs.*, 351 F.3d at 1238; *see also* Recording Indus. Ass'n of Am. v. Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 953 (M.D.N.C. 2005) ("While the RIAA's argument at first blush is tempting, the Court rejects it because it would necessarily amount to the rewriting of the statute.").

> The majority's interpretation of the statute . . . denies copyright holders the ability to obtain identification of those subscribers who purloin protected materials through § 512(a) conduit ISPs . . . . The suggestion that copyright holders should be left to file John Doe lawsuits to protect themselves from infringement by subscribers of conduit ISPs like Charter, instead of availing themselves of the mechanism Congress provided in the DMCA, is impractical and contrary to legislative intent. John Doe actions are costly and time consuming. Nowhere in the DMCA did Congress indicate that copyright holders should be relegated to such cumbersome and expensive measures against conduit ISPs.[145]

While Judge Murphy's observations concerning the practical consequences of a narrow interpretation of § 512(h) are unarguable, her colleagues rightly declined to "contort the statute" to make it applicable in P2P cases.[146]

Unable to use the DMCA's expedited subpoena provision to uncover the identities of alleged P2P infringers, rights owners predictably fell back on filing John Doe lawsuits and seeking expedited discovery under Rule 45 of the Federal Rules of Civil Procedure to identify accused file sharers.[147] To counteract the massive scale of P2P infringement, the RIAA vowed to fight fire with fire, suing massive numbers of file sharers beginning in 2003.[148] In an effort to make the litigation scalable, it named hundreds of John Doe defendants per filing in a coordinated legal campaign similar to mass tort litigation, but with the aggregation occurring on the defendant's side—a rarity in the world of aggregate proceedings.[149]

[145] *Charter Commc'ns, Inc.*, 393 F.3d at 782 (Murphy, J., dissenting).

[146] *See id.* at 777 (majority opinion) ("We agree with and adopt the reasoning of the [court] in *Verizon* as it pertains to this statutory issue. . . . As a court we are bound to interpret the terms of the statute and not to contort the statute to cover the situation presented by this case.").

[147] *See, e.g.*, UMG Recordings, Inc. v. Does, 64 Fed. R. Serv. 3d (Callaghan) 305 (N.D. Cal. 2006) (granting the plaintiff copyright owner's motion to serve immediate discovery on an ISP in the form of a Rule 45 subpoena seeking each John Doe defendant's true name, address, telephone number, e-mail address, and Media Access Control (MAC) address).

[148] *See* Liane Cassavoy, *Music Labels Declare War on File Swappers*, PC WORLD, Sept. 8, 2003, http://www.pcworld.com/article/112364/music_labels_declare_war_on_file_swappers.html ("The Recording Industry Association of America has filed lawsuits against 261 people . . . . These lawsuits are just the first of subsequent waves of litigation, [RIAA President Cary] Sherman says, noting the RIAA expects to file thousands more in the coming months.").

[149] *See* David Opderbeck, *Peer-to-Peer Networks, Technological Evolution, and Intellectual Property Reverse Private Attorney General Litigation*, 20 BERKELEY TECH. L.J. 1685, 1706 (2005) ("By filing large groups of bundled claims under the 'John Doe' procedure, obtaining information subpoenas in the central forum for essentially all the discovery relevant to each defendant's file trading activity, and then settling individual claims on standardized terms, the RIAA litigation bears all the hallmarks of an aggregate or mass tort proceeding.").

Defendant class actions are permitted under the Federal Rules of Civil Procedure, but such actions raise due process concerns that are not implicated in plaintiffs' class actions, and they are very seldom filed. *See* Robert R. Simpson & Craig Lyle Perra, *Defendant Class Actions*, 32 CONN. L. REV. 1319, 1323 (2000).

The first RIAA case targeted 261 John Doe defendants, with a promise of thousands more to follow.[150] By the time the RIAA ended its John Doe campaign in late 2008, it had sued more than 30,000 individuals.[151] Although the number of actual cases filed did not approach that number, given the RIAA's practice of aggregating defendants, the campaign coincided with a substantial increase in the copyright caseload in the perennially overburdened federal district courts. By way of comparison, the total number of new copyright cases filed between 2001 and 2003 was 6,599.[152] Between 2004 and 2006, that number swelled to 12,736—a 93 percent increase.[153] New copyright case filings peaked at just under 14,000 between 2006 and 2008.[154] In 2009, following the conclusion of the RIAA's campaign, the number of new cases dropped back down to approximately the level at which it had been in 2004.[155]

The number of new filings has spiked again, however, thanks in part to the efforts of two law firms that have taken up the mantle the RIAA laid down in 2008. Operating as the U.S. Copyright Group, the D.C. area firm of Dunlap, Grubb & Weaver filed suits in 2010 on behalf of a handful of independent filmmakers alleging infringement by over 14,000 individual John Doe file sharers.[156] In a single filing, over 4,500 individuals were sued for using BitTorrent to download the film *Far Cry*.[157] In another case, 5,000 Does were accused of illegally downloading *The Hurt Locker*.[158] Inspired by the U.S. Copyright Group's business model, a law firm in West Virginia—operating as the

[150] *See* Cassavoy, *supra* note 148; *see also* John Borland, *RIAA Sues 261 File Swappers*, CNET NEWS (Sept. 8, 2003), http://news.cnet.com/2100-1023_3-5072564.html (reporting on the first case filed in the campaign). Culling information from RIAA press releases, David Opderbeck compiled a table of filed cases from 2004 and 2005. *See* Opderbeck, *supra* note 149, at 1754. Between 400 and 800 Does were sued every month in 2004. *See id.* More than 700 Does were sued every month for seven months in 2005. *See id.*

[151] David Kravets, *File Sharing Lawsuits at a Crossroads, After 5 Years of RIAA Litigation*, WIRED, Sept. 4, 2008, http://www.wired.com/threatlevel/2008/09/proving-file-sh/.

[152] *See infra* Appendix A.

[153] *See infra* Appendix A. Not all of these cases, of course, were file sharing cases.

[154] *See infra* Appendix A.

[155] *See infra* Appendix A.

[156] *See* Nate Anderson, *The RIAA? Amateurs. Here's How You Sue 14,000+ P2P Users*, ARS TECHNICA (June 1, 2010), http://arstechnica.com/tech-policy/news/2010/06/the-riaa-amateurs-heres-how-you-sue-p2p-users.ars.

[157] *See* Achte/Neunte Boll Kino Beteiligungs GMBH & Co KG v. Does 1–4,577, No. 1:10-cv-00453, 2010 WL 3522256 (D.D.C. Mar. 18, 2010).

[158] *See* Complaint,Voltage Pictures, LLC v. Does 1–5,000, No. 1:10-cv-00873, 2010 WL 4955131 (D.D.C. May 24, 2010). Other cases filed by the U.S. Copyright Group include: Maverick Entertainment Group v. Does 1–1,000, No. 1:10-cv-00569 (D.D.C. Apr. 8, 2010); Call of the Wild Movie, LLC v. Does 1–358, No. 1:10-cv-00455 (D.D.C. Mar. 19, 2010); G2 Prods., LLC v. Does 1–83, No. 1:10-cv-00041 (D.D.C. Jan. 8, 2010); and Worldwide Film Entertainment, LLC v. Does 1–749, No. 1:10-cv-00038 (D.D.C. Jan. 8, 2010).

Adult Copyright Company and advertising "hardcore protection for hardcore content"—filed suits accusing some 16,000 John Does of infringing copyrights in two pornographic films, *Batman XXX: A Porn Parody* and *Teen Anal Nightmare 2*, via P2P networks.[159] Compared with this recent round of John Doe filings, the RIAA's now-abandoned ambitions for large-scale P2P litigation seem modest.

Of course, the intent of plaintiffs and their counsel in these cases is not to litigate the claims to judgment; the goal is to secure a high volume of quick settlements, transacted online, in the range of a few thousand dollars apiece.[160] As Julie Cohen noted with respect to the RIAA litigation, low filing and overhead costs allow these settlement programs to operate as a profit center for copyright owners.[161] Once an individual John Doe settles by making an electronic payment and accepting a standardized settlement agreement drafted by the plaintiff's counsel, he or she is dismissed from the case and thereby relieved of both the stress of litigation and the cost of hiring counsel.[162] Those who decline to settle are named and remain on the docket as parties.[163]

Attempting to scale up copyright infringement litigation by naming hundreds or thousands of John Doe defendants in a single action not only makes for unmanageable dockets and a potential three-ring circus of pre-trial motions, it also creates insoluble due process problems relating to joinder, venue, and personal jurisdiction. Citing the "panoply of facts, law, and defenses" presented in a 2004

[159] *See* Debra Cassens Weiss, *Porn Industry Lawyer Is New Copyright King with 16,700 Lawsuits Filed*, ABA JOURNAL, Nov. 10, 2010, http://www.abajournal.com/news/article/porn_industry_lawyer_is_new_copyright_king_with_16700_lawsuit_filed; Greg Sandoval, *Porn Studios to Subpoena Accused File Sharers*, CNET NEWS (Oct. 2, 2010), http://news.cnet.com/8301-31001_3-20018358-261.html; *see also* Complaint, Third World Media, LLC v. Does 1–1243, No. 3:10cv90 (N.D.W. Va. Sept. 24, 2010); Complaint, Patrick Collins, Inc v. Does 1–281, No. 3:10cv91(N.D.W. Va. Sept. 24, 2010); Complaint, Collins, Inc v. Does 1–118, No. 3:10cv92 (N.D.W. Va. Sept. 24, 2010); Complaint, West Coast Prods., Inc., v. Does 1–2010, No. 3:10cv93 (N.D.W. Va. Sept. 24, 2010); Complaint, West Coast Prods., Inc v. Does 1–535, No. 3:10cv94 (N.D.W. Va. Sept. 24, 2010); Complaint, Combat Zone, Inc v. Does 1–1037, No. 3:10cv95 (N.D.W. Va. Sept. 24, 2010); Complaint, Combat Zone, Inc v. Does 1–245, No. 3:10cv96 (N.D.W. Va. Sept. 24, 2010).

[160] *See USCG v. The People*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/uscg (last visited Oct. 28, 2010) (describing the U.S. Copyright Group's modus operandi). The U.S. Copyright Group maintains a web site for subpoena recipients seeking to settle their claims. *See* http://dglegal.force.com/SiteLogindglegal (visited Oct. 28, 2010). Although the site is practically devoid of information, the phrase "All Major Credit Cards Accepted" is displayed prominently. *Id.* Visitors to the site can log in and see further information only if they have a "Defendant Record ID." *Id.*

[161] *See* Julie Cohen, *Pervasively Distributed Copyright Enforcement*, 95 GEO. L.J. 1, 17 (2006).

[162] *See* Opderbeck, *supra* note 149, at 1705 (describing the modus operandi in the RIAA cases).

[163] *Id.*

RIAA case, a district court in Pennsylvania held *sua sponte* that 202 of 203 John Doe defendants had been improperly joined.[164] The court concluded that "wholesale litigation" of such disparate claims was not appropriate, notwithstanding the fact that it would be both "convenient and economical" from the plaintiff's point of view for the case to go forward.[165] A district court in Florida required severance of twenty-four out of twenty-five John Does in another RIAA case, citing unrelated parties and facts, unreasonable prejudice and expense to defendants, and substantial inconvenience in the administration of justice.[166] Courts in Ohio,[167] North Carolina,[168] and New York[169] also severed defendants in RIAA cases, citing the same reasons. Other courts, including the court in the post-RIAA *Far Cry* litigation, have allowed the cases to go forward; these courts have attempted, however, to streamline the Rule 45 process in a way that is fair to defendants by requiring the distribution of a court-approved standardized notice to every Internet user whose IP address is listed in the plaintiff's subpoena.[170] The notice in the *Far Cry* suit informs recipients that their identities will be disclosed by their ISPs in thirty days, unless they elect either to settle the suit or to file a motion to quash.[171] The notice also informs recipients that they may challenge the court's personal jurisdiction over them.[172]

[164] BMG Music v. Does 1–203, No. 04-650, 2004 U.S. Dist. LEXIS 8457, at *4 (E.D. Pa. Apr. 2, 2004).

[165] *Id.* at *2, *4.

[166] Interscope Records v. Does 1–25, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782, at *17–19 (M.D. Fla. Apr. 1, 2004).

[167] *See* Arista Records, LLC v. Does 1–11, No. 1:07-CV-2828, 2008 U.S. Dist. LEXIS 90183 (N.D. Ohio Nov. 3, 2008).

[168] *See* Laface Records, LLC v. Does 1–38, No. 5:07-CV-298, 2008 U.S. Dist. LEXIS 14544 (E.D.N.C. Feb. 27, 2008).

[169] *See* Elektra Entm't Grp., Inc. v. Does 1–9, No. 04-cv-2289, 2004 U.S. Dist. LEXIS 23560 (S.D.N.Y. Sept. 7, 2004).

[170] *See* Court-Directed Notice Regarding Issuance of Subpoena Seeking Disclosure of Your Identity, Achte/Neunte Boll Kino Beteiligungs GMBH & Co KG v. Does 1–4,577, No. 1:10-cv-00453 (D.D.C. July 15, 2010) [hereinafter Court-Directed Notice], *available at* http://www.eff.org/files/filenode/uscg/40-2%20Exhibit%201.pdf; *see also, e.g.*, London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, app. A (D. Mass. 2008) (reproducing the full text of a court-ordered notice of subpoena).

[171] *See* Court-Directed Notice, *supra* note 170. Defendants in some of the John Doe file sharing cases have been given as few as fourteen days to move to quash. *See, e.g.*, *London-Sire Records*, 542 F. Supp. 2d at app. A.

[172] *See* Court-Directed Notice, *supra* note 170. In these suits, courts have generally declined to quash Rule 45 subpoenas for lack of personal jurisdiction, holding that such determinations are premature. *See London-Sire Records*, 542 F. Supp. 2d at 181; *Elektra Entm't Grp.*, 2004 U.S. Dist. LEXIS 23560, at *20. Courts in the District for the District of Columbia, where the U.S. Copyright suits are pending, have upheld personal jurisdiction in past file sharing cases on the rationale that allowing people in the forum to download files via a P2P network creates sufficient minimum contacts with the forum, regardless of where the computer

Even if thousands of the defendants in the U.S. Copyright Group and Adult Copyright Company cases elect to settle at a very early stage in the litigation, it is all but impossible to imagine how these cases could progress through discovery as a practical matter; severance is inevitable.[173] Courts that postpone severance and require issuance of special notices effectively channel defendants into the plaintiffs' high-volume settlement apparatus and, by doing so, both deprive the courts of revenue and provide incentives for massive (mis)joinder in future cases.[174]

Considering the significant procedural due process and administration of justice issues associated with mass John Doe litigation, it is hard to imagine a compelling argument in favor of adjudicating online copyright disputes in this way. If the defendants in these suits were severed, the due process problems arising from mass joinder would be solved, and the courts would collect filing fees more accurately reflective of the number of controversies over which they are being asked to preside. Conversely, however, severance would swell both copyright caseloads for courts and enforcement costs for plaintiffs.

Simply put, litigation is not a scalable mechanism for dealing with the high volume of copyright disputes that arise from P2P file sharing; trying to *make* litigation scale by aggregating thousands of defendants in a single suit is efficient for plaintiffs, but the attendant costs for defendants and the justice system as a whole are unacceptably high. Including thousands of allegedly infringing files in a single § 512(c) takedown notice is a workable way of killing lots of birds with one stone when it comes to hosted content, but including thousands of defendants in a single copyright infringement lawsuit is

sharing the files and its owner are physically located. *See, e.g.*, Virgin Records, Inc. v. John Does 1–35, No. 05-1918, 2006 U.S. Dist. LEXIS 20652, at *11–12 (D.D.C. Apr. 18, 2006) ("[B]y installing P2P software and logging onto a P2P network, each defendant transformed his or her computer into an interactive Internet site, allowing others to complete transactions by downloading copyrighted works over the Internet. Importantly, each Defendant was disseminating copyrighted works to anyone that wanted them and was downloading copyrighted works from others who offered them—including residents of this jurisdiction."). For a critique of this rationale, see Joshua M. Dickman, *Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits*, 82 TUL. L. REV. 1049 (2008).

[173] Matters concerning severance, including the timing of it, are within the court's discretion. *See* FED. R. CIV. P. 21 (providing that a court, on motion or on its own, may "at any time, on just terms, add or drop a party" or "sever any claim against a party").

[174] *See* Arista Records, LLC v. Does 1–11, No. 1:07-CV-2828, 2008 U.S. Dist. LEXIS 90183, at *17 (N.D. Ohio Nov. 3, 2008) (explaining that "a consequence of postponing a decision on joinder in lawsuits similar to this action results in lost revenue of perhaps millions of dollars and only encourages Plaintiffs and other members of the RIAA to join (or misjoin) as many [D]oe defendants as possible").

not analogously effective in the P2P context. The next Part considers potentially more scalable mechanisms for P2P copyright enforcement.

IV. MORE SCALABLE ALTERNATIVES: COSTS AND BENEFITS

A. Amendment of § 512(h) versus "Notice and Notice"

Congress could amend § 512(h) of the DMCA to reach § 512(a) providers; that is, the statute could be amended to permit issuance of a subpoena upon submission of *either* a copy of a notice compliant with § 512(c)(3)(a) *or* a notice identifying the IP address of the alleged infringer's computer, along with information sufficient to establish the date, time, and content of the allegedly infringing transmission. Although the season for tinkering with the DMCA to make it accommodate P2P technologies is probably past,[175] such an amendment would effectively preempt mass John Doe file-sharing litigation. With an expanded scope for § 512(h), rights owners would have the ability to identify and contact alleged P2P infringers without recourse to the courts and Rule 45, which, as Judge Murphy argued in her dissent in *Charter*, is precisely how Congress intended the provision to function with respect to technologies extant when the DMCA was drafted.[176] While amending § 512(h) to reach users of P2P networks would raise privacy concerns related to the First Amendment right to speak anonymously online, the anonymous speech issue has been litigated time and again in cases involving motions to quash § 512(h) subpoenas, and courts have consistently held that the need to identify alleged copyright infringers outweighs the anonymous speech rights of the alleged infringers.[177] In light of

[175] In 2003, before the Court of Appeals for the D.C. Circuit reversed the district court's holding in *Verizon Internet Services*, the Senate Judiciary Committee heard testimony concerning the applicability of § 512(h) to conduit providers. *See Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. (2003). At the hearing, Register of Copyrights Marybeth Peters argued that Congress should amend the DMCA if necessary to make the subpoena provision reach P2P providers. *See id.* (statement of Hon. Marybeth Peters, Register of Copyrights), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=902&wit_id=2560 ("It is thus incumbent upon this Committee and this Congress to see to it that if the judiciary fails to enforce the DMCA and therefore fails to provide the protection to which copyrighted works are entitled, the legislature does."). By 2008, the RIAA had given up on lobbying Congress to amend the DMCA to address P2P file sharing. *See* Anne Broache, *RIAA: No Need to Force ISPs by Law to Monitor Piracy*, CNET NEWS (Jan. 30, 2008), http://news.cnet.com/8301-10784_3-9861460-7.html (quoting RIAA President Cary Sherman).

[176] *See* Recording Indus. Assoc. of Am. v. Charter Commc'ns, Inc., 393 F.3d 771, 778 (8th Cir. 2005) (Murphy, J., dissenting).

[177] *See, e.g.*, Sony Music Entm't Inc. v. Does 1–40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004); *Elektra Entm't Grp.*, 2004 U.S. Dist. LEXIS 23560; Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs , 257 F. Supp. 2d 244 (D.D.C. 2003) *rev'd*, 351 F.2d 1229 (D.C. Cir. 2003).

these decisions, if Congress were inclined to amend the DMCA to allow rights owners to identify alleged P2P infringers outside the litigation context, privacy-based arguments raised in opposition would be unlikely to undermine the amendment.

Amending § 512(h), however, is neither the only nor the optimal way of creating a scalable, out-of-court framework within which rights owners can warn alleged infringers of their potential liability and thereby deter them from using P2P networks to infringe. For several years, broadband ISPs have been entering into private agreements with corporate rights owners under which they have agreed to pass along notices of infringement to their subscribers. In 2005, the year in which the Eighth Circuit decided *Charter*, Verizon agreed to forward notices of infringement for Disney; in return, it received the right to transmit certain Disney programming over its network.[178] In late 2009, Verizon agreed to forward notices for the RIAA.[179] Comcast is also a party to notice-forwarding agreements.[180] Through these "notice and notice" arrangements, ISPs can assist rights owners in enforcing their copyrights in the P2P context without disclosing subscribers' identities and thereby compromising subscribers' privacy.[181] Moreover, there is growing evidence that notice forwarding is actually an effective curb on P2P infringement.[182]

[178] Nate Anderson, *Verizon to Forward RIAA Warning Letters (But That's All)*, ARS TECHNICA (Nov. 13, 2009), http://arstechnica.com/tech-policy/news/2009/11/verizon-to-forward-riaa-warning-letters-but-thats-all.ars. Some courts have interpreted § 512(i) of the DMCA, which requires termination of access for repeat infringers, to require all providers seeking safe harbor to process notices of infringement from rights owners. *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 758 (9th Cir. 2007) (holding that § 512(i) requires "a working notification system"), *amended on denial of reh'g*, 488 F.3d 1102 (9th Cir. 2007); Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) (holding that a reasonable jury could conclude that implementation of a termination policy is not reasonable where notices of infringement have gone unheeded by the provider); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004) (holding that § 512(i) requires adoption and implementation of a procedure for receiving complaints and conveying them to users).

[179] Anderson, *supra* note 156.

[180] *See* Chloe Albanesius, *Comcast, Others Deny 'Three Strikes' Piracy Plan*, PCMAG.COM (Mar. 27, 2009), http://www.pcmag.com/article2/0,2817,2343977,00.asp (reporting on the Leadership Music Digital Summit).

[181] Statutory implementation of notice and notice as an alternative to notice and takedown has been proposed in the context of Canadian copyright reform efforts. *See generally* Michael Geist, *The Effectiveness of Notice and Notice* (Feb. 15, 2007), http://www.michaelgeist.ca/content/view/1705/125/; *see also* Michael Geist, *All Rights Reserved? Cultural Monopoly and the Troubles with Copyright*, 10 MARQ. INTELL. PROP. L. REV. 411, 430 (2006) (proposing a "notice and notice" system for Canada modeled on Canada's approach to online child pornography).

[182] *See* David Carnoy, *Verizon Ends Service of Alleged Illegal Downloaders*, CNET NEWS (Jan. 20, 2010), http://news.cnet.com/8301-1023_3-10437176-93.html ("[The Verizon representative] also noted that . . . issuing warning letters is proving to be effective."); Greg Sandoval, *AT&T Exec: ISP Will Never Terminate Service on RIAA's Word*, CNET NEWS (Mar. 25,

After Congress declined to amend § 512(h) to overturn the results in *Verizon* and *Charter*, ISPs and rights owners stepped into the breach to reach a compromise among themselves that serves the interests of both privacy and efficiency. By dispensing altogether with pre-litigation subpoenas, the notice-and-notice framework streamlines P2P copyright enforcement while simultaneously protecting subscribers' privacy. Copyright owners are afforded a means of warning alleged infringers, and ISPs can facilitate that communication without handing over their users' personally identifying information.

B. Graduated Response and ADR for P2P

Since 2008, trade groups representing corporate rights owners have been lobbying worldwide for the adoption of graduated response or "three strikes" protocols as an alternative to mass litigation.[183] Pursuant to these protocols, ISPs either privately agree, or are statutorily required, to terminate Internet access for subscribers deemed to be "repeat infringers."[184] Several countries, including the U.K., France, South Korea, and Taiwan, have already incorporated graduated response into their domestic copyright enforcement systems.[185] Similar legislation is making its way through the legislative process in New Zealand,[186] although E.U. countries including Germany and Spain have declined to follow suit.[187]

2009), http://news.cnet.com/8301-1023_3-10204514-93.html ("[An AT&T vice president] said the notices worked. The company saw very few repeat offenders.").

[183] *See generally* Annemarie Bridy, ACTA and the Specter of Graduated Response, 26 AM. U. INT'L L. REV. (forthcoming 2011); Peter Yu, *The Graduated Response*, 62 FLA. L. REV. 1373 (2010).

[184] *See* Bridy, *supra* note 183, manuscript at 2, on file with author.

[185] *See* Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009) (discussing graduated response in France, South Korea, and Taiwan). The mandate in the UK is set forth in the Digital Economy Bill, which became law in April 2010. *See* Digital Economy Act, 2010, c. 24. The Act provides that technical measures, including protocols for temporary Internet disconnection, may be phased in by the Secretary of State if a notice regime set forth in the legislation proves inadequate to reduce the level of online infringement. *See* DIGITAL ECONOMY ACT 2010: EXPLANATORY NOTES, ¶¶ 33–34, *available at* http://legislation.data.gov.uk/ukpga/2010/24/notes/division/5/2/data.pdf.

[186] New Zealand's graduated response mandate is set forth in the Copyright (Infringing File Sharing) Amendment Bill, the text of which may be accessed online via the New Zealand government's web site. *See* Copyright (Infringing File Sharing) Amendment Bill 2010 119-2, *available at* http://www.legislation.govt.nz/bill/government/2010/0119/latest/DLM2764312.html. As it was in France, the path to mandatory graduated response in New Zealand is proving to be a rocky one. *See, e.g.*, Pat Pilcher, *So Long Section 92A - New Copyright Bill Revealed*, N.Z. HERALD, Feb. 24, 2010, http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10628193 (describing the controversy surrounding the implementation of graduated response in New Zealand, including the repeal of Section 92A of the Copyright Act, and the introduction of

In the United States, rights owners have elected not to lobby for statutorily mandated graduated response, opting instead to pursue voluntary agreements with ISPs.[188] Such agreements have not come to fruition, however, as broadband providers have resisted becoming the entertainment industries' copyright enforcers.[189] Although domestic ISPs that want to qualify for safe harbor under the DMCA are already required to adopt and reasonably implement a policy for terminating the access of repeat infringers,[190] the DMCA does not define "repeat infringer," and providers have been understandably reluctant to terminate users' access based solely on repeat allegations of infringement by rights owners. Whereas ISPs have been willing to forward notices of infringement to their customers, they have been unwilling to terminate subscriber accounts in large numbers. Executives at Cox Communications have acknowledged terminating account access for a small number of users who ignored repeat notices of infringement.[191] AT&T executives, by contrast, have said that the company will not terminate any user's account for copyright infringement without a court order.[192] Universally, representatives of the major U.S. broadband providers have denied participation in graduated response programs and attribute their cooperation with rights owners to their longstanding obligations under the DMCA.[193]

The courts, on which broadband providers should be able to rely for guidance concerning who is (or is not) a "repeat infringer" for

more user-friendly legislation in the form of the Copyright (Infringing File Sharing) Amendment Bill).

[187] *See* Howell Llewellyn, *'Three-Strikes' Off Anti-Piracy Agenda In Spain*, BILLBOARD.BIZ, June 22, 2009, http://www.billboard.biz/bbbiz/content_display/industry/e3i8071e0d9c25cb6b876d3771fb7e3d102; Jacqui Cheng, *Germany Says "Nein" To Three-Strikes Infringement Plan*, ARS TECHNICA (Feb. 6, 2009), http://arstechnica.com/tech-policy/news/2009/02/germany-walks-away-from-three-strikes-internet-policy.ars.

[188] *See* Bridy, *Response, supra* note 51, at 82.

[189] *See, e.g.*, David Kravets, *Top Internet Providers Cool to RIAA 3-Strikes Plan*, WIRED, Jan. 5, 2009, http://www.wired.com/threatlevel/2009/01/draft-verizon-o ("Two weeks after the Recording Industry Association of America announced it had struck deals with top internet service providers to cut off unrepentant music sharers, not a single major ISP will cop to agreeing to the ambitious scheme, and one top broadband company says it's not on board.").

[190] *See* 17 U.S.C. § 512(i) (2006) (requiring service providers to (1) adopt a policy that provides for the termination of access for repeat infringers in appropriate circumstances; (2) implement that policy in a reasonable manner; and (3) inform its subscribers of the policy).

[191] *See* Albanesius, *supra* note 180; Sarah McBride, *Relationship Status of RIAA and ISPs: It's Complicated*, WALL ST. J. (Mar. 26, 2009, 3:07 PM), http://blogs.wsj.com/digits/2009/03/26/relationship-status-of-riaa-and-isps-its-complicated.

[192] Sandoval, *supra* note 182 (quoting Jim Cicconi, a senior executive vice president at AT&T).

[193] Albanesius, *supra* note 180 (reporting that "Comcast, Cox, and AT&T this week denied that they are participating in a 'three strikes and you're out' anti-copyright [infringement] program"); Kravets, *supra* note 189.

purposes of DMCA compliance, are unhelpfully split on the question. Some have said that notices of infringement from a copyright owner, taken on their own, are sufficient to trigger the duty to terminate a subscriber's access under the DMCA.[194] Others have said that such notices do not provide sufficient evidence of repeat infringement, because they could be erroneous.[195] No court has quantified the number of infringements that puts the "repeat" in "repeat infringer."[196] Given the lack of judicial consensus on the repeat infringer question, the relationship between graduated response and DMCA compliance is murky. While it seems clear that adoption of a three-strikes-and-you're-out protocol would satisfy the DMCA's requirement of reasonable implementation of a policy for terminating the access of repeat infringers, the statute is drafted to give ISPs latitude in crafting and implementing repeat infringer policies, and courts have protected that latitude.[197] Their decisions track David Nimmer's suggestion that a mechanical understanding of compliance with § 512(i) should give way to an objective good faith standard.[198]

While voluntary adoption of graduated response regimes by broadband providers would create a scalable, out-of-court framework for enforcing copyrights in the P2P context, ten years of experience with the notice-and-takedown regime for hosted content have demonstrated that there is a significant risk of abuse inherent in a system that streamlines enforcement by dispensing with the neutral adjudication of claims. Moreover, the stakes of procedural

[194] Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004) (concluding that "an [I]nternet service provider who receives repeat notifications that substantially comply with the requirements of § 512(c)(3)(A) about one of its clients, but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy"), *rev'd on other grounds*, 481 F.3d 751(9th Cir. 2007).

[195] Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004) (concluding that notices from a copyright owner function to bring a potential infringement to the provider's attention, but do not, "in themselves, provide evidence of blatant copyright infringement" because they could be erroneous).

[196] In *UMG Recordings, Inc. v. Veoh Networks Inc.*, for example, the court declined to hold that termination of a user's access was required after a second notice when the first notice identified multiple alleged infringements. 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009). The notices in the case were generated by the copyright owner using Audible Magic's filtering system. *Id.*

[197] *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008) (stating that "section 512(i) does not require service providers to track users in a particular way or to affirmatively police users for evidence of repeat infringement"); *Corbis Corp.*, 351 F. Supp. 2d at 1101–02 (holding that a properly adopted termination policy need not precisely track the language of the DMCA, and it need not disclose to users the precise criteria the provider will apply to determine when termination of access is appropriate); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1178 (C.D. Cal. 2002) (stating that § 512(i) "creat[es] room for enforcement policies less stringent or formal than the 'notice and take-down' provisions of section 512(c), but still subject to 512(i)'s 'reasonably implemented' requirement").

[198] *See* David Nimmer, *Repeat Infringers*, 52 J. COPYRIGHT SOC'Y U.S.A.167, 221 (2005).

streamlining are much higher for users when the sanction at issue is suspension or termination of Internet access as opposed to the removal of isolated content. The stakes are higher for broadband providers, too, insofar as suspension of access entails suspension of revenue.

ISPs, predictably, are vocally opposed to graduated response to the extent that it requires them to sit in judgment of their customers. In recent comments to the Office of the Intellectual Property Enforcement Coordinator (IPEC), AT&T executive James Cicconi sharply criticized the notion that ISPs are positioned to fairly and responsibly administer graduated response protocols:

> The government and the courts, not ISPs, are responsible for intellectual property enforcement, and only they can secure and balance the various property, privacy and due process rights that are at play and often in conflict in this realm . . . . The notion of non-governmental players assuming, without legal authority, a governmental role simply would not endure.[199]

With these risks and stakes in mind, Cicconi recommended that the government assume responsibility for a "court-administered adjudication process" that relies upon a "streamlined claims adjudication body" to resolve civil infringement claims against file sharers and other alleged online infringers.[200] What Cicconi wants, in other words, is a specialized form of ADR for P2P—a shift from litigation to administration roughly analogous to the one that Richard Nagareda has traced in the mass tort system.[201]

In the mass tort context, Nagareda views the evolution toward administrative frameworks for mass dispute resolution partially in terms of scalability: "The sheer numbers of claims, their geographic breadth, their reach across time to unidentified future claimants, and their factual patterns, together, demand the kind of systematized

[199] Letter from James W. Cicconi to Victoria Espinel 2–3 (Mar. 24, 2010), *available at* http://attpublicpolicy.com/wp-content/uploads/ATT-Comments-for-Joint-Strategic-Plan-3-24-10.pdf; *see also* Coordination and Strategic Planning of the Federal Effort against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan, 75 Fed. Reg. 8137 (Feb. 23, 2010). Eircom, Ireland's largest broadband provider, controversially agreed in 2010 to privately implement and administer a graduated response protocol. *See* Bridy, *supra* note 183, at *18-19. The agreement came in settlement of secondary copyright infringement claims brought against Eircom by major rights owners. *See id.* For details of the Eircom protocol and its implementation, see *id.*

[199] Letter from James W. Cicconi, *supra* note 199, at 4..

[200] Letter from James W. Cicconi, *supra* note 199, at 4.

[201] *See* Richard Nagareda, MASS TORTS IN A WORLD OF SETTLEMENT (2007). Nagareda argues that "the evolving response of the legal system to mass torts has been a shift from tort to administration." *Id.* at viii. He defines "administration" to mean "an ongoing, institutionalized regime that sees its subject matter not as a series of isolated events, but, instead, as suitable for systematic treatment." *Id.*

treatment characteristic of administrative processes."[202] The elements of numerosity and geographic breadth, which Nagareda sees as contributing to the unworkability of a litigation-driven mass tort system, are also present in a litigation-driven system for adjudicating claims of P2P copyright infringement. Given these commonalities, P2P infringement claims, like mass tort claims, may be better managed administratively than judicially.

1. An ADR System Modeled on ICANN's UDRP

The idea of a dedicated, publicly administered alternative dispute resolution system for adjudicating online copyright infringement claims has been raised before. In 2005, Mark Lemley and Anthony Reese proposed amending the Copyright Act to create a system modeled on the Internet Corporation for Assigned Names and Numbers (ICANN) Uniform Dispute Resolution Policy (UDRP) for adjudicating disputes over trademarks in domain names.[203] Under Lemley and Reese's system, a copyright owner seeking to enforce a copyright against a P2P infringer could forego civil litigation in favor of an administrative proceeding before an administrative law judge (ALJ) in the Copyright Office.[204] Such a proceeding would be limited to cases in which the copyright owner could produce evidence that the targeted individual uploaded at least fifty copyrighted works during a thirty day period—a threshold intended to keep cases of de minimis or isolated infringement out of the system.[205]

In addition to imposing a quantitative threshold, Lemley and Reese incorporate a qualitative limit on the type of claims to be decided administratively: Only clear-cut cases would be subject to administrative adjudication. Any case in which the accused infringer could present evidence of a genuine factual dispute or a viable claim of fair use would be kicked out of the system without prejudice to the complainant's right to bring a civil suit in court.[206] For cases straightforward enough to remain in the administrative system, Lemley and Reese build in procedural protections for accused infringers, including the right to present evidence rebutting allegations, the right to appeal a finding of liability, and the right to

[202] *Id.*

[203] Mark A. Lemley & R. Anthony Reese, *A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes*, 23 CARDOZO ARTS & ENT. L.J. 1 (2005).

[204] *Id.* at 3–4.

[205] *Id.* at 4.

[206] *Id.* at 7. In order for the system to work as a true alternative to litigation, the authors point out that most cases would have to be decided administratively. *Id.* at 8. Only cases involving plausible factual disputes or legal defenses would be kept out of the system. *Id.*

seek penalties against complainants for bringing frivolous or bad-faith claims.[207] The system scales by foregoing face-to-face argument and litigation-style discovery, but only in uncomplicated cases, leaving legitimately contested claims to a forum in which they can be fully aired. The recognition that hard cases are unsuitable for expedited adjudication is as much a key to the scalability of the ADR system that Lemley and Reese propose as the recognition that most file sharing cases are, both in law and in fact, easy ones.

For ISPs, a key advantage of a system like Lemley and Reese's is the allocation of responsibility for adjudicating claims of online infringement to a neutral third party. Another advantage is the removal of ambiguity concerning who should be counted as a repeat infringer for purposes of DMCA compliance. Lemley and Reese attempt to give stable meaning to § 512(i)'s requirement of termination for repeat infringers by expressly defining a repeat infringer as any user who is twice found liable in administrative proceedings.[208] An ISP seeking to remain eligible for safe harbor under the DMCA would be required to terminate access for any user who meets this definition. Lemley and Reese attempt to strike a balance on repeat infringement: To make enforcement more efficient for rights owners, they do not require civil judgments of infringement to trigger the ISP's duty to terminate; at the same time, to protect users from enforcement mistakes and abuses, they do not treat notices of infringement from rights owners as sufficient to trigger the duty.[209] To ameliorate the harshness associated with the prospect of "exile" from the Internet, Lemley and Reese envision a five-year time limit on termination and a period of public education between the passage of enabling legislation and the actual implementation of their system.[210]

Needless to say, an administrative copyright tribunal designed to make enforcement scalable in the context of P2P has not become part of the enforcement landscape in the United States. The role outlined for the Copyright Office in IPEC's 2010 Joint Strategic Plan on Intellectual Property Enforcement is strictly supportive and

[207] *Id.* at 2–3.

[208] The two-strikes repeat infringer protocol that Lemley and Reese describe may seem at first glance to be more draconian than the three-strikes protocol advocated by rights owners in connection with graduated response; however, because Lemley and Reese set a fifty-file jurisdictional minimum for each administrative claim, a user cannot be designated a repeat infringer under their protocol without having shared at least a hundred copyrighted files. *See id.* at 4.

[209] *Id.* at 13 ("Keying the termination obligation to an administrative finding would protect the due process rights of those wrongfully accused of infringement without rendering the repeat infringer provision altogether ineffective.").

[210] *Id.* at 14. A five-year suspension seems unduly long, but Lemley and Reese are not committed to so long a period.

educational.[211] Whether the idea of a specialized ADR system for P2P can gain traction domestically, six years after Lemley and Reese's proposal and well beyond the peak of the P2P "crisis," may depend on the perceived success or failure of such systems abroad. The newly implemented HADOPI system in France is sure to be the bellwether.

2. France's HADOPI System

The seeds for governmentally administered graduated response in France were sown in 2004, when the concept was first mentioned in a report of France's High Council of Literary and Artistic Property.[212] The report recommended implementation of a system requiring broadband providers to send a specific number of warnings to users suspected of infringement, after which a fine would be imposed.[213] When France amended its copyright law in 2006 in compliance with EU directive 2001/29/CE, requiring harmonization of copyright law throughout the EU, it did not incorporate graduated response into the new law.[214] Rights owners persisted, however, and the idea soon resurfaced in a 2007 report sponsored by the French Ministry of Culture, which proposed the creation of an administrative body that would oversee a system of warnings and sanctions.[215] French ISPs initially agreed to the proposal along with other stakeholders, but they withdrew their support before long, leading supporters of graduated response to seek a legislative mandate.[216]

In 2008, the French Minister of Culture and Communication introduced legislation creating the administrative body proposed in the 2007 report.[217] The body, HADOPI,[218] was to be responsible for implementing a graduated response system in which three warning letters would be followed by a suspension of the accused subscriber's Internet access for a maximum of one year.[219] Debate over the bill was intense both inside and outside the French parliament, with the greatest degree of controversy surrounding privacy and due process

[211] *See* EXEC. OFFICE OF THE PRESIDENT, 2010 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 33, 44–45 (2010).

[212] *See* Thierry Rayna & Laura Barbier, *Fighting Consumer Piracy with Graduated Response: An Evaluation of the French and British Implementations*, 6 INT'L J. FORESIGHT & INNOVATION POL'Y 294, 299 (2010).

[213] *Id.*

[214] *Id.* at 300.

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] The acronym translates as the High Authority for the Distribution of Works and the Protection of Rights on the Internet.

[219] Rayna & Barbier, *supra* note 212, at 301.

issues.[220] After passage of the bill in 2009, the French Constitutional Council ruled that a user's Internet access could not be interrupted on the authority of an administrative body, without a court order.[221] To comply with the Council's ruling, the HADOPI legislation was promptly amended, and the system was reconfigured to include an accelerated legal proceeding presided over by a judge.[222] The judge has authority under the amended law to impose an access sanction without a hearing, but the affected subscriber has the right to an appeal at which he or she is represented.[223]

Notices of infringement in the HADOPI system are generated by an Internet security and content detection company selected by rights owners.[224] A notice contains relevant information concerning the alleged infringement: the IP address from which the files were available, the ISP of the alleged infringer, and the date and time of the alleged infringement.[225] The notice is forwarded from the security company to the copyright owner, who then refers the incident to HADOPI.[226] To protect the accused subscriber's privacy, HADOPI forwards the notice to the subscriber without disclosing his or her identity to the copyright owner.[227] If a subscriber is alleged to have infringed on a second occasion within six months of receiving the first notice, HADOPI forwards a second notice.[228] If a third infringement is alleged within a year of the second notice, HADOPI refers the matter to a prosecutor, and a judge can order the subscriber's Internet access

[220] *See Les Députés Adoptent la Loi Hadopi*, LE MONDE.FR, May 12, 2009, http://www.lemonde.fr/technologies/article/2009/05/12/les-deputes-adoptent-la-loi-hadopi_1192219_651865.html; Marguerite Reardon, *France Ignores EU and Passes Antipiracy Law*, CNET NEWS (May 12, 2009), http://news.cnet.com/8301-1023_3-10238912-93.html.

[221] *See* Conseil Constitutionnel [CC] [Constitutional Court] decision No. 2009-590DC, Oct. 22, 2009, Rec. 179. The original version of the law did not require judicial review.

[222] *See* Loi 2009-1311 du 28 Octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet [Law 2009-1311 of October 28, 2009 Regarding Criminal Protection for Intellectual Property on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O] [OFFICIAL GAZETTE OF FRANCE], Oct. 29, 2009, p. 18290; *see also* CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art. L331-21.

[223] *See* Rayna & Barbier, *supra* note 212, at 301.

[224] *Id.* at 301.

[225] *Id.*; *see also Quelles informations me concernant sont détenues par l'Hadopi si je fais l'objet d'une procédure de réponse graduée?*, HADOPI, www.hadopi.fr/faq.html (last visited Feb. 22, 2011) (explaining what information concerning an alleged infringement is transmitted to HADOPI by the copyright owner).

[226] Rayna & Barbier, *supra* note 212, at 301; *see also Réponse Graduée*, HADOPI, http://www.hadopi.fr/usages-responsables/nouvelles-libertes-nouvelles-responsabilites/reponse-graduee.html (last visited Dec. 8, 2010).

[227] Rayna & Barbier, *supra* note 212, at 301.

[228] *Id.* (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art. L331-25); *see also Comment fonctionne la réponse graduée?*, HADOPI, www.hadopi.fr/faq.html (last visited Feb. 23, 2011) (explaining the protocol).

suspended.[229] If the judge determines that the infringement was the result of a negligent failure on the subscriber's part to secure his or her Internet connection, the suspension is limited to one month.[230] If the judge determines that the infringement was not merely negligent, a one-year suspension may be imposed.[231] If the subscriber wants to contest the judge's decision to suspend access, he or she can exercise the right to be heard on appeal.[232]

The HADOPI system is still quite new, and it remains to be seen where along the road the inevitable bumps will arise. In terms of volume, as many as 25,000 infringements per day are expected to be reported[233]—enough to tax even the most streamlined of systems. Unlike Lemley and Reese's proposed system, which limits administrative ADR to cases in which a single user is alleged to have shared fifty or more files at one time, the jurisdiction of HADOPI is not subject to any minimum volume threshold. Rights owners can thus funnel every detected infringement into the system, resulting in a substantial burden.[234] The lack of a minimum volume threshold also means that an accused infringer in France could be subject to suspension of Internet access after only three isolated file transfers over a period of eighteen months.

The HADOPI framework, as amended to comply with the requirements of the French Constitutional Council, shares with Lemley and Reese's plan the overarching goal of creating an efficient but fair administrative system for deciding claims of copyright infringement involving P2P file sharing. Both systems are designed to alleviate the burdens and delays to all parties associated with litigation, which has proven not to scale well for adjudicating claims involving P2P. Both systems attempt to balance the need for prompt, effective enforcement with the right of alleged infringers to a fair and neutral adjudication of the claims against them. Neither system

[229] Rayna & Barbier, *supra* note 212, at 301 (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art L335-7); *see also Comment fonctionne la réponse graduée?*, *supra* note 228.

[230] This can occur, for example, in a situation where the subscriber is a parent whose child is the accused infringer. *See* Rayna & Barbier, *supra* note 212, at 301 (citing CODE DE LA PROPRIÉTÉ INTELLECTUELLE, art. L335-7-1); *Qu'est-ce que l'infraction de négligence caractérisée?*, HADOPI, www.hadopi.fr/faq.html (last visited Feb. 22, 2011).

[231] Rayna & Barbier, *supra* note 212, at 301. During this period, the subscriber remains responsible for the regular price of the subscription and may not subscribe to another service. *Id.* at n.13.

[232] *Id.* at 301–02.

[233] *See* Aymeric Pichevin, *French Anti-Piracy Scheme's 25,000 Daily Reports*, BILLBOARD.BIZ, Oct. 22, 2010, http://www.billboard.biz/bbbiz/content_display/industry/e3i1c1499752deb3a60a1584400533395b0.

[234] It may be prudent, from a public relations standpoint at least, for rights owners to refrain from introducing every isolated report of infringement into the system, focusing instead on cases in which substantial numbers of files are being obtained and/or offered by specific users.

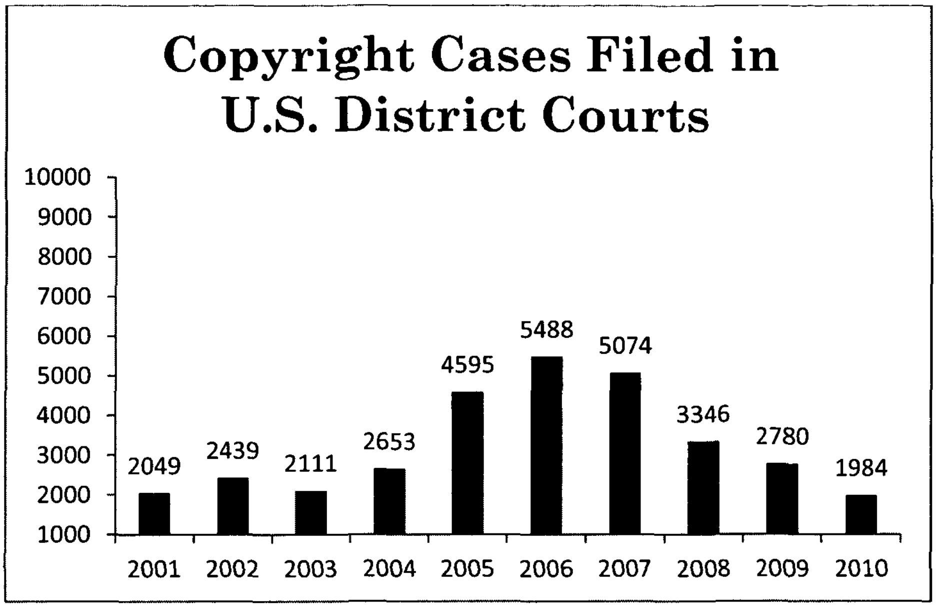
manages to preserve all of the due process protections associated with litigation, but it would be impossible to do so in a scalable way. Incorporating the right to contest allegations and limiting the duration of access-related sanctions help to mitigate harms to Internet users under both systems.

V. CONCLUSION

With each successive iteration, P2P network architecture has become not only more scalable and efficient, but also more perfectly adapted to "massive infringement." The key to effective online copyright enforcement in the P2P context is identifying and implementing enforcement strategies that are commensurately scalable. While the DMCA has scaled well with respect to enforcement of copyrights in hosted content, it has not scaled well at all for infringements over P2P networks. Rights owners continue to engage in mass John Doe litigation for convenience and efficiency, but litigation does not scale well either, particularly when the parties being aggregated en masse are defendants.

There are, however, litigation substitutes worth exploring, including voluntary notice-forwarding arrangements between ISPs and rights owners and streamlined systems of alternative dispute resolution designed specifically for the P2P context. Such systems, including the newly implemented HADOPI system in France, are untried but could succeed in proportion to their ability to honor the competing values of efficiency and fairness. Any high-volume system for enforcing copyrights online that is not both "architected" and implemented to balance these competing values will not scale and cannot succeed over the long term.

APPENDIX A



Source: Administrative Office of U.S. Courts, Federal Judicial Caseload Statistics, U.S. District Courts—Civil Cases Commenced by Nature of Suit During 12-Month Periods Ending March 31, http://www.uscourts.gov/Statistics/FederalJudicialCaseloadStatistics.aspx*

*Admin. Office of the U.S. Courts, *Federal Judicial Caseload Statistics*, UNITED STATES COURTS, http://www.uscourts.gov/Statistics/FederalJudicialCaseloadStatistics.aspx (following links for data from years 2001–2010) (last visited Feb. 22, 2011).