Master Copies, Unique Copies and Volitional Conduct: *Cartoon Network*'s Implications for the Liability of Cyber Lockers

Carrie Bodner[*]

INTRODUCTION

As technology advances, new types of devices and increasing compatibility of data formats make it possible to use files previously accessible on only one or two devices. For example, a person might wish to access a business file (formerly stored on a work computer or perhaps even in a file cabinet at the office) from her smart phone. Similarly, another might wish to access his MP3 collection (stored on an iPod or personal computer) from his work computer. Such technological progress has paved the way for innovative digital, cable and Internet services that enable users to enjoy copyrighted content in new ways: from time-shifting via VCRs[1] to place-shifting via new TV devices;[2] from instantly purchasing a movie through video on demand to watching a live stream of sports coverage on the Internet. One type of service that has recently proliferated is the digital storage locker—also known as the cyber locker.[3] Digital storage lockers enable users to

[*] J.D., Columbia Law School, 2012; B.A. English, Cornell University, 2007. Special thanks to Professor Jane Ginsburg and Professor June Besek for their insight on this Note, and for furthering my interest in and knowledge of copyright and trademark law as a law student. Many thanks to Bissie Bonner, Marissa Crespo and Rob Bernstein for their hard work and thoughtful feedback throughout the publication process, and also to Gerald Bodner, Candy Bodner, Ben Rankin and Megan Dubatowka for their encouragement and support.

1. Time-shifting is watching a television show at a later hour than its original broadcast. *See* 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8B.01[B] (Matthew Bender rev. ed. 2012) (discussing time-shifting and the landmark case *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), which held that time-shifting for private use is fair use).

2. Place-shifting is a service in which a device set by the provider receives and records television program broadcasts in one country and transmits the programs to its customers via the Internet, so that the customers can watch them from anywhere in the world. *See* Naoya Isoda, *Copyright Infringement Liability of Placeshifting Services in the United States and Japan*, 7 WASH. U. J.L. TECH. & ARTS 149, 153 (2011). Currently, U.S. place-shifting providers include Cablevision, SageTV, Orb Networks and Sony. *Id.* at 155. The term "space-shifting" was initially adopted by providers of file sharing services to favorably compare their services to that of time-shifting, which was protected by fair use. *Id.* at 155–56. Arguing that space-shifting was also fair use, such service providers claimed that a "person who owns a copyrighted compact disc who then copies the content to a digital file does not engage in infringement. Instead, that person is merely shifting material that she already owns from one 'space' to another." *See* Dominic H. Rivers, Note, *Paying for Cable in Boston, Watching It on a Laptop in L.A.: Does Slingbox Violate Federal Copyright Laws?*, 41 SUFFOLK U. L. REV. 159, 192 (2007).

3. *See, e.g.*, Jennifer Martinez, *Policing the Digital Storage Landscape*, POLITICO (Sept. 21, 2011, 10:41 PM), http://www.politico.com/news/stories/0911/64053.html (describing cyber lockers as the next "frontier" for storing movies, music and personal files on the Internet). While cyber lockers are often used for legitimate purposes, they are also frequently used by consumers to share copyrighted

upload content to a virtual locker located on a centralized server and access that content from virtually anywhere with an Internet connection.

Take, for example, the music services MP3.com and MP3tunes.com. A precursor to today's cyber lockers, MP3.com was created during a time when most consumers were still listening to music on CDs.[4] MP3.com founder Michael Robertson had the clever idea of creating a service that offered users songs in MP3 format from CDs they already owned.[5] The company purchased tens of thousands of popular CDs and—without seeking authorization from the record labels—converted them to MP3 format through the use of the new MP3 technology.[6] MP3.com offered its subscribers online access to listen to songs in MP3 format if they could prove they already owned the same song on a CD.[7] Although MP3.com portrayed its service as the "functional equivalent" of storing its users' CDs, subscribers were, in fact, listening to the converted copies made from the company's physical CD collection.[8]

About five years later, Robertson tried his hand at another digital storage locker for music with MP3tunes.com.[9] Like most cyber locker services today, MP3tunes.com allowed users to upload any MP3 files to the site's central server and play or download them again from any computer with an Internet connection.[10] Unlike MP3.com, MP3tunes users themselves provided the content they sought to access later, either from music files on their hard drive or, through the use of the MP3tunes-owned Sideload website and software, by searching for free music files on the Internet.[11]

Both MP3.com and MP3tunes were hit with copyright infringement lawsuits.[12] One site was shut down, but the other largely escaped liability (for the most part) in what was described as a legal victory.[13] Whereas MP3.com was held directly liable

content illegally. *Id.*; *see also* Ernesto, *MPAA Lashes out Against Rogue Cyberlockers*, TORRENTFREAK (Nov. 1, 2011), http://torrentfreak.com/mpaa-lashes-out-against-rogue-cyberlockers-111101/. Cyber locker providers include Rapidshare, Megaupload, Hotfile, YouSendIt, Bayfiles (from the creators of Pirate Bay) and DropBox, among others.

4. The decision in *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000), was handed down in 2000—more than a year before the first iPod was unveiled. *See* Benj Edwards, *The Birth of the iPod*, MACWORLD (Oct. 23, 2011, 6:00 AM) http://www.macworld.com/article/1163181/the_birth_of_the_ipod.html.

5. *MP3.com*, 92 F. Supp. 2d at 350.

6. *Id.*

7. *Id.* Technically, however, subscribers needed to prove only that they had access to a CD with the same song; even if the CD was borrowed from a friend, it would not have mattered.

8. *Id.*

9. *See* Capitol Records, Inc. v. MP3tunes, LLC, No. 07 CIV. 9931 WHP, 2011 WL 3667335 (S.D.N.Y. Aug. 22, 2011), *amended and superseded by* 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

10. *Capitol Records*, 821 F. Supp. 2d at 633.

11. *Id.* at 633–34.

12. For the related court opinions, see *supra* notes 4 and 9.

13. *See, e.g.*, Timothy B. Lee, *Record Labels Get Hollow Victory in MP3tunes Infringement Case*, ARS TECHNICA (Aug. 22, 2011, 6:39 PM), http://arstechnica.com/tech-policy/news/2011/08/record-labels-get-hollow-victory-in-mp3tunes-infringement- case.ars?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+arstechnica/index+(Ars+Technica+-+Featured +Content) ("If Judge William Pauley's reasoning is confirmed on appeal, it will put music locker

for copyright infringement, two factors essentially protected MP3tunes from liability: the availability of a safe harbor defense under the Digital Millennium Copyright Act,[14] and the reasoning in an influential Second Circuit opinion from 2008, *Cartoon Network LP v. CSC Holdings, Inc*.[15]

The advent of cloud computing, in which a user's files and data are stored on a central server and are accessible from just about everywhere, has raised new concerns about privacy,[16] blurred the line between the office and the home, and rendered data storage efficient in an unprecedented way. Cloud computing has also proven a puzzle to copyright law, requiring a reevaluation of some questions integral to copyright law: When is a performance public? Who makes a copy when a system is completely automated? Courts resolving copyright disputes relating to a variety of digital, cable and Internet services have attempted to answer these questions, and in doing so, they have largely shaped the legal discourse about copyright infringement and cyber lockers.

In particular, the Second Circuit's opinion in *Cartoon Network* has set the stage for cyber locker companies to avoid copyright liability for the infringement committed by its users. In *Cartoon Network*, plaintiffs, who held copyrights to numerous television programs and movies, brought suit against Cablevision, an operator of cable television systems, on the grounds that Cablevision's proposed offering of a new remote storage digital video recorder ("DVR" or "RS-DVR") would directly infringe their exclusive rights to reproduce and publicly perform their works.[17] The district court granted summary judgment for the plaintiffs and enjoined Cablevision from operating the DVR system without licenses from content providers.[18] The Second Circuit reversed, holding that Cablevision would not directly infringe plaintiffs' rights through its adoption of the DVR.[19] Notably, the Second Circuit opinion contained several key legal conclusions that will greatly decrease the likelihood of liability for cyber lockers. First, in assessing the viability of a copyright infringement claim based on the right of public performance, the

services on a solid legal foundation.").

14. The Digital Millennium Copyright Act ("DMCA") was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty. *See* Viacom Int'l, Inc., v. YouTube, Inc., 676 F.3d 19, 26 (2nd Cir. 2012) (citations omitted) (internal quotation marks omitted). It was "designed to clarify the liability faced by service providers who transmit potentially infringing material over their networks." *Id.* at 27 (citations omitted) (internal quotation marks omitted). Notably, the DMCA created four "safe harbors" that allow "qualifying service providers to limit their liability for claims of copyright infringement based on (a) 'transitory digital network communications,' (b) 'system caching,' (c) 'information residing on systems or networks at [the] direction of users,' and (d) 'information location tools.'" *Id.*; *see also* 17 U.S.C. § 512(a)–(d) (2012).

15. Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131–33 (2d Cir. 2008).

16. *See, e.g.*, Christian Cachin & Matthias Schunter, *A Cloud You Can Trust*, 48 IEEE SPECTRUM 28, 30 (Dec. 2011), *available at* http://spectrum.ieee.org/computing/networks/a-cloud-you-can-trust (stating that surveys show privacy is businesses' top concern with cloud computing).

17. *Cartoon Network*, 536 F.3d at 124.

18. *Id.* at 124.

19. *Id.* at 123.

Second Circuit drew a distinction between a master copy and unique copies.[20] Because Cablevision's DVR system transmitted a unique copy of the recorded program to the user who requested it, it was not "transmitted to the public" and thus not an infringement of the public performance right.[21] Second, the court concluded that when the DVR system automatically copied a program on the request of a viewer to make a playback copy, such copying did not constitute volitional conduct on the part of the service provider, so Cablevision could not be directly liable.[22]

This Note explores the implications of *Cartoon Network* for copyright liability of digital storage lockers. Part I.A presents an overview of the *Cartoon Network* case, including a discussion of the two aforementioned aspects of the opinion: the public performance reasoning and the volitional conduct analysis. Part I.B provides an overview of cyber locker services; in particular, it examines the structural differences between cyber lockers that are used predominantly for legitimate purposes and those that facilitate piracy. Part II features a close analysis of the *Cartoon Network* reasoning, and subsequently discusses recent copyright infringement cases against cyber locker sites MP3tunes, Megaupload and Hotfile, in which courts have applied the *Cartoon Network* reasoning.[23] In light of this recent case law, Part III assesses the implications of *Cartoon Network* for the liability of cyber lockers: Part III.A looks at the public performance reasoning; Part III.B, the volitional requirement; and Part III.C, the interaction between the DMCA and *Cartoon Network*, as seen in *Capitol Records v. MP3tunes*.[24] Finally, the conclusion offers additional thoughts and suggestions as to how to balance better the rights of copyright owners and the interests of digital storage locker providers after *Cartoon Network*.

I. AN INTRODUCTION TO *CARTOON NETWORK* AND A TAXONOMY OF CYBER LOCKERS

A. *CARTOON NETWORK*

Cartoon Network involved a legal challenge to Cablevision's remote storage digital video recorder (RS-DVR) system, which enabled Cablevision subscribers to record television shows and play them back later at their convenience.[25] DVRs had already been in existence, and those that functioned similarly to typical VCRs were

20. *Id.* at 135.

21. *Id.* at 139 ("Because each RS-DVR playback transmission is made to a single subscriber using a single unique copy produced by that subscriber, we conclude that such transmissions are not performances 'to the public,' and therefore do not infringe any exclusive right of public performance.").

22. *Id.* at 131.

23. Capitol Records Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 649 (S.D.N.Y. 2011); Perfect 10, Inc. v. Megaupload Ltd., No. 11CV0191-IEG BLM, 2011 WL 3203117, at *6 (S.D. Cal. July 27, 2011); Disney Enters., Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303, 1309–10 (S.D. Fla. 2011).

24. *Capitol Records*, 821 F. Supp. 2d at 649–50.

25. *Cartoon Network*, 536 F.3d at 124.

presumed to be protected under the *Sony* doctrine.[26] But Cablevision's RS-DVR was slightly different: rather than saving recorded programs on the user's individual set-top cable or DVR storage box, the RS-DVR stored programs remotely on central hard drives maintained by Cablevision.[27] Accordingly, the technology at issue with Cablevision was closer to today's cloud computing—in that it was stored on a central server—than to the VCR technology protected in *Sony*. Cartoon Network, Universal and other producers of copyrighted movies and TV shows sued, alleging that through the use of its RS-DVR, Cablevision made unauthorized reproductions and public performances of their works.[28] The Second Circuit reversed the district court's grant of summary judgment in favor of the plaintiffs, holding that Cablevision was not directly liable for infringement by offering the RS-DVR to consumers.[29]

Two aspects of the Second Circuit's reasoning are particularly noteworthy: (1) the distinction drawn between master copies and unique copies in analyzing the claim about the public performance right; and (2) and the treatment of automatic reproduction by a system as nonvolitional conduct.

1. Unique Copies Do Not Infringe the Public Performance Right

One of the exclusive rights granted to copyright holders in the Copyright Act is the right to perform the work publicly.[30] Section 101 contains two definitions for "public performance."[31] Under section 101(1), known as the public place clause, a performance is considered public if it occurs either "at a place open to the public" or at "any place where a substantial number of persons outside a normal circle of a family and its social acquaintances is gathered."[32] Under section 101(2), the transmit clause, a performance is public if it is transmitted to a public place (as defined in the previous subsection) or if it is transmitted to the public by means of any device or process.[33]

The plaintiffs in *Cartoon Network* argued that the playback of the recorded

26. *See, e.g.*, Jane C. Ginsburg, *Recent Developments in US Copyright Law—Part II, Caselaw: Exclusive Rights on the Ebb?* 16 (Columbia Law Sch. Pub. Law & Legal Theory Working Paper Grp., Paper No. 08-192, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1305270. In *Sony*, the Supreme Court held that the videotaping of free broadcast television by individual users for their later use ("time-shifting") was noninfringing. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1988); *see also* 2 NIMMER & NIMMER, *supra* note 1, § 8B.01[B] (describing the landmark *Sony* decision).

27. *Cartoon Network*, 536 F.3d at 123–24.

28. *Id.*

29. *Id.* at 123. The secondary liability issues were not litigated. *See, e.g.*, Vivian I. Kim, *The Public Performance Right in the Digital Age:* Cartoon Network LP v. CSC Holdings, 24 BERKELEY TECH. L.J. 263, 263–64 (2009).

30. 17 U.S.C. § 106(4) (2012). The public performance right is limited to literary, musical, dramatic, choreographic works, pantomimes, motion pictures and other audiovisual works. *Id.*

31. *See* Ginsburg, *supra* note 26, at 25 ("Public performances or displays can occur in public places, or by transmission.").

32. 17 U.S.C. § 101(1).

33. *Id.* § 101(2).

programs constituted an unauthorized public performance.[34] Because the Cablevision subscribers were watching the recorded programs on the RS-DVR in the privacy of their homes, the public performance claim hinged on whether this kind of viewing constituted a public performance under the transmit clause.[35] Cablevision argued that the customer, not Cablevision, did the transmitting and that the transmission was not "to the public."[36] The court agreed.[37] According to the court, Cablevision's remote DVR system transmitted a unique copy of the recorded program to the subscriber who requested it, and that unique copy could only be decoded "exclusively by that subscriber's cable box."[38] Because "only one subscriber is capable of receiving any given RS-DVR transmission," the Second Circuit concluded, the RS-DVR transmissions are not "to the public" within the meaning of the transmit clause.[39]

But how did the transmission of a unique copy become legally salient? The Second Circuit drew this conclusion from *Columbia Pictures v. Redd Horne*.[40] In that case, the Third Circuit held that a video rental service transmitted video performances to the public (and thus infringed the public performance right) when it played a master copy of a video for viewers in on-site private viewing rooms.[41] The court wrote: "In concluding that [the defendant] violated the transmit clause, [the Third Circuit] explicitly relied on the fact that defendants showed the same copy of a work seriatim to its clientele."[42] Although unable to find an adequate explanation in *Redd Horne*, the Second Circuit contrived a reason for the master/unique distinction: "the use of a unique copy may limit the potential audience of a transmission and is therefore relevant to whether that transmission is made 'to the public.'"[43]

2. Reproduction by an Automated System Is Nonvolitional

Since *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[44] numerous courts have held that volitional conduct is a key component in sustaining a claim of direct copyright infringement.[45] In *Netcom*, the

34. *Cartoon Network*, 536 F.3d at 134.
35. *Id.* ("The parties agree that this case does not implicate clause (1).").
36. *Id.*
37. *Id.*
38. *Id.* at 135.
39. *Id.* at 134 The court emphasized that the transmit clause speaks of "people *capable* of receiving a particular 'transmission' or 'performance,'" and not of the potential audience of a particular work. *Id.* (emphasis added).
40. *See* Columbia Pictures Indus., Inc. v. Redd Horne, Inc., 749 F.2d 154, 159 (3d Cir. 1984).
41. *Id.* ("Although Maxwell's has only one copy of each film, it shows each copy repeatedly to different members of the public. This constitutes a public performance.").
42. *Cartoon Network*, 536 F.3d at 138.
43. *Id.*
44. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1369 (N.D. Cal. 1995).
45. *See, e.g.*, *Cartoon Network*, 536 F.3d at 130 ("[V]olitional conduct is an important element of

rights holders of the written works of L. Ron Hubbard, founder of the Church of Scientology, brought a copyright suit against an Internet service provider that hosted third-party bulletin boards when a user posted portions of the works on a board without permission.[46] The court rejected the direct liability claims against the service providers on the grounds that something more was necessary to hold the service provider liable for the infringement of a user: "Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."[47] Without a requirement of volition, the acts of one person could create "many separate acts of infringement" and lead to "unreasonable liability."[48] *Netcom* was substantially codified by the DMCA.[49] Although *Netcom* was a reproduction case in the Northern District of California, the volitional conduct requirement has been embraced by courts in other circuits[50] and extended to direct infringement claims of all exclusive rights under the Copyright Act.[51]

In *Cartoon Network*, the Second Circuit adopted the volitional element in its analysis of a copyright infringement claim based on unauthorized reproduction regarding playback copies created by copying program data to storage hard disks.[52] There was no question that the playback copies were fixed copies. Instead, the question of liability turned on discerning *who* created the playback copies:

direct liability"); 3 WILLIAM PATRY, PATRY ON COPYRIGHT § 9.5.50 (2012) (discussing the volitional conduct requirement).

46. *Netcom*, 907 F.Supp. at 1365–66. The user, a former minister in the church, was also named as a defendant. *Id.*

47. *Id.* at 1369.

48. *Id.*

49. *See, e.g.*, Jane C. Ginsburg, *User-Generated Content Sites and Section 512 of the US Copyright Act*, COPYRIGHT ENFORCEMENT AND THE INTERNET 183, 188 (Irini A. Stamatoudi ed., 2010). *But see infra* Part III.C (discussing whether courts should apply *Netcom* to storing and linking service providers after the enactment of the DMCA).

50. *See, e.g.*, CoStar Group, Inc. v. Loopnet Inc., 373 F.3d 544, 550 (4th Cir. 2004). But not all circuit courts have adopted this element. *See* Andrey Spektor, *How "Choruss" Can Turn into a Cacophony: The Record Industry's Stranglehold on the Future of Music Business*, 16 RICH. J.L & TECH 3 (2009) (regarding the Ninth Circuit's lack of instruction regarding the volitional element).

51. *See, e.g.*, Perfect 10, Inc. v. Megaupload Ltd., 11CV0191-IEG BLM, 2011 WL 3203117, at *4 (S.D. Cal. July 27, 2011); Arista Records LLC v. Usenet, 633 F. Supp. 2d 124, 147 (S.D.N.Y. 2009) ("The line of cases on which the Cablevision court relied-beginning with [*Netcom*] suggest that the volitional-conduct requirement should apply equally to all exclusive rights under the Copyright Act."); 4 NIMMER & NIMMER, *supra* note 1, § 13.08[C] ("Although *Cartoon Network* addressed only the reproduction and public performance rights, subsequent cases have extended its requirement of volitional conduct across the board.").

52. Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 127, 130 (2d Cir. 2008). The plaintiffs also argued that their reproduction right was infringed when the program data went through a buffer. *Id.* at 125. Through a questionable interpretation of the Copyright Act's definition of fixed, the court held that the works were not "fixed" because they were not embodied in the buffer for a period of more than transitory duration. *Id.* at 130. Given that they were not fixed, they did not constitute copies, and plaintiff's reproduction rights were not infringed when the copyrighted program data went through the buffer. *Id.* For a discussion of the flaws in the court's understanding of the fixation requirement, see Ginsburg, *supra* note 26, at 9.

Cablevision or the RS-DVR user.[53] The distinction was important because of the litigants' agreement to drop their strongest arguments: the plaintiffs would not pursue a claim of secondary liability, and Cablevision would not raise a fair use defense.[54] Consequently, a conclusion that the copies were in fact "made" by the end user would be the end of plaintiffs' case—at least relating to the reproduction right.[55] To answer the question of authorship, the Second Circuit first invoked the volitional requirement from *Netcom*.[56]

In the court's view, there were two instances of volitional conduct in the present case, but only one was responsible for the copying: it was either Cablevision's "conduct in designing, housing, and maintaining a system that exists only to produce a copy," or the RS-DVR user's "conduct in ordering that system to produce a copy of a specific program."[57] The Second Circuit compared a copy machine operated by a store employee with a copy machine located on the proprietor's premises but operated by the customer. Although both copy machines can be used to create an infringing copy, in the former example, the human employee "volitionally operates" the machine to make that copy upon a customer's request, whereas in the latter, the machine "automatically obeys" the customer's command and "engages in no volitional conduct."[58] Because the reproduction occurred through a completely automated system, Cablevision's RS-DVR was more like the latter.[59] Thus, the Second Circuit concluded, it was the RS-DVR user, rather than Cablevision, who "made" the copy.[60]

B. TAXONOMY OF CYBER LOCKERS

Like many other Internet services, cyber locker and related cloud-based service providers offer file hosting and file sharing services over the Internet. Through a typical cyber locker service, users upload files from their own computer to their "lockers," which essentially consist of personal storage space on the service

53. *Cartoon Network*, 536 F.3d at 130.

54. *See, e.g.*, Kim, *supra* note 29, at 264. The question of authorship is of increasing importance even in the absence of such stipulations. *See* RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 15.6 (2012) ("In an environment involving increasingly 'intelligent' systems, the question of 'online who engages directly in the copying, display or performance of a work' frequently involves having to draw close distinctions, grounded in technology choices, between the actions of two or more persons.").

55. *See, e.g.*, *Cartoon Network*, 536 F.3d at 130 ("The question is *who* made this copy. If it is Cablevision, plaintiffs' theory of direct infringement succeeds; if it is the customer, plaintiffs' theory fails because Cablevision would then face, at most, secondary liability, a theory of liability expressly disavowed by plaintiffs.")

56. *Id.* at 131 ("When there is a dispute as to the author of an allegedly infringing instance of reproduction, *Netcom* and its progeny direct our attention to the volitional conduct that causes the copy to be made.")

57. *Id.*

58. *Id.* at 131–32. The court's choice of words—a machine that "obeys" a customer's "command" versus an employee operating a machine at a customer's "request"—nicely emphasizes the volitional difference between the examples.

59. *Id.*

60. *Id.* at 133; *see also* Ginsburg, *supra* note 26, at 14.

provider's centralized server. Users can subsequently reaccess their files from any other computer or device with an Internet connection, either by streaming or downloading the file.

Many cyber locker services offer both free and subscription accounts, the former having limits on storage size and download time, and the latter offering increased or unlimited storage and faster downloads.[61] With most services, users upload content to their locker via an Internet browser, although some service providers employ desktop software to make file storing even easier.[62] If what the dominant computer companies are doing is any indication, cloud-based storage will play a major role in the next generation of computing: Microsoft and Apple both updated their latest operating systems to seamlessly integrate with their respective cloud-based file storage services, SkyDrive and iCloud.[63]

Certain cyber locker providers have largely avoided acquiring reputations for facilitating piracy. DropBox, for example, is widely used among academics and businesspeople and is often grouped alongside digital storage services from reputable companies, such as Amazon and Apple.[64] One reason might be attributable to marketing: services like DropBox and Amazon Cloud are pitched primarily as a backup service, similar to an external hard drive.[65] Although file sharing is also a large part of cloud-based services like DropBox and Google Docs, the purpose of file sharing through these services tends to be for productive or business use, rather than for entertainment.[66] For example, a major benefit of

61. *See, e.g.*, *Premium Accounts*, HOTFILE, http://hotfile.com/premium.html (last visited Mar. 4, 2013); *Pricing*, DROPBOX, http://www.dropbox.com/pricing (last visited Mar. 4, 2013). In light of the growing number of cyber lockers, one tech blog made a chart comparing the amount of storage, file size limit, account price (if any) and upload methods of various digital storage lockers. *See* Kevin Purdy, *Free Online Storage Feature-by-Feature Comparison Chart*, LIFEHACKER (Oct. 17, 2008, 10:00 AM), http://lifehacker.com/5064688/free-online-storage-feature+by+feature-comparison-chart.

62. *See, e.g.*, Victoria Barrett, *Dropbox: Files Without Borders*, FORBES (June 10, 2010, 12:40 PM), http://www.forbes.com/forbes/2010/0628/technology-file-sharing-dropbox-google-files-without-borders.html (describing Dropbox's desktop software).

63. *See* Peter Bright, *Bigger Files, Remote Access, Open Document, and More Coming to SkyDrive*, ARS TECHNICA (Feb. 20, 2012, 1:35 PM), http://arstechnica.com/microsoft/news/2012/02/bigger-files-remote-access-opendocument-and-more-coming-to-skydrive.ars (discussing updates to Microsoft's Skydrive to integrate it with Windows 8); *see also* Sarah Perez, *Apple's iCloud Is No Dropbox Killer (It's Much More)*, TECHCRUNCH (Feb. 16, 2012), http://techcrunch.com/2012/02/16/apples-icloud-is-no-dropbox-killer-its-much-more/ (describing Apple's deep integration of iCloud in its newest operating system as "building a new computer paradigm.").

64. Dropbox has not, however, completely avoided legal controversy: an FTC complaint alleged Dropbox failed to adequately inform users that it had the capacity to access and view all uploaded files. *See* George Wong, *Dropbox Isn't as Safe as You Thought*, UBERGIZMO (May 13, 2011, 4:37 PM), http://www.ubergizmo.com/2011/05/dropbox/.

65. *See, e.g.*, Janko Roettgers, *Will the MPAA Target RapidShare, Megaupload or Dropbox?*, GIGAOM (Feb. 9, 2011, 12:33 PM), http://gigaom.com/video/mpaa-lawsuit-hotfile-rapidshare-megaupload-dropbox/ (referring to Dropbox as a backup service).

66. *See, e.g.*, Jon Brodkin, *Before Shutdown, Megaupload Ate up More Corporate Bandwith than the Dropbox*, ARS TECHNICA (Jan. 19, 2012, 5:01 PM), http://arstechnica.com/business/news/2012/01/before-shutdown-megaupload-ate-up-more-corporate-bandwidth-than-dropbox.ars (noting a distinction between "tools that help me get my job done and tools that help us stay entertained"). In addition to storing and sharing files with others, Google Docs offers a web-based Word processor that enables users

DropBox and Google Docs is that both services synchronize different versions and drafts of a particular document such that multiple users can simultaneously work on that document, from different locations, with all edits instantaneously reflected in the master file.[67]

But the business/entertainment distinction is not the defining line: some cyber locker sites and software that are strictly for storing music files have nevertheless avoided an illicit reputation, like iTunes Match, Amazon Cloud Player and Google Music Beta.[68] The legitimacy of these locker services is certainly linked to their affiliation with such reputable tech companies. It might also help that all three services go hand-in-hand with the companies' online stores that sell digital music legitimately (iTunes, Amazon.com and Google Music, respectively).[69] Because many users might have an extensive digital musical collection, some of these cyber locker services facilitate uploading content into the cloud by automatically uploading any song files purchased through the service provider's MP3 store, such as iTunes or Amazon.[70]

On the opposite end of the spectrum is a type of cyber locker sites, often called "direct download links" or "one-click file hosts," which are widely known as breeding grounds for copyright infringement. These cyber lockers, which include Rapidshare, Hotfile, Megaupload, MediaFire and 4Shared, among others, share certain structural and business elements that facilitate the use of their services for unlawful file sharing. Through these locker services, users upload a file on a Web browser, and the service automatically generates a URL (or "hotlink") specific to that file's location on the server.[71] The user can subsequently retrieve the file again by going to that URL from any Internet browser and downloading the file. Because of the nature of file retrieval, the direct download link cyber lockers typically lack any restriction on who can subsequently download a file—anyone who has the

to create documents through their web browsers, without having to open up the application. *See, e.g.*, Anne Eisenberg, *Digital Storage Options for Workers on the Go*, N.Y. TIMES, Jan. 18, 2009, at BU4.

67. *See, e.g.*, Eisenberg, *supra* note 66, at BU4. iCloud also has a useful synchronization function: synching information stored on different applications. *See* Perez, *supra* note 63 ("But Apple's iCloud is not just about building a better Dropbox—it's about keeping everything in sync: Mail, Contacts, Calendars, Reminders, Bookmarks, Notes, Photos, Accounts, and more.").

68. Both Google and Amazon also have general cloud-based lockers for storing all types of files (Google Docs and Amazon Cloud, respectively), in addition to more specific services or applications for storing and syncing music files (for example, Google Music and Amazon Cloud Player). *See* Claire Cain Miller, *Amazon Introduces a Digital Music Locker*, N.Y. TIMES (Mar. 29, 2011, 12:42 AM), http://bits.blogs.nytimes.com/2011/03/29/amazon-introduces-a-digital-music-locker/?scp=7&sq=digital%20storage%20locker&st=cse.

69. While Apple and Amazon's music lockers were created after the companies began selling digital music files, Google's locker service predated its music store. *See* Ben Sisario, *Google Opens a Digital Music Store*, N.Y. TIMES (Nov. 16, 2011, 6:55 PM), http://mediadecoder.blogs.nytimes.com /2011/11/16/google-opens-a-digital-music-store/?scp=1&sq=% 22google%20music%22&st=cse.

70. *See* Miller, *supra* note 68.

71. *See, e.g.*, Roettgers, *supra* note 65 (stating that direct download link sites like Hotfile allow users to directly link or "hotlink" files hosted on the server); *see also* Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 704 (2011) (describing RapidShare and MegaUpload as direct download links).

URL can download it.[72] The user can send the URL to third parties, even those without cyber locker accounts of their own, or the user could post the URL on a bulletin board so that third parties can download the same content.[73] Although services like Dropbox and iCloud also enable file sharing, such file sharing services are substantially more private and subject to greater restrictions than the file sharing services offered by the direct download links.[74] Moreover, whereas one-click file hosts could feasibly make the links expire after a certain time period or number of subsequent downloads, many choose not to do so.[75]

Although virtually all of these cyber locker companies prohibit uploading copyrighted content in their terms of use,[76] it is unsurprising that the direct download link locker services are frequently—and perhaps predominantly—used to store and share pirated works.[77] Many of these cyber locker providers actually

72. Disney and the other plaintiffs alleged in their complaint that Hotfile "engineers its URL links so that anyone can download the linked-to content," despite its ability to "substantially mitigate the massive public distribution of copyrighted content by password-protecting the ability to download files, thereby ensuring that only the account-holder (or those individually authorized by the account-holder) could make copies of the files uploaded by the account-holder." *See* Complaint for Copyright Infringement at 13, Disney Enters., Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303 (S.D. Fla. 2011) (No. 11CV20427).

73. *See, e.g.*, Seth Ericsson, *The Recorded Music Industry and the Emergence of Online Music Distribution: Innovation in the Absence of Copyright (Reform)*, 79 GEO. WASH. L. REV. 1783, 1795 n.55 (noting that direct download links can be posted on Internet message boards or blogs). In fact, sharing a file easily with friends was one of the purposes the founder of RapidShare sought to fulfill. *See About Us*, RAPIDSHARE, https://rapidshare.com/#!rsag_about (last visited Mar. 4, 2013).

74. *See* Matt Burns, *With MegaUpload Down, Who's Next? RapidShare? SoundCloud? DropBox?*, TECHCRUNCH (Jan. 20, 2012), http://techcrunch.com/2012/01/20/megaupload-computer-abuse-reinforcement-education (describing file sharing through DropBox, iCloud and Amazon S3 as inherently more private than file sharing through MegaUpload).

75. For example, Hotfile states in its Frequently Asked Questions: "In principle, we host data without a time limit," although expiration is clearly possible, as "files that have not been accessed for 90 days are deleted to relieve the system of forgotten and not needed content." *See FAQ*, HOTFILE, http://www.hotfile.com/faq.html (last visited Mar. 4, 2013). Note, however, that this rule does not apply to premium account members, whose hotlinks are apparently never deleted for systematic cleaning. *Id.* Similarly, Hotfile does not limit the number of daily downloads, although free account holders are subject to a thirty minute wait between downloads. *Id.*

76. *See, e.g.*, *Terms of Service*, HOTFILE, http://hotfile.com/terms-of-service.html (last visited Feb. 15, 2013) ("You promise that you have all intellectual property rights (including without limitation copyright and trademark rights), licenses, and permissions that may be needed to upload, store, or share your User Content. By uploading, storing, or sharing any User Content, you promise that doing so does not infringe any intellectual property rights of another person.").

77. *See, e.g.*, Perfect 10, Inc. v. Megaupload Ltd., No. 11CV0191-IEG BLM, 2011 WL 3203117, at *2 (S.D. Cal. July 27, 2011) ("This much is clear: Megaupload allegedly stores billions of dollars of 'pirated' full-length movies, songs, software, and images on its servers."); *see also* Eriq Gardner, *Read the MPAA's Big Lawsuit Against 'Cyberlocking' Site Hotfile*, HOLLYWOOD REP. (Feb. 8, 2011), http://www.hollywoodreporter.com/blogs/thr-esq/read-mpaas-big-lawsuit-cyberlocking-97400 (describing Paramount Pictures COO Fred Huntsberry's declaration that cyber lockers are Hollywood's biggest threat). Traditionally, copyright piracy referred to the unauthorized copying or manufacturing of protected material, to be distributed and sold, for commercial gain. *See* Darrell Panethiere, *The Persistence of Piracy: The Consequences for Creativity, for Culture, and for Sustainable Development*, E-COPYRIGHT BULL., July-Sept. 2005, at 2, *available at* http://portal.unesco.org/culture/en/files/28696/11513329261panethiere_en.pdf/panethiere_en.pdf. However, a modern version of copyright

offer monetary incentives to users who substantially increase web traffic, such as paying cash to a user when a file uploaded by that user is downloaded more than one thousand times.[78] Additionally, users who pay for premium accounts can typically avoid any restrictions on download speed or wait time.[79] With business tactics like this, it is no wonder several of the direct download link type of cyber locker sites have made their way onto lists of the world's most trafficked websites.[80] Accordingly, there is a strong argument that such cyber lockers induce, contribute to and profit from the infringement that takes place through their services.[81]

From the legitimate to the questionable, all cyber lockers have two key features in common: one that reduces the use of the service for piracy, and another that somewhat competes with the first. First, most cyber lockers lack one structural element common to many file sharing systems which were notorious for facilitating infringement: a search function through which a user can search through the respective pool of shared files to find and download files.[82] As many cyber locker providers market their lockers for personal use only, permitting third parties to access content stored in another's locker without that user's permission would undermine the (alleged) purpose.[83] However, there have been allegations that some

piracy generally includes any infringement of another's exclusive rights to a copyrighted work, even without an economic gain. *See id.* Thus, the unauthorized distribution of copyrighted works over the Internet, even without any economic gain, would generally be considered piracy. *E.g.*, *id.*; *see also What is Online Piracy?*, RIAA, http://www.riaa.com/physicalpiracy.php?content_selector=What-is-Online-Piracy (last visited Apr. 8, 2013).

78. *See* Disney Enters., Inc. v. Hotfile Corp., 798 F.Supp.2d 1303, 1306–07 (S.D. Fla. July 8, 2011) (describing Hotfile's incentives plan); *see also Megaupload*, 2011 WL 3203117, at *2 (describing Megaupload's Rewards programs); Roettgers, *supra* note 65 (stating rewards systems like Hotfile's are a business model common to one-click file hosts).

79. *See, e.g.*, Ernesto, *supra* note 3.

80. *See* Bill Wyman, *So Long, and Thanks for All the Piracy*, SLATE (Jan. 20, 2012, 6:08 PM), http://www.slate.com/articles/business/technology/2012/01/megaupload_shutdown_what_the_site_s_departure_means_for_other_traffic_hogging_cyberlockers_.html. For example, the cyber locker site MediaFire currently appears at number sixty-five on a list of the most-visited sites, based on web traffic over the past three months. *See MediaFire.com Site Info*, ALEXA, at http://www.alexa.com/siteinfo/mediafire.com (last visited Mar. 4, 2013). Approximately fifty-three percent of visits to MediaFire.com consist of only one page view. *Id.*

81. The district court in *Megaupload* specifically noted that, in its motion to dismiss, the cyber locker company did not even dispute the allegation that it induces, causes or materially contributes to infringing conduct. *Megaupload*, 2011 WL 3203117, at *6.

82. Napster's search engine, located on a centralized server, played a large part in the finding of liability. *See generally* Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345 (describing the *Napster*, *Grokster* and *Aimster* copyright suits and the structural differences between the respective services). *See also* Roettgers, *supra* note 65 (comparing Hotfile to file sharing services like Napster which "got in trouble because they offered a central, searchable index of files to download").

83. *See, e.g.*, *FAQ*, *supra* note 75 ("Q: Can I search the Hotfile server for certain files? A: No. Hotfile protects the privacy of our users. Only the person storing a file on Hotfile gets the download link. That person decides who should have access to the link. A file can only be downloaded if the download link details are known."). Of course, in the case of direct download links, a recipient can pass the URL for the shared file to countless third parties, who would technically be able to access the work

of the direct download link sites make payments to third party sites that catalog URLs of popular, infringing work stored on the cyber lockers servers.[84]

Second, most of the cyber locker services do not restrict the type or original source of file that can be uploaded, other than by limits on file size. For example, instead of storing all MP3s regardless of original source, Apple could feasibly restrict the use of its locker service to storing only MP3s purchased through its iTunes store.[85] In fact, Apple limits MP3 storage in this respect on one of its cloud services, iCloud.[86] But through its counterpart locker service, iTunes Match, subscribing customers can store music obtained from other sources, even music the customer imported from CDs.[87] Similarly, Amazon also permits all music files to be uploaded, and it only gives incentives to store music purchased from its stores.[88] One might guess that these companies feel that restricting their entire digital locker service to storage of files purchased through their online store would broadly limit the utility and attractiveness of such storage services. Both iTunes Match and Google Music limit the manner in which users can reaccess stored content, however: iTunes Match enables only streaming transmissions of stored content, rather than download transmissions; in contrast, Google Music apparently permits download transmissions, as well as streaming transmissions, as long as the download transmission contains music purchased through its music store.[89]

Because of this second characteristic, virtually all cyber locker providers face a common problem: an inability to ascertain whether an upload file was purchased legally elsewhere or downloaded illegally.[90] In fact, cyber locker precursor MP3.com arguably made more of an attempt to verify ownership (however easily evaded) at the upload stage than most modern cyber lockers.[91] Those who portray their service as primarily an external hard drive may not see any legal problem. For example, Amazon's director of music declared: "We don't need a license to store music."[92] In spite of such assurances, a multitude of copyright questions exists

without needing express approval from the initial uploader.

84. This was alleged in the complaint against Megaupload. *See Megaupload*, 2011 WL 3203117, at *2.

85. *See* Miller, *supra* note 68.

86. *See iCloud*, APPLE, http://www.apple.com/icloud/features/ (last visited Mar. 4, 2013) (stating that iCloud will store new and past music purchased on iTunes).

87. *See iTunes Match*, APPLE, http://www.apple.com/itunes/itunes-match/ (last visited Mar. 4, 2013).

88. For example, Amazon's Cloud Player automatically uploads songs users bought on Amazon, but users have to manually upload songs purchased from other music stores. *See* Miller, *supra* note 68.

89. *See id.*; *see also* Jacqui Cheng, *Google Opens Music Download Store, Welcomes Artists to Upload Directly*, ARS TECHNICA (Nov. 16, 2011, 6:43 PM), http://arstechnica.com/gadgets/news/2011/11/google-opens-music-download-store-welcomes-artists-to-upload-directly.ars. For an explanation of the difference between download and stream transmissions, see *infra* Part III.A.

90. *See, e.g.*, Miller, *supra* note 68 (describing an issue common to all cyber lockers).

91. In order to access a specific digital song, an MP3.com user had to "prove" he owned a copy of it on a CD digital file either by inserting the copy of his CD into his CD-ROM drive, or purchasing the CD from one of the site's cooperating online retailers. *See* UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000).

92. *See* Miller, *supra* note 68.

when cyber locker services are used to store copyrighted content, even that which is purchased legally: Is what is stored in the locker technically a copy of a work, and, if so, does it violate the reproduction right? When a user streams a file stored in his or her locker, does that constitute a public performance within the meaning of the Copyright Act? If a user shares a copyrighted work stored in his or her locker with others, without authorization from the right holder, could the cyber locker provider be held directly or secondarily liable?

Despite the proliferation of cyber locker services, there is very little case law on them, in part because of their relative novelty.[93] Judicial opinions, however, in three recent cyber locker cases involving MP3tunes, Megaupload and Hotfile, discussed in Part II, shed some perspective on these questions.

II. ASSESSMENT OF THE *CARTOON NETWORK* REASONING AND ITS APPLICATION IN THE *MP3TUNES*, *MEGAUPLOAD* AND *HOTFILE* DECISIONS

At first glance, it might seem unlikely that the reasoning in a case about a cable television provider's DVR system would have any impact whatsoever on cyber lockers because of basic structural differences in the technologies. For example, a DVR user is more limited in the variety of content (i.e., scheduled television programming) he can record through DVR, whereas a cyber locker user could conceivably upload a variety of types of content (music, television shows, movies, documents, spreadsheets and so on) obtained from numerous sources. Additionally, the nature of the DVR system places inherent limitations on the performance of stored content (and arguably precludes unauthorized distribution): although the user can watch the recorded content upon his demand, it will play only on that very DVR machine or on select TVs with receivers or set tops in that home.[94] But direct download cyber lockers facilitate subsequent distribution: the

93. Litigation strategy is another reason for the lack of case law: several cyber lockers have gained a bit of a reputation for quickly settling, and organizational plaintiffs like the MPAA have taken their time to bring select, strategic suits. *See* enigmax, *Hotfile Battles MPAA over Private User Data Disclosure*, TORRENTFREAK (June 25, 2011), http://torrentfreak.com/hotfile-battles-mpaa-over-private-user-data-disclosure-110625 (suggesting the MPAA chose to go after Hotfile in particular because of Hotfile's track record for settling quickly and relative lack of might compared to Megaupload and Rapidshare).

94. Some television service providers now offer "multi-room" services in which a user can watch recorded content on multiple TVs in her house, which is advertised to allow for a more "seamless" user experience. *See SAMSUNG Announces Set-Top "Boxless" Viewing in All 2012 Smart TVs*, SAMSUNG (Jan. 9, 2012), http://www.samsung.com/us/news/20087; *see also About Verizon FiOS TV Multi-Room DVR*, VERIZON, http://www22.verizon.com/support/residential/tv/fiostv/receivers/multi-room+dvr/multi-room+dvr.htm (last visited Apr. 8, 2013); *Direct TV Whole-Home DVR*, DIRECTV, http://www.directv.com/technology/wholehome (last visited Apr. 8, 2012). Yet even with this service, the television subscriber's use and enjoyment of stored content is still tethered to her home: typically, only televisions with a corresponding receiver or set-top box will be able to access the content stored on the primary DVR player. *See, e.g.*, *About Verizon FiOS TV Multi-Room DVR*, *supra* (explaining that each TV set must be connected to a set-top box in order to play stored content); *What Is the Maximum Number of TVs that Can Share One HD DVR?*, DIRECTV, http://support.directv.com/app/answers/

download URL is all that is needed to send an exact copy of the content to others.[95]

Despite such differences, DVRs and cyber lockers share a common feature: each employs automated technology to enable users to store and subsequently reaccess or play content, and grants users increased control over when (for both DVRs and cyber lockers) or where (for cyber lockers) such subsequent access will take place. In this respect, and as will be discussed below in Part II.A, *Cartoon Network*'s formulation of how transmissions, performances and reproductions that take place on an automated system fit into and coexist with our copyright scheme carries particular relevance for both cyber locker providers and rights holders. Parts II.B and II.C examine three recent cyber locker cases in which the *Cartoon Network* reasoning was applied.

A. ASSESSMENT OF THE *CARTOON NETWORK* REASONING

1. Public Performance Right

Although a bright line rule distinguishing master copies from unique copies has its efficiencies, such a rule is based on an interpretation of the transmit clause which is inconsistent with the statutory text.[96] First, the transmission clause specifies "capable of receiving a performance," yet the Second Circuit seemed to interpret it as capable of receiving a particular *transmission*. As Professor Ginsburg states:

> The court's declaration "that when Congress speaks of transmitting a performance to the public, it refers to the performance created by the act of transmission," demonstrates that the court confused "performance" and "transmission." The statute does not refer to the performance *created* by the act of transmission. The transmission does not itself "perform" (as in "play" or "render") the work; it communicates a work so that its performance will be perceived as the member of the public receives the communication.[97]

Second, even if the court's interpretation were correct—that the performance is created by a transmission—then only simultaneous transmission can be to the

detail/a_id/2734 (last visited Apr. 8, 2013) ("With DIRECTV's Whole-Home DVR service, up to 15 TVs can share one DVR. One of them must be connected to the HD DVR receiver and the others must be connected to HD receivers"). In this respect, television service providers maintain substantial control over the performance of the stored content.

95. *See supra* Section I.B (discussing the structure of direct download links).

96. *See, e.g.*, Ginsburg, *supra* note 26, at 26 ("The court's parsing of the text of the Copyright Act is peculiar if not perverse.").

97. *Id.* The Second Circuit nevertheless persisted with this interpretation in a subsequent opinion: "As we concluded in *Cartoon Network*, 'when Congress speaks of transmitting a performance to the public, it refers to the performance created by the act of transmission,' not simply to transmitting a recording of a performance. ASCAP's alternative interpretation is flawed because, in disaggregating the 'transmission' from the simultaneous 'performance' and treating the transmission itself as a performance, ASCAP renders superfluous the subsequent 'a performance . . . of the work' as the object of the transmittal."). United States v. Am. Soc'y of Composers, Authors & Publishers, 627 F.3d 64, 73 (2d Cir. 2010), *cert. denied*, 132 S. Ct. 366 (2011).

"public."[98] But the transmit clause expressly contemplates the possibility of serial receipt of the transmission by encompassing a performance regardless of "whether the members of the public . . . receive it . . . at the same time or different times."[99] Accordingly, the court's interpretation would obviate part of the statutory definition of public performance by transmission.[100]

In addition to conflicting with the statutory text, the court's reading of the transmit clause broadly limits the public performance right in two ways. First, whenever a transmission is tailored to a particular person, such that only that person is capable of receiving that transmission, it is not "to the public."[101] It is easy to see how many transmissions could be reframed as "unique" and thus nonpublic under this reasoning. For example, when a customer purchases a movie on demand via Cablevision, the transmission is (presumably) customized to reach that paying customer's cable box.[102]

In addition, the Second Circuit's interpretation of the transmit clause also creates a legal distinction between downloading and streaming. When the focus is (incorrectly) on the performance *created by* the act of transmission, one might note a difference between streaming transmissions, in which the audiovisual work plays while it is transmitted, and download transmissions, in which the work can only be played after transmission. Under this logic, it must follow that content delivered through a streaming transmission constitutes a public performance, whereas content delivered by a download transmission does not.[103] The Second Circuit reached these conclusions in *United States v. American Society of Composers, Authors and Publishers*, where it reiterated its flawed reading from *Cartoon Network*.[104]

98. Ginsburg, *supra* note 26, at 26 ("[I]t is not possible to transmit a performance 'created by the act of transmission' to members of the public 'at different times.'").

99. 17 U.S.C. § 101 (2012); *see also* Ginsburg, *supra* note 26, at 25.

100. Ginsburg, *supra* note 26, at 26 ("The court's interpretation thus reads non simultaneous receipt out of the statute.").

101. *Id*.; *see also* Jeffrey Malkan, *The Public Performance Problem in Cartoon Network LP v. CSC Holdings, Inc.*, 89 OR. L. REV. 505, 532 (2010) ("Switching the words 'performance' and 'transmission' changed the outcome of the case because there will be viewers who will be capable of receiving a performance of a network telecast (subscribers to Cablevision's feed of HBO) but not capable of receiving particular transmissions of that performance (nonsubscribers to Cablevision's RS-DVR service). This is because nonsubscribers won't have access to any RS-DVR copies, and even RS-DVR subscribers will have access only to their own copies.").

102. *See, e.g.*, Ginsburg, *supra* note 26, at 26 (suggesting on-demand services might be nonpublic under the Second Circuit's reading of the transmit clause). This is an interesting twist, as Cablevision emphasized the unique copy distinction in order to distinguish itself from video on demand. *See* Malkan, *supra* note 101, at 522 ("The challenge that Cablevision faced was to distinguish RS-DVR from VOD. It would have to convince the court that RS-DVR would not give rise to public performances because each RS-DVR transmission would emanate from a distinct copy.").

103. The proposed and ultimately unenacted legislation to stop online piracy included higher criminal penalties for illegal streaming, because as it currently stands, the maximum possible penalty for criminal streaming is a misdemeanor, which discourages prosecutors from pursuing cases of willful, criminal streaming. *See Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. 8 (2011) (statement of Maria A. Pallante, Register of Copyrights).

104. *See* 627 F.3d 64, 74–75 (2d Cir. 2010).

2. Volitional Conduct

Like the public performance reasoning, the Second Circuit's volitional conduct analysis has raised numerous questions.[105] In particular, was it proper to extend *Netcom*, which concerned an Internet service provider, to cable television? *Netcom* was motivated by the concern that, absent a volitional element, the entire Internet could be held liable for the conduct of a single user.[106] Although the *Cablevision* district court thought *Netcom* should be limited to its Internet context, the Second Circuit expressly disagreed, finding the volitional element a "particularly rational interpretation of § 106, rather than a special-purpose rule applicable only to ISPs."[107] Yet even if the substantive context were similar enough, the *Netcom* decision was handed down in 1995; significant changes in technology and copyright law have since taken place.[108]

The Second Circuit's decision to impose a volitional element at all was also somewhat surprising.[109] Is volitional conduct merely a subcomponent of an infringement claim that has always existed (just not explicitly), or did *Cartoon Network* essentially create an affirmative defense for service providers?[110] One hypothesis suggests that lurking behind the court's reasoning was an implicit conclusion that the services of the RS-DVR were all too similar to those of the VCR, which the Supreme Court deemed noninfringing in *Sony Corp. of America v. Universal City Studios*.[111]

Much confusion remains regarding the volitional element. Although the Second Circuit described what is *not* volitional conduct when it comes to automated systems, what exactly *is* volitional conduct when it comes to an automated service? Moreover, should it apply to Internet service providers who may be eligible for safe harbor protection under the DMCA? These questions will be further explored below through a comparison of cyber locker cases that reached different

105. *See, e.g.*, Ginsburg, *supra* note 26, at 15 ("[I]t is not clear that volition must always be a distinct element of the violation of the reproduction right.").

106. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995); *see also* Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121,131 (2d Cir. 2008) (discussing the *Netcom* court's concern).

107. *Cartoon Network*, 536 F.3d at 131. This is the same conclusion the Fourth Circuit reached in *CoStar*. *See* CoStar Group, Inc. v. Loopnet Inc., 373 F.3d 544, 549 (4th Cir. 2004).

108. For example, the legal disputes over Napster and Grokster and the enactment of the DMCA. Professor Nimmer describes the *Netcom* decision as an appropriate resolution of the "novel issues then pending," but "inapposite at present" in light of amendments to the Copyright Act. 4 NIMMER & NIMMER, *supra* note 1, § 13.08[C]. Furthermore, there is an argument that the DMCA codified *Netcom*'s volitional requirement for some but not all of the safe harbors. *See infra* Part III.C.

109. *See, e.g.*, 4 NIMMER & NIMMER, *supra* note 1, § 13.08[C] (describing the Second Circuit's description of volition as an element as "revolutionary," given that cases up to the Supreme Court level have defined only two elements for copyright infringement).

110. *E.g.*, *id.*

111. *See* Ginsburg, *supra* note 26, at 16 ("Because the users' were engaged in a higher-tech form of 'time shifting,' and, under *Sony*, time shifting (at least of free broadcast television) is non infringing, then the higher-tech version must be non infringing, too. That calculus may have informed the court's assessment of 'who' made the copy.").

conclusions about volition, despite nearly identical facts.

B. THE *MP3TUNES* DECISION[112]

On the spectrum from respected digital storage services to the less scrupulous direct download link providers, MP3tunes.com sat somewhere in the middle. Although the service did not offer monetary incentives for uploading content that generated vast web traffic, it facilitated searching for free content on the web. MP3tunes worked in conjunction with other software created by Robertson to facilitate finding and storing content in lockers. MP3tunes's partner program and website, Sideload.com, featured a search engine that enabled users to search for free songs on the Internet by keywords, such as an artist's name; it also enabled users to play or download ("sideload") the songs into their storage lockers.[113] MP3tunes kept track of the sources of songs in users' lockers, including (because of Sideload) third-party websites from which users sideloaded songs.[114] Moreover, Sideload's searching capability improved as more users used it: whenever a user sideloaded a song, the artist, song and third-party website would be added to Sideload's search engine database.[115]

The copyright dispute began when record label EMI sent takedown notices identifying infringing songs and the URLs of websites that had posted these songs without authorization. EMI also demanded that MP3tunes remove all other content by the identified EMI artists.[116] MP3tunes removed links on Sideload.com to the identified URLs, but it did not remove from users' lockers songs which had been sideloaded from those websites.[117] It also asked EMI to identify additional infringing links, but EMI declined, stating the representative list was sufficient.[118] EMI subsequently initiated a copyright suit, claiming infringement of its reproduction, distribution and public performance rights, as well as secondary liability for inducing copyright infringement.[119] On the direct infringement claims, the court granted summary judgment in part for MP3tunes because it complied with its obligations under section 512 and thus qualified for safe harbor.[120] Nevertheless, it was not protected by the safe harbor for its failure to remove from storage lockers songs that had been sideloaded from the sites listed in the takedown notices.[121] With respect to those songs, the court granted summary judgment on

112. Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

113. *Id.* at 634. Sideload offered free plug-in software that enabled users to sideload free songs on third-party websites directly from the third-party site via a Sideload button. *Id.*

114. *Id.*

115. *Id.* ("Thus, as users discover free songs on the Internet, the number of songs available through Sideload.com increases.")

116. *Id.* at 635.

117. *Id.*

118. *Id.*

119. Complaint, *MP3tunes*, 821 F. Supp. 2d 627 (No. 07 CIV 9931).

120. *See MP3tunes*, 821 F. Supp. 2d at 646.

121. *Id.*

the contributory liability claims for EMI.[122]

Overall, the decision was widely viewed as a victory for cyber lockers, particularly for two reasons: (1) the application of the *Cartoon Network* public performance reasoning protected a widely-used digital storage technique; and (2) that MP3tunes largely escaped liability because of a safe harbor under the DMCA.[123]

First, through the application of the master/unique distinction, the opinion endorsed a common data compression method known as deduplication.[124] The court found that MP3tunes did not use a master copy to store or play back songs stored in the digital locker: its system, which incorporated a "standard data compression algorithm that eliminates redundant digital data," preserved the "exact digital copy of each song uploaded."[125] Some critics feared the *Cartoon Network* distinction between master copies and unique copies implied that Internet service providers would be more vulnerable to copyright claims if they used deduplication to save hard drive space.[126] But *MP3tunes* ratified the use of this technology because the company retained unique copies of the music files, and thus any performances were not to the public under the transmit clause.[127]

An examination of the underlying technology suggests this conclusion about MP3tunes' storage technology is somewhat dubious. MP3tunes used a standard algorithm that created an identification number, or hash tag, based on the data sequences in a music file.[128] But if "different users upload[ed] the same song containing identical blocks of data to MP3tunes' servers," those blocks were assigned the same hash tag and "typically saved only once."[129] When a user played or downloaded a song from the cyber locker, MP3tunes' storage system used "the hash tags associated with the uploaded song to reconstruct the exact file the user originally uploaded to his locker."[130] Consequently, the district court's conclusion that the service "preserved" the unique digital copy uploaded by a user depends on the following conclusions: that the saving of the data comprising a particular increment of a song does not constitute a master copy, although each part of a song is saved only once; and that the "reconstruction" of the exact file uploaded, from

122. *Id.* at 643.

123. *See, e.g.*, Timothy B. Lee, *Record Labels Get Hollow Victory in MP3tunes Infringement Case*, ARS TECHNICA (Aug. 22, 2011, 6:39 PM), http://arstechnica.com/tech-policy/2011/08/record-labels-get-hollow-victory-in-mp3tunes-infringement-case/.

124. *See, e.g.*, *id.*; *see also* Timothy B. Lee, *Unlicensed: Are Google Music and Amazon Cloud Player Illegal?*, ARS TECHNICA (July 4, 2011, 7:00 PM), http://arstechnica.com/tech-policy/2011/07/are-google-music-and-amazon-cloud-player-illegal/ (stating that deduplication techniques are common to the IT industry, used by mail servers, cloud-storage systems and backup software).

125. *MP3tunes*, 821 F. Supp. 2d at 650.

126. Lee, *supra* note 123 (stating that the *Cartoon Network* decision had suggested that locker sites would be more vulnerable to copyright infringement claims if they used deduplication technology to save hard drive space).

127. *See MP3tunes*, 821 F. Supp. 2d at 650.

128. *Id.* at 634.

129. *Id.*

130. *Id.*

these singularly-saved chunks of data, forms a unique copy.

The second noteworthy aspect of the *MP3tunes* decision is the great extent to which MP3tunes was protected by the safe harbor defense—and the lack of substantial hurdles to qualify for the defense. As Internet service providers who store material at the direction of users, cyber lockers are likely to seek safe harbor under the DMCA. One of the requirements for claiming the safe harbor is that service providers must promptly remove or disable access to unauthorized material identified in notices by rights holders.[131] But this removal obligation does not extend particularly far: take-down notices must identify more than just the copyrighted work that is allegedly infringed; they must also provide reasonably sufficient information for the service provider to locate the infringing material (usually by providing the URL).[132] The DMCA does not impose an affirmative duty to monitor for infringement.[133]

Accordingly, the district court held that MP3tunes' responsibility for searching the contents of storage lockers on its servers was limited to that which was specified in the notices from EMI and which its system was capable of searching—i.e., MP3tunes only had to search its storage lockers for content from the third-party websites, specified in EMI's takedown notices, and remove the same.[134] Beyond that, MP3tunes had no obligation to conduct a "burdensome investigation in order to determine whether songs in its users' accounts were unauthorized copies."[135]

A counterfactual raises questions about willful blindness: suppose MP3tunes did not own Sideload.com and thus lacked the capability of tracking the source (via URL) of the works uploaded into lockers. In this respect, it would be more akin to the direct download link type of cyber lockers, like Hotfile. Even if rights holders were somehow able to search the lockers to identify infringing content in takedown notices,[136] the cyber locker company would still have to ascertain whether copies of the work were authorized or unauthorized on a locker-by-locker basis. In that case, the court's statement rejecting a "burdensome investigation" seems to imply there would be no takedown obligation.

131. 17 U.S.C. § 512(c)(1)(C) (2012).

132. *See, e.g.*, 3 NIMMER & NIMMER, *supra* note 1, § 12.B04[B][2].

133. 17 U.S.C. § 512(m)(1)–(2). Outside of the notification context, a service provider must also act expeditiously to remove infringing material if it gains actual knowledge of infringing material or becomes aware of facts or circumstances from which infringing material is apparent (i.e., red flags). *Id.* § 512(c)(1)(A)(i)–(iii).

134. *MP3tunes*, 821 F. Supp. 2d at 643 ("There is no genuine dispute that MP3tunes complies with the requirements of the DMCA with respect to songs sideloaded from websites not listed in the takedown notices."),

135. *Id.*

136. The DMCA places the burden of searching for unauthorized content on the right holder, rather than the service provider—a seemingly backwards approach, given that the service provider is arguably better-situated than the right holder to scan newly posted or hosted material. *See, e.g.*, Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1202–03 (2011) ("Thus, content owners must constantly monitor the entire repertoire of every site on the Internet, in every file format, in order to locate infringing materials.").

The *MP3tunes* opinion thus seems to suggest that cyber locker purveyors might avoid liability (and more easily satisfy their obligations under the DMCA) by forgoing any indexing and assuming the user is uploading legally obtained content for her personal use.[137] The next section examines two recent cases outside of the Second Circuit involving cyber lockers that lacked such indexing capabilities.

C. THE *MEGAUPLOAD* AND *HOTFILE* DECISIONS

One-click file hosts Megaupload and Hotfile recently defended copyright infringement claims—with surprisingly different results. Although neither suit was brought in the Second Circuit, the *Cartoon Network* decision and volitional conduct approach played a central role in both opinions.

Although Megaupload's site was recently shut down by the FBI on charges of criminal copyright infringement, the company also faced civil liability during the summer of 2011.[138] In *Perfect 10 v. Megaupload*, Perfect 10, which was in the business of creating and selling "adult entertainment products" and media, alleged that Megaupload stored pirated works worth billions of dollars on its servers and that Megaupload "depends on, and provides substantial payouts to, affiliate websites who catalogue the URLs providing access to the mass of pirated content on Megaupload's servers."[139]

Moving to dismiss, Megaupload argued that it did not engage in volitional conduct and cited *Cartoon Network* and *MP3tunes.com* as support.[140] The court disagreed: Megaupload was neither a passive conduit nor a "mere file storage system," and Perfect 10 adequately alleged that Megaupload engaged in volitional conduct to support the claim of direct infringement.[141] Although there was no allegation that Megupload itself (i.e., its employees) uploaded infringing content,[142] the court listed specific actions taken by Megaupload that, taken together, evinced volitional conduct: (1) the defendant's distinct websites, such as megaporn.com and megavideo.com, which were created "presumably in an effort to streamline

137. *See, e.g.*, Mike Masnick, *EMI Loses yet Again in Its Quixotic War with Michael Robertson and MP3Tunes*, TECHDIRT (Nov. 3, 2011), http://www.techdirt.com/articles/20111103/04442116611/emi-loses-yet-again-its-quixotic-war-with-michael-robertson-mp3tunes.shtml ("[T]he judge makes it clear that with a music locker like MP3Tunes, there's no legal reason why the company should automatically cut off someone who is a repeat infringer, since all uploads are for personal use, and not to the wider [I]nternet.").

138. For more about the criminal investigation and indictment, see Geoffrey A. Fowler, Devlin Barrett & Sam Schechner, *U.S. Shuts Offshore File-Share 'Locker,'* WALL ST. J. (Jan. 20, 2012), at http://online.wsj.com/article/SB10001424052970204616504577171060611948408.html?mod=WSJ_hp_mostpop_read.

139. Perfect 10, Inc. v. Megaupload Ltd., 11CV0191-IEG BLM, 2011 WL 3203117, at *1, *2 (S.D. Cal. July 27, 2011).

140. *Id.* at *4; *see also* Reply Memorandum of Law in Support of Defendant's Motion to Dismiss, *Megaupload*, 2011 WL 3203117 (May 16, 2011) (No. 11CV00191), 2011 WL 2618814. But note that the opinions in *Megaupload* and *Hotfile* were written before either the initial decision (August 2011) and amended decision (October 2011) in the *MP3tunes* case, and thus relied on a prior opinion.

141. *Megaupload*, 2011 WL 3203117, at *4.

142. *Id.* at *4 n.3.

users' access to different types of media"; (2) encouragement and occasional payment of users via the Rewards program to incentivize uploading popular media; (3) payouts to affiliate websites that maintain a catalog of all available files; and (4) awareness that its service was being used for infringement.[143] A motion to dismiss the contributory infringement claim was also denied, whereas the vicarious liability claim was dismissed without prejudice.[144]

A Florida district court reached the opposite conclusion about volitional conduct with a virtually identically file-storing service in *Disney Enterprises v. Hotfile*.[145] The court discussed *Netcom* and stated that the volitional conduct requirement has been approved by other courts, including the Second Circuit in *Cartoon Network*.[146] Without further discussion of the facts at hand, the court concluded that "the law is clear" that Hotfile was not liable for direct infringement.[147] Although the defendants "allegedly encourage massive infringement," the website allows users to upload and download copyrighted material "without volitional conduct from Hotfile."[148] Citing *MP3tunes* and *Arista Records v. Usenet*, Disney also argued that Hotfile was directly liable because it created a plan to induce infringement.[149] The court, however, thought the cases were wrongly decided: *Arista* ignored the language of *Netcom* and subsequent cases which stated that knowledge and inducement only gives rise to secondary liability.[150] As for *MP3tunes*, the court stated that the opinion had "no analysis" and "simply cited *Arista* and *Russ Hardenburgh* for support."[151] Yet, according to the *Hotfile* court, the direct liability in *Russ Hardenburgh* was justified because the defendant committed a volitional act by having its employees upload copyrighted material to the server.[152] Furthermore, although Hotfile made additional copies of the works once uploaded to the server, the "automatic conduct of software, unaided by human intervention, is not volitional."[153]

There is notable tension between the *Megaupload* and *Hotfile* courts' suggestions about what constitutes volitional conduct for a direct download link service provider. *Arista Records v. Usenet* is of particular interest,[154] as the

143. *Id.* at *4.

144. *Id.* at *6. The parties settled the lawsuit in the fall of 2011. *See* Greg Sandoval, *Megaupload Settles Copyright Suit with Porn Studio*, CNET (Nov. 3, 2011, 7:34 AM), http://news.cnet.com/8301-31001_3-57317577-261/megaupload-settles-copyright-suit-with-porn-studio/.

145. Disney Enters., Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303 (S.D. Fla. July 8, 2011).

146. *Id.* at 1308.

147. *Id.*

148. *Id.*

149. *Id.* Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009), is discussed *infra* notes 154–60 and accompanying text.

150. *Hotfile*, 798 F. Supp. 2d at 1309.

151. *Id.* at 1309; *see also* Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997).

152. *Id.*

153. *Id.* at 1309–10 (citing *Costar* and *Cartoon Network*).

154. *Arista*, 633 F. Supp. 2d 124 (addressing online bulletin boards on which users uploaded pirated content).

Megaupload court relied upon the case, whereas the *Hotfile* court expressly disagreed with it. Usenet was an online network of groups of message and bulletin boards on which subscribers could read and post messages and content.[155] The services were "overwhelmingly" used for copyright infringement.[156]

Citing *Cartoon Network*, the Usenet defendants argued that the volitional element was lacking, but the court found volitional conduct sufficient to show Usenet was actively engaged in unlawful distribution of the copyrighted works and thus directly liable.[157] Usenet was aware that the digital music files were among the most popular items on its site, and "took active measures" to exploit this:[158] for example, although old content was automatically deleted, Usenet maintained servers with increased retention time that were specifically for storing music content.[159] Additionally, Usenet exercised control, both "automated filtering and human review," to reject certain content and users. Such actions transformed the defendants "from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement," and their active engagement satisfied the volitional conduct requirement.[160]

III. ANALYSIS

A. PUBLIC PERFORMANCE REASONING

As *MP3tunes* exemplifies, the *Cartoon Network* public performance reasoning will essentially protect digital storage lockers from successful public performance claims. Assuming the user is listening to or watching the content stored in the locker in his own home (either alone or with no more than the normal circle of family and social acquaintances), the right holder would have to argue that it is a public performance under the transmit clause. Yet because of the Second Circuit's emphasis on the master copy/unique copy distinction, as long as the cyber locker stores a copy unique to that particular person or locker, it would not be a performance to the public.

The application of *Cartoon Network*'s public performance reasoning in *MP3tunes* demonstrates the inherent flaws in forcing the master copy/unique copy distinction onto digital technologies.[161] Deduplication might indeed be a standard,

155. *Id.* at 130. Unlike cyber lockers, users could search for content on the Usenet system to download via a search feature or by the subjects and headers of the individual boards. *Id.*

156. *Id.* at 131.

157. *Id.* at 147–49. In its reasoning, the court relied heavily on the similarity of the facts at hand to the facts of *Russ Hardenburgh*, 982 F. Supp. 503 (N.D. Ohio 1997), in which another online bulletin board company was held directly liable for the infringing content on its site. *Id.* at 512–14.

158. *Arista*, 633 F. Supp. 2d at 148.

159. *Id.* at 131.

160. *Id.* at 148–49.

161. The Second Circuit even noted the lack of an explanation for the master copy reasoning in *Redd Horne*, and thus came up with its own justification. Cartoon Network LP vs. CSC Holdings, Inc., 536 F.3d 121, 138 (2d Cir. 2008) ("Unfortunately, neither the *Redd Horne* court nor Prof. Nimmer explicitly explains why the use of a distinct copy affects the transmit clause inquiry . . . .").

valuable storage-saving methodology, the use of which we would not want to deter through copyright law.[162] But as it is described in *MP3tunes*, it simply does not accord with the court's conclusion that the system saves unique copies, rather than master copies. Moreover, the difference between whether a service utilizes a master copy or unique copies might depend on how a court understands the technical manner in which the service stores uploaded files on its servers.

Furthermore, under the Second Circuit's interpretation of the transmit clause, a cyber locker can avoid "publicly performing" by distributing the stored content through a download, rather than a streaming transmission.[163] Not only is this inconsistent with the statutory text, but it is also counterintuitive, for rights holders are better protected against future infringement when content is delivered through a streaming transmission. In a streaming transmission, as the service provider transmits the file, it temporarily stores buffer copies of portions of the file on the user's computer.[164] Once the audiovisual work is played, the buffer copy is automatically deleted, thus leaving no copies of the file on the user's computer after the streaming transmission is concluded.[165] If the content is sent via a download transmission, the user retains a copy of the file on her hard drive (and can potentially share it with whomever she wants).[166] Therefore, the very nature of a streaming transmission enables service providers to minimize any unlawful sharing by a user.

Significantly, most of the cyber locker sites on which infringement proliferates are those with a direct download link model, where users and third parties can only access the content stored in a locker by downloading it again.[167] Delivery by download enables these sites to rack up profitable pages views because users can easily disseminate popular pirated content to an unlimited number of third parties. Accordingly, by the flawed transmit clause interpretation, the Second Circuit's precedent favors a method of delivery that is the core of the problematic sites' business model and incentivizes massive infringement.

Ironically, Cablevision compared its remote DVR service to a virtual storage locker in its appellate brief:

162. Indeed, in a reply brief, MP3tunes claimed deduplication is protected by fair use because it facilitates users' access to information stored in the cloud. *See* MP3tunes' Reply Brief to EMI's Motion for Summary Judgment at 37–38, Capitol Records, Inc. v. MP3tunes, 821 F. Supp. 2d 627 (S.D.N.Y. Nov. 25, 2010) (No. 07-9931).

163. *See supra* note 104 and accompanying text.

164. *See, e.g.*, Spektor, *supra* note 50, at 46–50 (2009) (describing the difference between streaming and download transmissions).

165. *Id.*

166. *Id.*; *see also* Matthew J. Astle, *Will Congress Kill the Podcasting Star?*, 19 HARV. J.L. & TECH. 161, 165 (2005) (describing how podcasts utilize an upload-download model, rather than a stream, such that once a user has downloaded a file, he has permanent control over that copy and could potentially distribute it further copies).

167. Although Megavideo.com, one of Megaupload's partner sites, used a streaming format, viewers could also choose to download the video. *See* Ellen Seidler, *Cyberlockers: Explaining Piracy's Profit Pyramid*, POP UP PIRATES (Dec. 15, 2011), http://popuppirates.com/?p=1249. There are also numerous cyber locker sites that stream pirated audiovisual work. *Id.*

> The correct analogy for the RS-DVR is not [video-on-demand], but the "virtual locker" that allows users to store and retrieve their own files from a central server. A virtual locker provider does not "publicly perform" a work merely because multiple users happen to store and retrieve their own copies of the same song . . . .[168]

The analogy was likely a defensive strategy to distinguish the RS-DVR from video on demand and instead align it with the VCR, as time-shifting via VCR is protected by the *Sony* doctrine. Somewhat presciently, the analogy forecasted how *Cartoon Network*'s public performance reasoning would largely shield cyber lockers from public performance liability.

B. WHAT CONSTITUTES VOLITIONAL CONDUCT?

Despite holding that the reproduction by an automated system at the direction of the user does not constitute volitional conduct on the part of Cablevision, the *Cartoon Network* decision is not instructive as to what would constitute volitional conduct such as to hold the provider of an automated service directly liable.[169] The varying volitional analyses in *Megaupload*, *Hotfile* and *Arista* elucidate the lack of clarity among district courts from different circuits.[170] This subsection will examine some of the factors considered by the courts in the case law previously mentioned.

Although the Copyright Act does not expressly require a human actor for direct liability,[171] some courts appear to emphasize some degree of actual human involvement as nearly a prerequisite to finding volitional conduct in a claim against an automated service. Several cyber locker cases analyzed more specifically whether the defendant company itself (i.e., its employees) uploaded infringing content. For example, the *Hotfile* court distinguished the case at hand from the finding of volitional conduct in *Russ Hardenburgh* by noting that in the latter case, company employees uploaded the copyrighted content to the server.[172] Similarly,

168. Reply Brief for Defendants-Counterclaimants-Appellants at 44, Cartoon Network v. CSC Holdings, Inc., 536 F.3d 121 (2nd Cir. 2008) (No. 07-1480), 2007 WL 6101594.

169. As discussed *supra* text accompanying notes 57–60, the Second Circuit believed the only volitional conduct of Cablevision was its design and maintenance of "a system that exists only to produce a copy," but concluded that this conduct was not enough to render Cablevision directly liable for any unlawful reproduction that occurs on that system. *See Cartoon Network*, 536 F.3d at 131. Yet the court did not discuss whether a provider of an automated system, like Cablevision, could *ever* be directly liable as a result of the design and maintenance of a system existing solely to produce copies, or if there might be any other conduct by such a provider that would be considered volitional. *See generally id.* at 131–32.

170. Not all circuits have embraced the volitional requirement. For example, in *Warner Bros. v. WTV Systems*, a California district court declined to apply a volitional requirement absent express instruction from the Ninth Circuit. *See* Warner Bros. Entm't Inc. v. WTV Sys., Inc. (*Zediva*), 824 F.Supp.2d 1003 (C.D. Cal. 2011).

171. *See* NIMMER, *supra* note 54, § 15.3 ("The Copyright Act does not specify that there must be a human actor involved for direct infringement.")

172. Disney Enters., Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303, 1310 (S.D. Fla. 2011) ("But, as already explained, the defendant in *Russ Hardenburgh* committed a direct, volitional act by having its employees upload the copyrighted material to its server."); *see also id.* at 1309 ("[I]n some of the cases

the *MP3tunes* court found a genuine issue of material fact about whether MP3tunes employees sideloaded EMI's songs in the scope of their employment, and the court denied EMI summary judgment on the claim of direct liability.[173] But the factor is not dispositive: there was no plausible allegation that Megaupload itself directly uploaded any infringing content, and yet the *Megaupload* court still found sufficient volitional conduct to pass the motion to dismiss stage.[174] Nonetheless, it appears to play a key role in the volitional conduct analysis.

But without similar employee involvement, can a service provider ever be held directly liable for creating an automated service that enables or even induces infringement? The Second Circuit suggested the question remained open: "We need not decide today whether one's contribution to the creation of an infringing copy may be so great that it warrants holding that party directly liable for the infringement, even though another party has actually made the copy."[175] In spite of this assertion, it is easy to read *Cartoon Network* as answering that question in the negative. Then again, as the divergent outcomes in the factually similar *Hotfile* and *Megaupload* cases demonstrate, it is not clear how broadly or narrowly courts will construe the *Cartoon Network* holding.[176] On the one hand, the *Arista* and *Megaupload* courts took a more flexible approach to the volitional element, finding the requisite volition from a totality of factors, such as awareness and exploitation of the use of its service for infringement as well as control over the infringement.[177] But the *Hotfile* opinion suggests that more is needed—perhaps a substantial, overt action. [178]

cited by the plaintiffs, rather than having users upload the copyrighted material, the defendant took a volitional act, i.e., uploading the copyrighted work itself or using software to search for material to upload.") As an example of the latter cases, the court referenced *N.Y. Times v. Tasini*, 121 S. Ct. 2381 (2001), where the publisher "codes each article to facilitate computerized retrieval, then transmits it in a separate file" before it becomes part of LexisNexis' database. *Hotfile*, 798 F. Supp. 2d at 1309. Is this really that different than the automated system?

173. Capitol Records, Inc. v. MP3tunes, LLC, No. 07 CIV. 9931(WHP), 2011 WL 3667335 (S.D.N.Y. Aug. 22, 2011), *amended and superseded by* 821 F. Supp. 2d 627, 649 (S.D.N.Y. 2011) ("Because a genuine dispute exists as to whether any of the 171 songs in question were downloaded by employees in the course of their employment, EMI's motion for summary judgment on this claim is denied.").

174. Perfect 10, Inc. v. Megaupload Ltd., No. 11CV0191-IEG(BLM), 2011 WL 3203117, at *4 n.3 (S.D. Cal. July 27, 2011) ("Perfect 10 does not plausibly allege Megaupload itself uploaded any Perfect 10 materials.").

175. Cartoon Network L.P. v. CSC Holdings, Inc., 536 F.3d 121, 133 (2d Cir. 2008); 4 NIMMER & NIMMER, *supra* note 1, § 13.08[C].

176. *See, e.g.*, Eric Goldman, *Mixed DMCA Online Safe Harbor Ruling in Cloud-Based Music Locker Case*, ERIC'S BLOG, 16 No. 8 Cyberspace Law 18 (Sept. 2011) (Westlaw).

177. *See* Perfect 10, Inc. v. Megaupload Ltd., 11CV0191-IEG BLM, 2011 WL 3203117, at *4 (S.D. Cal. July 27, 2011) (listing several different acts by Megaupload that, considered together, evinced volitional conduct sufficient to hold Megaupload directly liable); Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 148–49 (S.D.N.Y. 2009) (concluding that defendants' awareness that music files were the most popular items on their service, creation of servers dedicated solely to MP3 files, and control and filtering capabilities over the content on their servers altogether satisfied the volitional conduct requirement for direct infringement).

178. *See* Disney Enters., Inc. v. Hotfile Corp., 798 F.Supp.2d 1303, 1308 (S.D. Fla 2011)

In one regard, volition *is* present; the overt act of the service provider merely takes place at an earlier stage—the design and creation of the automated system.[179] The Second Circuit in *Cartoon Network* even acknowledged that this was volitional conduct; it just was not the volitional conduct that mattered.[180] Presumably, the court was looking for something with a greater causal connection to the infringing act. But when a system is purposely designed to automatically download, copy, play and display content upon a user's command, without any nonautomated interaction with the service provider, it seems irrational to require human involvement after the system is up and running.[181]

Furthermore, when a service provider induces or exploits the use of its automated system for infringement, it hardly seems reasonable to preclude direct liability simply on the automated nature of the system.[182] For example, as the *Arista* court emphasized in finding that the defendants satisfied the volitional conduct requirement, Usenet was aware that the digital music files were among the most popular items on its site, and Usenet "took active measures" to exploit this.[183] Similarly, both the *Hotfile* and *Megaupload* opinions noted the defendants' inducement of uploading; the *Hotfile* opinion even goes as far as to acknowledge explicitly that Hotfile encourages massive *infringement*.[184] (The *Megaupload* court was a bit more tentative about this, describing merely that Megaupload encouraged users to upload popular media.)[185] Yet a rigid adherence to the volitional analysis of *Cartoon Network* means that cyber lockers will most likely avoid direct liability.[186] Despite Hotfile's encouragement of massive infringement, the court rejected Disney's claim that Hotfile could be held directly liable by creating a service that induced infringement.[187]

As the Second Circuit treated it, the volitional element also fails to account for other differences that are arguably an important factor in determining liability. For

(acknowledging that Hotfile allegedly encouraged the massive infringement but stating there was no allegations that Hotfile took "direct, volitional steps" to violate plaintiffs' rights, such as an allegation that Hotfile itself uploaded copyrighted material).

179. *See, e.g.*, NIMMER, *supra* note 54, § 15.3 ("To the extent that voluntary acts are required, they can often be found in the creation and deployment of a service or system, intending to and in fact encouraging its use for infringing acts.").

180. *See Cartoon Network*, 536 F.3d at 131.

181. *See, e.g.*, NIMMER, *supra* note 54, § 15.3 ("Automation of a type intended to supplant or substitute for human conduct should be treated as equivalent to human conduct.").

182. *See, e.g., id.* (finding it difficult to accept the argument that under copyright law, mere automation should "shift[] the entire focus of infringement liability").

183. Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 148–49 (S.D.N.Y. 2009).

184. *See supra* notes 143, 178 and accompanying text.

185. *See* Perfect 10, Inc. v. Megaupload Ltd., 11CV0191-IEG BLM, 2011 WL 3203117, at *4 (S.D. Cal. July 27, 2011) (noting that Megaupload "encourages and, in some cases pays, its users to upload vast amounts of popular media through its Rewards Programs").

186. One such example might be *Hotfile*. *See supra* note 178.

187. Disney Enters., Inc. v. Hotfile Corp., 798 F. Supp. 2d 1303, 1309 (S.D. Fla. 2011). The court also found that copies created by Hotfile once the content was uploaded to the server failed to establish volition because they too were created automatically. *Id.*

example, shouldn't the source of the copyrighted work matter?[188] A service provider that both provides and stores a copy arguably acts with more volition than a service provider that merely stores a copy. With digital storage lockers and Internet bulletin boards, the user provides the copy that he uploads or posts and that will be stored on the service provider's server.[189] In *Cartoon Network*, on the other hand, the copy was made by Cablevision and retained on Cablevision's hard disks.[190] Though MP3tunes users uploaded their own content, MP3tunes lent a helping hand through its Sideload subsidiary, which enabled users to search for free music files online and seamlessly sideload them into their storage lockers.[191] Had MP3tunes lacked safe harbor protection under section 512, it is questionable whether the fact that MP3tunes enabled or assisted the user finding free (often unauthorized) songs on third party websites would have been enough to make the conduct volitional under the Second Circuit's definition.

The imposition of a volitional requirement on copyright infringement taking place over an automated system creates an even more fundamental problem for rights holders, however: it could mean the difference between a case and no case at all. A copyright owner who cannot pursue a direct infringement claim against a cyber locker—e.g., because of a lack of volition—might also be unable to assert a claim of secondary liability against the storage locker, for a secondary infringement claim must be based on direct infringement by another party.[192] Additionally, a direct liability suit against the infringing user might not be feasible: the right holder might be unable to identify the infringing user; the costs of litigating might outweigh the benefits if each user only engaged in one or two instances of infringement; or the user might be able to raise a fair use defense. In these situations, rights holders would lack any legal redress at all. But this is not at all in touch with the underlying policy concerns that led the *Netcom* court to impose a

188. *See* Ginsburg, *supra* note 26, at 15 ("By contrast, Cablevision's own transmissions are the *source* of the copies the subscribers request."). In its appellate brief, Cablevision argued that the source is irrelevant. Reply Brief for Defendants-Counterclaimants-Appellants at 45, Cartoon Network L.P. v. CSC Holdings, Inc., 536 F.3d 121, 133 (2d Cir. 2008) (Nos. 07-1480-cv(L), 07-1511-cv(CON)), 2007 WL 6101594 ("A virtual locker provider does not 'publicly perform' a work merely because multiple users happen to store and retrieve their own copies of the same song—even when . . . the same company also provides the content."). However, it does not appear that the Second Circuit discussed the source of the content in the opinion. *See Cartoon Network*, 536 F.3d 121.

189. *See, e.g.*, Malkan, *supra* note 101, at 526–27 ("In the virtual locker, customers upload their copies to the locker. The copy is stored there and played back on demand from wherever the customer is at the time.").

190. *See id.* at 527 ("In the RS-DVR service, by contrast, the customer won't upload anything to Cablevision. The copy will be made by Cablevision at the customer's request (perhaps lawfully, if Sony applies to this method of time-shifting) and retained by Cablevision for the customer's subsequent access.") (footnote omitted)); *see also* Ginsburg, *supra* note 26, at 15 (contrasting the passive conduit in *Netcom*, which merely conveyed copies from one subscriber to another, with Cablevision, which was the source of the copies the subscribers requested).

191. *See supra* note 113; section II.B.

192. *See, e.g.*, Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 149 (S.D.N.Y. 2009) ("For all three theories of secondary copyright infringement, there must be the direct infringement of a third party.").

volitional requirement. In fact, *Netcom*'s rejection of direct liability against the service providers was explicitly premised on the direct liability of the user:

> Where the infringing subscriber is *clearly directly liable for the same act*, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet. Such a result is unnecessary *as there is already a party directly liable* . . . .[193]

Accordingly, the Second Circuit's imposition of a volitional requirement inaccurately reflects the *Netcom* court's justifications for the same, and it inadequately protects the rights of copyright holders.

C. *CARTOON NETWORK* AND THE DMCA

Cartoon Network's volitional and public performance reasoning has even greater implications for cyber lockers than it did for Cablevision: as Internet service providers who store material at the direction of users, cyber lockers are likely to seek safe harbor under the DMCA—an option that is not available to cable providers.[194] Limited to the cable TV context, perhaps the Second Circuit correctly decided *Cartoon Network*; there were certainly policy reasons and judicial considerations in favor of protecting cable providers by imposing a volitional requirement.[195]

But in the context of Internet service providers, to which *Cartoon Network* has been applied, the *Cartoon Network* decision lacks similar policy justifications because digital service providers already have substantial protection from the DMCA.[196] *MP3tunes* serves as an apt example: because the cyber locker fulfilled its minimal obligations under the DMCA, it was largely protected from monetary damages. Even with regard to those songs it failed to remove (and, thus, for which it lacked safe harbor protection), MP3tunes nevertheless has a strong defense against liability because of *Cartoon Network*. Now, following this Second Circuit precedent, MP3tunes can argue that its system stored unique copies of songs and that any copying was done by an automated system at the direction of a user; thus, MP3tunes can argue that any copying was nonvolitional.

As *MP3tunes* suggests, cyber locker providers have a strong incentive to set up automated systems without indexing the content and to let users find and choose

193. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (emphasis added).

194. Provided that the cyber lockers meet the prerequisites for safe harbor set forth in section 512, such as developing a repeat infringer policy. *See* 17 U.S.C. § 512 (2012).

195. For example, the Second Circuit may have felt it was treading too closely to the Supreme Court's "Betamax" decision, given that the RS-DVR was viewed by many as a logical outgrowth of the VCR.

196. Section 512 provides valuable limitations on copyright liability for qualifying service providers that comply with the threshold requirements: as long as a service provider responds to a notice of infringement and removes the infringing content expeditiously, it will incur neither direct nor derivative liability for monetary damages. *See* Ginsburg, *supra* note 49, at 186.

what content to upload without any assistance.[197] Unsurprisingly, virtually all direct download link cyber lockers have those features in common. But might a court find that by merely assuming users are uploading legally obtained files, such cyber lockers are willfully blinding themselves to the infringement on their sites? In another copyright infringement suit against Hotfile, plaintiff Liberty Media made this very argument: "Hotfile cleverly avoids cataloging or indexing the files in order to be willfully blind to their users' uploads and downloads."[198] In a similar vein, the defendant in *In re Aimster* attempted to use the structure of the file-swapping program as a shield.[199] Focusing on language from *Sony*, the *Aimster* defendant argued that he lacked the requisite knowledge for contributory infringement because the encrypted nature of the service prevented him from knowing what songs users were copying through the service.[200] But the Seventh Circuit rejected such a defense, stating that in copyright law "willful blindness is knowledge."[201] According to the court, one who is aware of "shady dealings" yet takes steps to avoid acquiring full knowledge of the nature and extent of those dealings is "held to have a criminal intent."[202]

Yet the Second Circuit's approach in a 2012 opinion suggests the court may be less inclined than the Seventh Circuit to entertain a willful blindness argument in this context. In *Viacom v. YouTube*, the Second Circuit questioned whether a willful blindness argument was even *possible*—specifically, whether the DMCA abrogated the common law principle of willful blindness.[203] Pointing to section 512(m), the court noted that safe harbor protection could not be conditioned on any affirmative duty to monitor, but also acknowledged that willful blindness could not be defined as an affirmative duty to monitor.[204] Finding neither section 512(m) nor the rest of the DMCA spoke directly to willful blindness, the court concluded that the DMCA did not abrogate the doctrine of willful blindness, and thus the doctrine may be applied where appropriate to demonstrate "knowledge or awareness of specific instances of infringement under the DMCA."[205] Notwithstanding the conclusion, the methodology itself hints at some implicit resistance to a willful blindness argument: for example, the Seventh Circuit in *Aimster* did not question

197. *See supra* notes 134–35 and accompanying text (regarding the *MP3tunes* court's statement that "[a]bsent adequate notice, MP3tunes would need to conduct a burdensome investigation in order to determine whether songs in its users' accounts were unauthorized copies"); *see also supra* Part II.B (discussing a counterfactual in which MP3tunes did not operate Sideload.com).

198. Complaint at 7, Liberty Media Holdings, LLC v. Hotfile Corp., No. 1:11CV20056 (S.D. Fla. Jan. 6, 2011), 2011 WL 161734. The case ultimately settled in May without a decision from the court.

199. *In re* Aimster Copyright Litigation, 334 F.3d 643, 650 (7th Cir. 2003).

200. *Id.*

201. *Id.*

202. *Id.*

203. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2d Cir. 2012).

204. *Id.* As defined by the Second Circuit, "[a] person is 'willfully blind' or engages in 'conscious avoidance' amounting to knowledge where the person was aware of a high probability of the fact in dispute and consciously avoided confirming that fact." *Id.* at 38 (citations omitted) (internal quotation marks omitted).

205. *Id.* at 35.

whether the doctrine might be foreclosed.[206] Furthermore, Second Circuit precedent suggests a high bar for a willful blindness challenge to succeed in a similar context.[207]

Even if courts disagree that a cyber locker could be held liable simply because of purposeful choices in structuring its service, they must deny safe harbor to cyber lockers that turn a blind eye to clear signs of infringement. To remain eligible for safe harbor protection under section 512(c), service providers have an affirmative obligation to remove or disable access to infringing material upon gaining actual knowledge of infringement or in the presence of "red flags"—i.e., under "facts or circumstances from which infringing activity is apparent."[208] By their very business model, one might argue that many direct download link providers regularly ignore a red flag: disproportionately voluminous, predominately single-time-viewing page views of a particular URL.[209] Unless these service providers promptly act to cut off access to these files, they should not be able to avail themselves of the safe harbor.[210]

Under current judicial practice, however, it is not certain that courts will foreclose a safe harbor defense because of such indicators of piracy.[211] Copyright academics, such as Professor Jane Ginsburg, have noted that courts tend to conflate the actual knowledge and red flag provisions by requiring too high a degree of specificity for there to be a red flag that would require action by the service provider.[212] Recently, the Second Circuit denied such misinterpretation and explained that the difference between actual and red flag knowledge is not a matter of specific or generalized knowledge, but, rather, a matter of a subjective or objective standard.[213] In the Second Circuit's view, both provisions apply only to specific instances of infringement.[214] This interpretation strains the text of the

206. *In re Aimster*, 334 F.3d 643.

207. In *Tiffany v. eBay*, the Second Circuit rejected a willful blindness challenge and held that even though eBay "knew as a general matter that counterfeit Tiffany products were listed and sold through its website," such knowledge was insufficient to trigger liability. 600 F.3d 93, 110 (2d Cir. 2010). Later, in its *Viacom* opinion, the court rationalized that the conclusion in *Tiffany* was based on "the extensive findings of the district court with respect to willful blindness," presumably to bolster its suggestion that a willful blindness challenge could potentially succeed. *Viacom*, 676 F.3d at 35 n.10.

208. 17 U.S.C. § 512(c)(1)(A) (2012).

209. *See, e.g.*, Ginsburg, *supra* note 49, at 191 (listing disproportionately high web traffic as one example that could, or at least should, constitute a red flag).

210. Megaupload had not yet raised a DMCA defense at the time during which the district court for the Southern District of California denied the motion to dismiss. *See* Perfect 10, Inc. v. Megaupload Ltd., No. 11CV0191-IEG (BLM), 2011 WL 3203117 (S.D. Cal. July 27, 2011).

211. *See, e.g.*, Ginsburg, *supra* note 49, at 190 ("The case law interpreting the statutory 'red flag' standard suggests the flag may need to be an immense crimson banner before the service provider's obligation to intervene comes into play.")

212. *Id.*

213. *See Viacom*, 676 F.3d 19 at 30–32. The court explained that "the actual knowledge provision turns on whether the provider actually or 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person." *Id.* at 31.

214. *Id.*

DMCA, which distinguishes between the two provisions with language about specificity of knowledge: "(i) does not have *actual knowledge* . . . ; (ii) in the *absence of actual knowledge*, is *not aware* of facts or circumstances from which infringing activity is *apparent* . . . ."[215] But whether it is a misinterpretation or not, the prevailing judicial construction of the red flag provision sets a high bar for the type of knowledge that would trigger a service provider's take-down obligations. Consequently, and as was demonstrated in *MP3tunes*,[216] cyber locker providers have an easier time keeping their safe harbor protection. There is yet another potential problem with transporting the *Cartoon Network* volitional reasoning to service providers who are eligible for safe harbor: it is questionable if, after the enactment of the DMCA, a volitional requirement is *ever* appropriate for Internet storage providers like cyber lockers. Only two of the four safe harbors, transmitting and caching, contain the language "carried out through an automatic technological process."[217] Reading this as a deliberate Congressional choice, Professor Nimmer argues that courts should only apply the *Netcom* volitional requirement in the case of transmitting and caching because those provisions "codify that element by requiring that something beyond an 'automatic technical process' be implicated."[218] Accordingly, *Netcom*'s volitional factor is inappropriate for the other two safe harbors, storing and linking.[219] If Professor Nimmer is correct, courts should not require volitional conduct to support a claim of direct liability for cyber lockers, which presumably store information at the direction of a user.

IV. CONCLUSION

The problem with the reasoning in *Cartoon Network* is that in its public performance and volitional analyses, it reached for analogies and case law that fit uncomfortably with our present technological era. Not only is the Second Circuit's reading of the transmit clause in tension with the statutory text, its copy shop analogy is outdated, given that so many modern services and technologies are purposely designed to be completely automated or at the direction of a user.[220] The

215. 17 U.S.C. § 512(c)(1)(A) (2012) (emphasis added). The court's settlement on a distinction out of line with the plain language of the DMCA is less surprising when the starting point is considered: the Second Circuit looked first to the judicial usage of "actual knowledge" and "facts or circumstances" in cases completely unrelated to copyright. *See Viacom*, 676 F.3d at 31 (citing United States v. Quinones, 635 F.2d 590 (2d Cir. 2011), and Maxwell v. City of New York, 380 F.3d 106 (2d Cir. 2004)).

216. Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011) ("Undoubtedly, MP3tunes is aware that some level of infringement occurs. But, there is no genuine dispute that MP3tunes did not have specific 'red flag' knowledge with respect to any particular link . . . ."). Indeed, the Second Circuit cited *MP3tunes* as an example that its interpretation of section 512(c) was correct. *See Viacom*, 676 F.3d at 32.

217. 17 U.S.C. § 512; *see also* 3 NIMMER & NIMMER, *supra* note 1, § 12B.06[B][2][c][i].

218. 3 NIMMER & NIMMER, *supra* note 1, § 12B.06[B][2][b].

219. *Id.*

220. *See, e.g.*, NIMMER, *supra* note 54, § 15.3 ("Modern technology enables automation of many

distinction between master copies and unique copies may be suitable for physical chattels, but, as seen in *MP3tunes*, it does not translate well to the manner in which digital files are stored over the Internet. Moreover, literal adherence to the master/unique copy reasoning would arguably preclude the use of innovative and efficient storage-saving processes like deduplication. The application of the master copy/unique copy distinction in *MP3tunes* suggests that the *Cartoon Network* reasoning will greatly shield digital storage lockers from liability, provided they comply with their obligations under section 512.

With its volitional reasoning, *Cartoon Network* clings to a concept that is out of touch with our present technological age. *Netcom*'s volitional requirement—motivated by a concern that the entire Internet could be held liable for the act of a single user—may have made sense in 1995.[221] Today, however, service providers already have adequate protection: the limitations on liability available through section 512. Given that automated services are increasingly the norm, the Second Circuit's holding that reproduction by an automated system is nonvolitional thus goes too far.[222] Furthermore, the automated nature of a system does not necessarily mean the service provider is unaware or impassive about infringement taking place; indeed, the *Hotfile*, *Megaupload* and *Arista* opinions all noted some knowledge that the services were used for infringement, along with a certain degree of inducement. Finally, the volitional conduct analyses (or lack thereof) in the case law surveyed in this Note demonstrate how unsettled the law is regarding a volitional requirement: whether it is actually a required element; if it still applies after the enactment of section 512; and exactly what constitutes volitional conduct when the system is automated.

More troublesome, however, is the impact that *Cartoon Network* will have on digital storage lockers. As *MP3tunes* implies, *Cartoon Network* essentially sets up a roadmap for avoiding direct liability.[223] To avoid volition that will render a provider directly liable: make the entire system completely automatic, so copying, transmitting and playing content are solely upon the command of a user. To avoid successful public performance claims: maintain unique copies of content for each user. To easily satisfy safe harbor requirements: avoid tracking the sources of user-uploaded content or the content itself. *MP3tunes* thus demonstrates just how beneficial the *Cartoon Network* reasoning can be for cyber lockers.

In combination, the *Cartoon Network* reasoning and the availability of claiming safe harbor could substantially shield cyber lockers from any copyright liability occurring through their sites, at least in the Second Circuit. More needs to be done for rights holders, who may consequently lack any legal redress at all.

The best hope is that other circuits refuse to follow the Second Circuit's lead in *Cartoon Network*—or at least treat automation of a type intended to supplant or

functions that once required direct human involvement.").

221. *See, e.g.*, *id.* (suggesting that Netcom reached the proper result in its particular context).

222. *Id.*; *see also supra* note 220.

223. *See* Ginsburg, *supra* note 26, at 27 (noting the Second Circuit's subsequent limitation in light of the "potential onslaught of new copyright-avoiding business models that its decision might inspire").

substitute for human conduct as the equivalent of human conduct.[224] Of course, this could create a more serious problem: too high a cost of operation for valuable services, like search engines. Additionally, the safe harbors might still substantially shield cyber lockers from liability, at least given the current manner in which courts construe the red flag provision in section 512(c).

A legislative intervention would certainly be the most effective solution, but is the least likely to occur.[225] Ironically, the two main changes proposed in the (ultimately unenacted) Stop Online Piracy Act, increased criminal penalties and methods to cut off financial support, might actually make a substantial difference in fighting piracy. After U.S. prosecutors shut down Megaupload, former Megaupload users flocked to different cyber locker sites, such as Rapidgator, whose web traffic increased exponentially.[226] Yet, when PayPal announced it was ending service to RapidGator customers, RapidGator announced it would close.[227] But the current range of criminal penalties does not adequately deter all would-be infringers, and we have yet to see other payment providers voluntarily cut off access like PayPal has.

Another possibility is to require structural changes to minimize the use of cyber locker services for infringing purposes. Congress could impose an obligation to make a reasonable and technologically feasible effort to monitor for infringement.[228] For example, cyber lockers could utilize content identification software like Vobile's vCloud9 technology, which scans uncompressed and "difficult-to-scan" compressed files and then compares data to its registry of copyrighted audiovisual works.[229] A data match triggers (quite appropriately) an automated action, chosen by the content owner, such as a complete removal of the content from the website.[230] But this could go too far and curb what are actually fair uses of cyber lockers, for content identification software does not discern whether the copy was legally purchased. Another possibility would be to limit the

224. *See* NIMMER, *supra* note 54, § 15.3.

225. Given the enormous controversy generated by the recent proposed antipiracy legislation, the Stop Online Piracy Act, and the strong coalition that emerged to block its passage and protect Internet freedom, it looks like it will be a while before a substantive Internet antipiracy bill is passed.

226. Cyber locker site RapidGator saw its web traffic increase from a few hundred visits to over 100,000 per day. *See* Ernesto, *Cyberlocker to Shut down After PayPal Ban*, TORRENTFREAK (Feb. 26, 2012), http://torrentfreak.com/cyberlocker-to-shut-down-after-paypal-ban-120226/.

227. *Id.*

228. This language was inspired by language from that of the aforementioned proposed antipiracy legislation.

229. *Vobile Expands Copyright Infringement Technology*, WALL ST. J. (Dec. 8, 2011, 5:31 PM), http://blogs.wsj.com/speakeasy/2011/12/08/vobile-expands-copyright-infringement-technology/.

230. *Id.* In 2008, a German court chose a similar solution as part of the remedy for a cyber locker's copyright infringement. *See* Caitlin Cimpanu, *Rapidshare Loses Lawsuit, Will Filter Some Book Titles*, SOFTPEDIA (Feb. 26, 2010, 3:34 PM), http://news.softpedia.com/news/Rapidshare-Loses-Lawsuit-Will-Filter-Some-Book-Titles-136125.shtml. On appeal, however, the appellate court reversed the earlier judgment and deemed the mandated remedies to be ineffective; content scanning, for one, would simply lead to encrypted files. *See* Nate Anderson, *Court: RapidShare Doesn't Need to Filter User Uploads*, ARS TECHNICA (May 4, 2011), http://arstechnica.com/tech-policy/news/2010/05/court-rapidshare-doesnt-need-to-filter-uploads.ars.

upload capability so that cyber lockers only store content purchased from an affiliate digital store. Yet this vastly reduces the utility of cyber lockers, and locker providers are unlikely to take this action voluntarily.

Perhaps a better solution would be to focus structural changes on the retrieval of the content from the locker. Because a streaming transmission does not leave a permanent copy on the hard drive after it is played, this mode of redelivery helps curb subsequent infringement. Notably, this is one step that some legitimate cyber locker services have taken, such as Apple's iTunes Match. Streaming, however, also has practical downfalls, such as requiring a live Internet connection for the duration of the performance. Additionally, streaming itself only limits subsequent infringement by the recipient, but it is not necessarily legitimate itself: there is a growth of rogue sites which transmit pirated works through streaming feeds. For sites that deliver stored files by download transmissions, piracy could also be reduced through limits on file size and the number of times a single file can be downloaded.[231]

Whether the *Cartoon Network* decision will continue to impact cyber locker lawsuits outside of the Second Circuit remains an open question. With Megaupload's recent criminal indictment, the MPAA plaintiffs in the *Hotfile* litigation have moved for summary judgment, arguing that Hotfile's business model is "virtually indistinguishable" from that of Megaupload.[232] The Florida district court could again rely on the volitional element from *Cartoon Network* and find the one-click file host cannot be held directly liable. One hopes, however, that the court recognizes the extent to which the one-click host model of cyber lockers profits from and incites massive infringement through its services—and that the court finally holds such providers accountable.

231. For example, one reason Megaupload consumed so much bandwidth is because of the large size of many files that were stored and shared on its systems, including movie trailers, software applications and games. *See, e.g.*, Brodkin, *supra* note 66. Dropbox, in comparison, also has high traffic but the files shared are smaller in size, which suggests a mix of work and personal files. *Id.*

232. *See* Plaintiffs' Motion and Memorandum of Law in Support of Summary Judgment at 10, Disney Enters., Inc. v. Hotfile Corp., No. 11-20427 (S.D. Fla. Mar. 5, 2012) (Doc. No. 322).