

The Future of Online User-Generated Content in the Video-Sharing Business: *Capitol Records LLC v. Vimeo LLC*

I.	OVERVIEW OF THE CASE	375
II.	BACKGROUND	376
A.	<i>Threshold Requirements to Safe Harbor Protection</i>	376
1.	Service Provider	377
2.	Policy Against Repeat Infringers	378
3.	Technical Measures Noninterference	379
B.	<i>Information Residing on Systems at Direction of Users</i>	379
C.	<i>Pre-1972 Sound Recordings</i>	380
III.	COURT'S DECISION.....	381
IV.	ANALYSIS	384

I. OVERVIEW OF THE CASE

Capitol Records and EMI—record and music publishing companies—brought copyright infringement action against Vimeo LLC, an online video-sharing platform that allowed users to upload videos to the website, in 2009, seeking to remove 199 music videos on Vimeo.¹ Vimeo started off as an online platform that allowed users to upload and share original video content.² Unlike other video-sharing platforms, Vimeo required uploaders to have participated in the process of creating the uploaded video, thereby offering filmmakers a place to display their work.³ Vimeo had grown significantly since its first launch in 2004, becoming one of the most frequently visited websites and one of the top online distributors of video content by September 2012.⁴ Vimeo also grew its staff size from twenty to seventy-four by the end of 2013.⁵ At the time of the suit, Vimeo had approximately 12.3 million registered users across forty-nine countries, who uploaded nearly 43,000 new videos each day.⁶

1. Capitol Records, LLC v. Vimeo, LLC (*Vimeo I*), 972 F. Supp. 2d 500, 506-07 (S.D.N.Y. 2013).

2. *Id.* at 504.

3. *Id.* at 505.

4. *Id.*

5. *Id.*

6. *Id.*

Capitol and EMI each filed complaints over a total of 199 videos posted to Vimeo's platform,⁷ claiming ownership of copyrights to musical recordings in each.⁸ These videos contained copyrighted music from well-known artists such as The Beatles, The Beach Boys, The Jackson 5, and Beyoncé.⁹ Vimeo did not dispute that its users used the content without authorization and infringed the plaintiff's copyrights.¹⁰ Instead Vimeo moved for summary judgment, alleging that they did not know they were hosting the content, which entitled them to summary shelter under the Digital Millennium Copyright Act's "safe harbor" provisions in September 2012.¹¹ Capitol Records cross-moved for partial summary judgment, seeking a ruling that Vimeo was disqualified for safe harbor protection.¹²

The noted case discusses two main complexities. First, it decides whether Vimeo is entitled to safe harbor protection under the Digital Millennium Copyright Act (DMCA). Second, the noted case considers whether the DMCA safe harbor protection applied to recordings fixed before February 15, 1972. This Note will evaluate both complexities, emphasizing the first. The United States District Court for the Southern District of New York *held* that (1) Vimeo LLC was entitled to safe harbor protection as to 161 of the 199 videos, but "triable issues remain[ed] as to whether Vimeo [was] entitled to safe harbor protection [regarding the remaining 38] of the 199 Videos-in-Suit that Vimeo employees interacted with or uploaded,"¹³ and (2) any infringing video in suit recorded prior to February 15, 1972, was not eligible for safe harbor protection. *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 537 (S.D.N.Y. 2013).

II. BACKGROUND

A. *Threshold Requirements to Safe Harbor Protection*

The Digital Millennium Copyright Act (DMCA) is a United States copyright act that implements treaties of the World Intellectual Property Organization (WIPO) to address treaty obligations not covered under

7. *Id.* at 506-07.

8. *Id.* at 507.

9. *Id.* at 521.

10. *Id.* at 507.

11. *Id.*

12. *Id.*

13. *Id.* The court initially held that Vimeo was entitled to summary judgment for 144 videos and later in the December 2013 opinion amended to include 17 more. See *Capitol Records, LLC v. Vimeo, LLC (Vimeo II)*, 972 F. Supp. 2d 537, 556 (S.D.N.Y. 2013).

existing U.S. law.¹⁴ It prohibits the act of circumventing any technological measure¹⁵ that effectively controls access to copyrighted works.¹⁶ On October 28, 1998, the DMCA amended Title 17 of the United States Code to extend the reach of copyright by creating new prohibitions on circumvention of protective measures.¹⁷ It also limited the liability of online service providers for copyright infringement by their users in certain types of activities such as storing information on networks at direction of users.¹⁸ Specifically, DMCA title II, the Online Copyright Infringement Liability Limitation Act (OCILLA), later codified at 17 U.S.C. § 512(c), creates a safe harbor for online service providers against copyright infringement liability, provided they first meet three threshold requirements.¹⁹ The threshold requirements under the DMCA safe harbor protection are that the party “(1) must be a ‘service provider’ as defined by the statute; (2) must have adopted and reasonably implemented a policy for the termination [of] repeat infringers; and (3) must not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works.”²⁰ The United States Congress enacted the safe harbor provision in an attempt to balance the legitimate interests of copyright owners with those of consumers of copyrighted products.²¹

1. Service Provider

Under 17 U.S.C. § 512(k)(1)(B), a “service provider” is defined as “a provider of online services or network access, or the operator of facilities therefor.”²² Courts have interpreted this term widely so that websites that provide services “over and above the mere storage of uploaded user content” are service providers too.²³ This interpretation

14. *Executive Summary of the Digital Millennium Copyright Act*, U.S. COPYRIGHT OFF., http://www.copyright.gov/reports/studies/dmca/dmca_executive.html (last visited Oct. 28, 2014).

15. Such measures are commonly known as digital rights management or DRM.

16. *Executive Summary of the Digital Millennium Copyright Act*, *supra* note 14.

17. *Id.*

18. *Summary of the Digital Millennium Copyright Act of 1998*, U.S. COPYRIGHT OFF., <http://www.copyright.gov/legislation/dmca.pdf> (last visited Sept. 16, 2014).

19. 17 U.S.C. § 512(c)(i) (2012).

20. *Vimeo I*, 972 F. Supp. 2d 500, 510 (S.D.N.Y. 2013) (alteration in original) (citing *Wolk v. Kodak Imaging Network*, 840 F. Supp. 2d 724, 743 (S.D.N.Y. 2012)).

21. *Chamberlain Grp., Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1202-03 (Fed. Cir. 2004); WILLIAM F. PATRY, PATRY ON COPYRIGHT § 16A:1 (2007).

22. 17 U.S.C. § 512(k)(1)(B).

23. *Vimeo I*, 972 F. Supp. 2d at 511; *see, e.g., Wolk*, 840 F. Supp. 2d at 744 (“Because Photobucket offers a site that hosts and allows online sharing of photos and videos at the direction of users, Photobucket, like YouTube.com or Veoh.com, qualifies as a ‘service provider’ under § 512(k)(1)(B).”).

essentially allows website oversight and interaction not to hamper the availability of the safe harbors defense.

2. Policy Against Repeat Infringers

The second threshold requirement for safe harbor protection states that a service provider must have “adopted and reasonably implemented, and inform[ed] subscribers and account holders of the service provider’s system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers.”²⁴ To implement this requirement, Courts have additionally required that service providers must “(i) adopt a policy that provides for the termination of service access for repeat copyright infringers; (ii) inform users of the service policy; and (iii) implement the policy in a reasonable manner.”²⁵ Other courts have observed that “[t]he purpose of subsection 512(i) is to deny protection to websites that tolerate users who flagrantly disrespect copyrights.”²⁶

Specifically, courts have held that the standard of adopting a repeat infringer policy should not be difficult to achieve.²⁷ Courts have also held that “[a] policy stating [that] a user’s access may be terminated [was considered] sufficient communication.”²⁸ Finally, courts have defined “reasonable implementation” of a policy to allow service providers to “utilize a ‘variety of procedures’ and does not require that the service provider ‘affirmatively police its users for evidence of repeat infringement.’”²⁹ The court in *Perfect 10, Inc. v. Google, Inc.*, held that § 512(i) does not require service providers to document the actions of their users.³⁰ However, the court in *Perfect 10, Inc. v. CCBill, LLC*, held, “A substantial failure to record [infringers] may raise a genuine issue of

24. 17 U.S.C. § 512(i)(1)(A).

25. *Wolk*, 840 F. Supp. 2d at 744; *see, e.g.*, *Ellison v. Robertson*, 357 F.3d 1072, 1080 (9th Cir. 2004).

26. *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 637 (S.D.N.Y. 2011), *rev’d on other grounds*, 107 U.S.P.Q. 2d 1770 (S.D.N.Y. 2013).

27. *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004).

28. *Vimeo I*, 972 F. Supp. 2d at 514 (summarizing *Perfect 10, Inc. v. CCBill, LLC (CCBill I)*, 340 F. Supp. 2d 1077, 1088–89 (C.D. Cal. 2004)).

29. *Id.* (citing *Perfect 10, Inc. v. CCBill LLC (CCBill II)*, 488 F.3d 1102, 1109–11 (9th Cir. 2007)).

30. No. CV 04–9484 (AHM), 2010 WL 9479059, at *5 (C.D. Cal. July 26, 2010).

material fact as to the implementation of the service provider's repeat infringer policy.”³¹

3. Technical Measures Noninterference

The third threshold requirement states that the service provider “must not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works.”³² Section 512(i)(2) defines “standard technical measures” as “measures that are used by copyright owners to identify or protect copyrighted works.”³³ In general, courts have held a service provider liable when it “[r]efuse[s] to accommodate or implement a ‘standard technical measure.’”³⁴

B. *Information Residing on Systems at Direction of Users*

Once a service provider proves that it has met the above three threshold requirements, it must then prove that it meets the requirements of the particular safe harbor provision under which it claims protection. In the noted case, Vimeo claims protection under § 512(c).³⁵ Section 512(c)(1) regulates information residing on systems or networks at direction of users and provides:

A service provider shall not be liable for monetary relief, or . . . for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider . . . does not have actual knowledge that the material or an activity using the material on the system or network is infringing; . . . does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and upon notification of claimed infringement . . . responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.³⁶

31. 488 F.3d at 1110; *see also* Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) (explaining that “allow[ing] notices of potential copyright infringement to fall into a vacuum and to go unheeded” was unreasonable).

32. Wolk v. Kodak Imaging Network, 840 F. Supp. 2d 724, 743 (S.D.N.Y. 2012) (citing *Corbis*, 351 F. Supp. 2d 1099). One example of a standard technical measure is a digital watermark imposed on a copyrighted photograph.

33. 17 U.S.C. § 512(i)(2) (2012).

34. Viacom Int'l, Inc. v. YouTube Inc., 676 F.3d 19, 41 (2d Cir. 2012).

35. *Vimeo I*, 972 F. Supp. 2d 500, 510 (S.D.N.Y. 2013).

36. 17 U.S.C. § 512(c)(1).

Thus, a service provider is not protected under § 512(c) if it has actual knowledge of the infringement in question.³⁷ Furthermore, there are some instances when a service provider may not have actual knowledge of infringement, but may nonetheless be disqualified from this safe harbor provision. If the service provider is “aware of facts or circumstances from which infringing activity is apparent,” it is disqualified as having “red flag” knowledge of the infringement.³⁸ Red flag knowledge, as explained in *Viacom International, Inc. v. YouTube, Inc.*, is found when a provider is “subjectively aware of facts that would have made the specific infringement ‘objectively’ obvious to a reasonable person.”³⁹

C. Pre-1972 Sound Recordings

DMCA safe harbors do not apply to pre-1972 sound recordings. Section 301(c) of the Copyright Act states, “With respect to sound recordings fixed before February 15, 1972, any rights or remedies under the common law or statutes of any State shall not be annulled or limited by this title until February 15, 2067.”⁴⁰ Furthermore, the Copyright Office has explicitly stated that DMCA safe harbors do not apply, noting that it “sees no reason . . . why the section 512 ‘safe harbor’ [clause] should not apply to the use of pre-1972 sound recordings.”⁴¹ However, it concludes, “[I]t is for Congress, not the courts, to extend the Copyright Act to pre-1972 sound recordings”⁴² No federal court prior to the noted case addressed the potential conflict between state laws with regard to pre-1972 sound recordings and the DMCA safe harbor provisions.⁴³ However, the Supreme Court of the State of New York addressed this issue in *UMG Recordings, Inc. v. Escape Media Group, Inc.*, and came to the same conclusion that pre-1972 sound recordings were not subject to DMCA safe harbor protection.⁴⁴

37. *Id.* § 512(c)(1)(A)(i).

38. *Id.* § 512(c)(1)(A)(ii).

39. *Viacom*, 676 F.3d at 31.

40. 17 U.S.C. § 301(c).

41. *Federal Copyright Protection for Pre-1972 Sound Recordings*, U.S. COPYRIGHT OFF. 130 (Dec. 2011), <http://www.copyright.gov/docs/sound/pre-72-report.pdf>.

42. *Id.* at 132.

43. *Id.*

44. 107 A.D.3d 51, 110-12 (N.Y. App. Div. 2013).

III. COURT'S DECISION

In the noted case, the Southern District of New York followed the framework created by the United States Court of Appeals for the Second Circuit in *Viacom* to analyze Vimeo's safe harbor protection claims.⁴⁵ It addressed (1) whether Vimeo was a service provider pursuant to § 512(k)(1)(B); (2) whether Vimeo had adopted an informed, reasonably implemented policy to terminate users who repeatedly posted infringing content; (3) whether Vimeo interfered with "standard technical measures"; (4) whether the content on Vimeo's website was stored "at the direction of the user"; (5) whether Vimeo possessed actual or "red flag" knowledge of the infringing material; (6) whether Vimeo was capable of controlling the infringing material; (7) whether Vimeo removed the material at issue in a timely manner; and (8) whether DMCA applied to videos recorded prior to February 1972.⁴⁶ Judge Abrams, in writing the opinion for the court, reviewed all eight elements, granting in part and denying in part Vimeo's motion for summary judgment.⁴⁷

Vimeo qualified as a service provider under § 512(k)(1)(B): "Vimeo is a provider of online services that hosts and distributes user material by permitting its users to upload, share and view videos."⁴⁸ The court further noted, "Even though Vimeo's activities are not limited to such . . . Vimeo qualifies as a service provider under § 512(k)(1)(B)'s expansive definition."⁴⁹

Vimeo had a policy in place for the termination of repeat infringers.⁵⁰ While there is little case law directly addressing what constitutes a sufficient policy, courts have generally adopted the attitude that the "threshold requirement of the adoption of a repeat infringer policy should not be an overly burdensome one to meet."⁵¹ Judge Abrams further explained that this is because "[t]he fact that Congress chose not to adopt such specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined."⁵² Because of this loose requirement, Judge Abrams concluded that Vimeo's policy to remove infringing material and delete the user accounts of those who

45. See *Vimeo I*, 972 F. Supp. 2d 500 (S.D.N.Y. 2013).

46. *Id.* at 506-37.

47. *Id.*

48. *Id.* at 511.

49. *Id.*

50. *Id.* at 513.

51. *Id.*

52. *Id.* (citing *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004)).

repeatedly uploaded infringing content was a sufficient repeat infringer policy.⁵³

Vimeo informed its users of the policy for termination of repeat infringers.⁵⁴ Judge Abrams reasoned that while service providers are not required to reveal their decision-making process, this requirement “has been interpreted to require that the service provider ‘put users on notice that they face exclusion from the service if they repeatedly violate copyright laws.’”⁵⁵ Judge Abrams explained, “Vimeo provided contact information for its DMCA designated agent, required registered users to agree not to infringe others’ copyrights, and notified users that their accounts may be terminated for violation of the Terms of Service.”⁵⁶ Thus, the court found that Vimeo sufficiently informed its users of its repeat infringer policy.⁵⁷

Vimeo’s repeat infringer policy was reasonably implemented.⁵⁸ Judge Abrams noted that although the term “reasonably implemented” is not defined in the statute, “case law provides that a reasonably implemented policy can utilize a ‘variety of procedures’ and does not require that the service provider ‘affirmatively police its users for evidence of repeat infringement.’”⁵⁹ Conversely, courts have found that a service provider that repeatedly fails to track repeat infringers may not have adopted reasonable implementation of a repeat infringer policy.⁶⁰ However, Vimeo presented evidence to show that repeat infringers were systematically identified and their user accounts were disabled, sometimes only after the first DMCA takedown notice.⁶¹ Thus, the court found that Vimeo’s repeat infringer policy was reasonably implemented.⁶²

Vimeo did not interfere with standard technical measures used by Capitol Records and EMI.⁶³ Judge Abrams explained that while “[Capitol Records and EMI claimed] that Vimeo’s privacy settings prevent[ed] copyright owners from collecting information needed to

53. *Id.*

54. *Id.* at 513-14.

55. *Id.* at 513 (citing *Corbis*, 351 F. Supp. 2d at 1102).

56. *Id.*

57. *Id.* at 514.

58. *Id.* at 517.

59. *Id.* at 514 (citing *CCBill II*, 488 F.3d 1102, 1109–11 (9th Cir. 2007)).

60. *CCBill II*, 488 F.3d at 1110 (holding that a policy was unreasonably implemented where defendant “allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded”); *Ellison v. Robertson*, 357 F.3d 1072, 1080 (9th Cir. 2004).

61. *Vimeo I*, 972 F. Supp. 2d at 514-15.

62. *Id.* at 515-16.

63. *Id.* at 517.

issue a takedown notice . . . privacy settings do not constitute interference with standard technical measures.”⁶⁴

The court then held that triable issues remained as to whether the infringing videos were stored at the direction of a user.⁶⁵ The court reasoned that it was unclear whether “the employee-uploader was acting on behalf of [Vimeo or as a user because] [r]easonable minds could differ . . . as to the extent to which the videos at issue here were uploaded by Vimeo employees in their personal capacities as opposed to as agents of Vimeo.”⁶⁶

In evaluating whether Vimeo had actual or red flag knowledge of infringement, the court dismissed 144 of the counts, because no evidence of whether Vimeo acquired actual or red flag knowledge was presented regarding those videos.⁶⁷ However, the court did not rule that, as a matter of law, the fifty-five videos to which the evidence *did* relate constituted red flag knowledge.⁶⁸ Instead, the court found triable issues of fact as to whether the employee interactions lead Vimeo to have red flag knowledge of the infringing content.⁶⁹ In reaching this conclusion, the court relied on the analysis in *Columbia Pictures Industries, Inc. v. Fung* and reasoned that triable issues remain as to whether “[t]he material in question was sufficiently current and well-known that it would have been objectively obvious to a reasonable person that the material solicited and assisted was both copyrighted and not licensed to random members of the public.”⁷⁰

Vimeo did not have substantial control over infringing content.⁷¹ Relying on *Viacom*, the court recognized that “the right and ability to control . . . requires *something more* than the ability to remove or block access to materials posted on a service provider’s website.”⁷² In the noted case, Vimeo had established a monitoring program that can be effective at removing undesirable content from the website.⁷³ However, due to the small size staff, the practical ability for Vimeo to exercise that ability is

64. *Id.*; see *Obodai v. Demand Media, Inc.*, No. 11 Civ. 2503 (PKC), 2012 WL 2189740, at *5 (S.D.N.Y. June 13, 2012).

65. *Vimeo I*, 972 F. Supp. 2d at 537.

66. *Id.* at 519.

67. *Id.* at 523.

68. *Id.*

69. *Id.*

70. *Id.* (citing *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013) (internal quotation marks omitted)).

71. *Id.* at 530.

72. *Id.* at 526 (citing *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012)).

73. *Id.* at 528.

“de minimis.”⁷⁴ Therefore, the court found no right and ability to control the website’s content on Vimeo’s part.⁷⁵

Vimeo diligently removed the infringing content at issue.⁷⁶ Vimeo responded to the plaintiffs’ takedown notice and removed the videos identified on three occasions.⁷⁷ The court reasoned that the two occasions where Vimeo responded within one day constituted sufficiently diligent removal.⁷⁸ Furthermore, the three-and-one-half week period it took to comply with removing 170 infringing videos also constituted sufficiently diligent removal in comparison to the total number of infringing uploads in the noted case.⁷⁹

Finally, the court held that DMCA safe harbor protection did not extend to pre-February 1972 sound recordings.⁸⁰ On this issue, the court opined, “[I]t is for Congress, not the courts, to extend the Copyright Act to pre-1972 sound recordings, both with respect to the rights granted under the Act and the limitations on those rights (such as section 512) set forth in the Act.”⁸¹ Thus, the court granted summary judgment to the plaintiffs for all applicable videos in suit.⁸²

IV. ANALYSIS

The district court correctly decided that Vimeo was entitled to safe harbor protection regarding 161 of the videos in suit under DMCA. However, many of the standards employed in the opinion, namely assessment of red flag knowledge and what constitutes a substantial enough monitoring program, remain vague. For companies providing streaming content and media services online, the noted case has the potential to shape the industry because it provides invaluable guidance on what the company should and should not instruct its employees to do on a daily basis. More importantly, the noted case and the surrounding laws have the potential to shape the future of our Internet culture.

74. *Id.* at 530.

75. *Id.*

76. *Id.* at 536.

77. *Id.* at 535.

78. *Id.* at 536.

79. *Id.*

80. *Id.* at 536-37.

81. *Id.*; *Federal Copyright Protection for Pre-1972 Sound Recordings*, *supra* note 41; UMG Recordings, Inc. v. Escape Media Grp., Inc., 107 A.D.3d 51, 59 (N.Y. App. Div. 2013) (commenting that it would “be far more appropriate for Congress, if necessary, to amend the DMCA to clarify its intent, than for this Court to do so by fiat”).

82. *Vimeo I*, 972 F. Supp. 2d at 537.

Licensed broadcasters and production companies have historically created and supplied standard video-on-demand content.⁸³ These video producers were able to influence video content through professional editorial control.⁸⁴ The video market has experienced revolutionary changes with the increasing popularity of user-generated content (UGC).⁸⁵ Today, Internet users can publish their own work online.⁸⁶ This self-publishing trend shortened video content length and production time so much that *Wired* magazine refers to this social phenomenon as “media snacking” and the small-sized content pop culture as “bite-size bits for high-speed munching.”⁸⁷

However, the future success of this market lies in jeopardy due to a lack of editorial control over UGC.⁸⁸ Not only do these copyright issues hinder the capability of these systems to function normally, but they also cause expensive lawsuits that drain the court system of its time and resources.⁸⁹

The relevant laws surrounding the noted case are hostile and counterproductive towards solving the problem of copyright infringement. Requirements such as red flag knowledge encourages service provider employees in the industry to keep UGC at arm’s length and never inspect it closely. Worse yet, such requirements encourage business owners of video sharing services to employ a bare minimum number of staff so that the service’s chance of exposure to UGC is significantly reduced. This strategy allows businesses to minimize liability at the cost of providing better services for consumers. Given the high cost and damage to reputation a potential lawsuit could bring, it would not be unreasonable for businesses to adopt this strategy. The result is a shrinking market that could have integrated new technologies that fostered creativity—a result that the U.S. copyright system was set out to avoid.

As we increasingly rely on the Internet for entertainment and productivity, consumers’ demand for a healthy and efficient online environment is more pressing than ever. Unfortunately, the laws

83. Meeyoung Cha et al., *I Tube, You Tube, Everybody Tubes: Analyzing the World’s Largest User Generated Content Video System*, KAIST 1, <http://an.Kaist.ac.Kr/traces/papers/imc131-cha.pdf> (last visited Sept. 16, 2014).

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.* (citing Nancy Miller, *Manifesto for a New Age*, WIRED (Mar. 2007), <http://archive.wired.com/wired/archive/15.03/snackmanifesto.html>).

88. *Id.*

89. *Id.* at 2. For a thorough statistical analysis of user-generated content systems, see *id.*

regulating the online community of person-to-person sharing hamper efficiency by disincentivizing editorial control and consequently encouraging more lawsuits. Copyright protection was designed to strike a balance between consumer and producer interests, but cases like *Viacom* achieved a result that runs the risk of hurting both sides and burying an entire industry. Understandably, Judge Abrams was not at liberty to significantly change the laws on red flag knowledge due to the precedent the Second Circuit had set in *Viacom*. He did, however, take a step in the right direction and set a precedent by allowing state laws regulating pre-1972 sound recordings to fall outside of safe harbor protection. If state laws were allowed to regulate UGC more extensively, the corrosive effects relevant provisions of the DMCA have on the online UGC market might just diminish.

Tong Xu*

* © 2014 Tong Xu. Junior Member, Volume 17, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2016, Tulane University Law School; M.A. 2013, Tulane University; B.A. 2012, *cum laude*, Tulane University. The author would like to thank her friends and family for their love and support in writing this Note; the author would also like to thank the editors and staff of Volume 17 for their hard work and dedication to the *Journal*.