SMU | Dedman School of Law

SMU Law Review

Volume 64 | Issue 2 Article 7

January 2011

A Contractual Deterrence Strategy for User-Generated Copyright Infringement and Subsequent Service Provider Litigation

Amanda Harmon Cooley

A CONTRACTUAL DETERRENCE STRATEGY FOR USER-GENERATED COPYRIGHT INFRINGEMENT AND SUBSEQUENT SERVICE PROVIDER LITIGATION

*Amanda Harmon Cooley**

TABLE OF CONTENTS

I. INTRODUCTION 692
II. WHY INTERNET AND ONLINE SERVICE PROVIDERS SHOULD DO MORE TO DETER USER-GENERATED COPYRIGHT INFRINGEMENT THAN MEET THE DMCA'S THRESHOLD REQUIREMENTS FOR SAFE HARBOR ELIGIBILITY 696
A. *VIACOM INTERNATIONAL INC. V. YOUTUBE, INC.* 696
B. DMCA SAFE HARBOR ELIGIBILITY UNDER 17 U.S.C. § 512(i) 699
C. THE NEED FOR INCREASED DETERRENCE OF USER-GENERATED COPYRIGHT INFRINGEMENT BY INTERNET AND ONLINE SERVICE PROVIDERS 708
III. DETERRENCE OF USER-GENERATED COPYRIGHT INFRINGEMENT THROUGH STRENGTHENED USER AGREEMENTS 713
A. CONTRACT FORMATION AND ACCOUNT CREATION 716
B. CONTRACT DRAFTING: DMCA ACCOUNT TERMINATION POLICIES AND OTHER REMEDIAL PROVISIONS IN USER AGREEMENTS 725
C. THE OPEN ENFORCEMENT OF CONTRACTUAL PROVISIONS IN USER AGREEMENTS 729
IV. CONCLUSION 732

LEGISLATION . . . is enacted, it is true, from an experience of evils but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes. Therefore a principle, to be vital, must be

* Assistant Professor of Law, South Texas College of Law. J.D., The University of North Carolina at Chapel Hill, 2003. B.A., The University of North Carolina at Chapel Hill, 2000. The author would like to thank South Texas College of Law for its research support.

capable of wider application than the mischief which gave it birth."[1]

I. INTRODUCTION

As technology evolves, society is confronted by a broad spectrum of new problematic conduct with which legislatures and courts often struggle to keep pace.[2] Internet activity has presented novel legal dilemmas, especially when such activity is compared to traditional conceptions of civil and criminal law.[3] In many situations, there is little, if any, precedent for addressing harm that has been facilitated or magnified by dramatic advances in online technology.[4] As a result, the elemental constructs, confines, and remedies of cyberlaw are still in a state of dynamic expansion.[5]

A growing area of development in this terrain of law involves statutory safe harbor and Good Samaritan provisions that have been interpreted to limit the liability of Internet and online service providers for certain tortious or infringing conduct of their service users.[6] Prominent examples of federal legislation with these types of statutory provisions include the Digital Millennium Copyright Act (DMCA)[7] and the Communications Decency Act (CDA).[8] In many instances, federal courts have construed these statutory provisions of the DMCA and the CDA broadly, granting service providers protection from liability for a variety of copyright in-

1. Weems v. United States, 217 U.S. 349, 373 (1910).

2. *See* Edward Lee, *Technological Fair Use*, 83 S. CAL. L. REV. 797, 839 (2010) (discussing the dynamic relationship between emerging technology and the development of the law).

3. *See* Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 46 (2007) (discussing the courts' struggles with new issues in technology in both criminal and civil matters).

4. *See, e.g.*, David Hunn & Joel Currier, *Law Lags as Taunts Ruin Lives*, ST. LOUIS POST-DISPATCH, Nov. 19, 2007, at B1 (explaining how cyberbullying could not be the basis for a state criminal prosecution as it had not yet been addressed by the Missouri legislature).

5. *See, e.g.*, Adrian McCoy, *Cyberspace Becoming a Legal Battleground*, PITTSBURGH POST-GAZETTE, July 5, 2008, at A1 ("Unlike other areas of commerce that can turn to historical traditions to help settle disputes and guide the development of the law, the law of the Internet has no history to fall back on. . . . As a result, the legal principles governing . . . cyberspace are still in a state of flux.").

6. *See, e.g.*, S. REP. NO. 105-190, at 19 (1998) (explaining its reasoning in the creation of the Digital Millennium Copyright Act as "[r]ather than embarking upon a wholesale clarification of these [common law copyright infringement] doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers").

7. *See* 17 U.S.C. § 512(c) (2006) (providing the Online Copyright Infringement Liability Limitation Act (OCILLA) safe harbor provisions, which outline the conditions of safe harbor protection for Internet and online service providers from copyright infringement liability).

8. *See* Communications Decency Act, 47 U.S.C. § 230 (2006) (providing immunity to Internet and online service providers for claims related to publication of third-party created content under its Good Samaritan provision).

fringement claims[9] and state law claims.[10] A significant example of this type of construction of the DMCA was at the basis of the landmark decision in *Viacom International Inc. v. YouTube, Inc.*[11]

These types of DMCA safe harbor decisions have provoked—and will continue to create—considerable controversy regarding the proper balance between Internet freedom and the safeguarding of individual rights in a cyber medium.[12] Given the high stakes of these decisions,[13] it is likely that future industry, scholarly, and media commentary will concentrate on whether or not there has been congressional nearsightedness[14] or judicial overreaching[15] in the area of statutory limitation of liability provisions for Internet and online service providers. Although the participants in this debate represent a divergent spectrum of perspectives,[16] most of these participants agree on the malignancy of cyber-harms and the importance of maintaining legal rights even in the context of evolving Internet technology.[17]

---

9. *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1155 (N.D. Cal. 2008) (finding that the defendant was entitled to safe harbor protection from the copyright infringement lawsuit premised on user-generated content on the defendant's website).

10. *See, e.g.*, Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969 (N.D. Ill. 2009) (finding that Craigslist was entitled to CDA immunity in a public nuisance lawsuit brought by Cook County Sheriff Thomas Dart based on content that allegedly solicited prostitution).

11. *See* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 529 (S.D.N.Y. 2010) (finding that the defendants were entitled to safe harbor protection pursuant to the DMCA).

12. *See, e.g.*, David Ludwig, *Shooting the Messenger: ISP Liability for Contributory Copyright Infringement*, 2006 B.C. INTELL. PROP. & TECH. F. 478, ¶ 2 (2006) (arguing that cases involving narrow judicial interpretation of the DMCA safe harbor provisions risk a "significant chilling effect on ISP investment in the internet").

13. *See* David Carr, *Heedlessly Hijacking Content*, N.Y. TIMES, June 28, 2010, at B1 (discussing the $1 billion remedy sought in the *Viacom* lawsuit and Viacom's announced intention to appeal the decision).

14. This type of critical analysis will likely center on the DMCA's failure to achieve its legislative purpose. *See, e.g.*, H.R. REP. NO. 105-551, pt. 2, at 49–50 (1998) ("The liability of on-line service providers and Internet access providers for copyright infringements that take place in the on-line environment has been a controversial issue. Title II of the [DMCA] addresses this complex issue. Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.").

15. *See, e.g.*, Ronald A. Cass, *Google Wins Round One Against Viacom*, FORBES (June 24, 2010, 6:40 PM), http://www.forbes.com/2010/06/24/google-viacom-youtube-lawsuit-opinions-contributors-ronald-a-cass.html (arguing that the *Viacom* court's "capacious reading of the [DMCA's] quite limited insulation of Internet site operators creates a harbor broad enough to sink the protection copyright holders had enjoyed under the law").

16. *Compare id.* (advocating for narrow judicial interpretation of the DMCA) *with* Ludwig, *supra* note 12, ¶ 2 (advocating for broad judicial interpretation of the DMCA).

17. *See, e.g.*, Cass, *supra* note 15 (describing intellectual property rights in the context of Internet technology as "cornerstones of successful societies"); *see also* Ludwig, *supra* note 12, ¶ 80 (discussing the important value of protecting intellectual property rights in the context of Internet technology). *But see* Debora Halbert, *Mass Culture and the Culture of the Masses: A Manifesto for User-Generated Rights*, 11 VAND. J. ENT. & TECH. L. 921, 935–36 (2009) (arguing that all direct appropriations of copyrighted work as posted on YouTube should be considered "fair use" rather than copyright infringements).

Essentially, it is this infringing behavior by users, which disregards others' intellectual property rights,[18] that has been the genesis for DMCA safe harbor-related litigation involving Internet and online service providers.[19] This root cyber-harm needs solutions. While a statutory amendment or a Supreme Court interpretation of the DMCA might clarify the rights of service providers in the context of DMCA safe harbor-related litigation,[20] these measures do not squarely address the underlying problem of user-generated copyright infringement. Additionally, while the DMCA conditions safe harbor eligibility on an adopted, reasonably implemented, and announced account termination policy for repeat infringers,[21] mere account termination in its present form is not a sufficient deterrent to online copyright infringement.[22] Apart from these avenues, aggrieved copyright owners can continue to pursue direct liability lawsuits against the infringer.[23] However, this solution often is a fruitless one, given both the anonymity and solvency issues that can arise in an Internet direct copyright infringement lawsuit.[24] The question then becomes what other remedies might be available to deter infringing conduct by users of an online medium.

This Article explores the ways in which Internet and online service providers could contribute to the deterrence of online user-generated copyright infringement, and also proactively avoid future DMCA safe harbor-related litigation for infringing user conduct, via strengthened

18. Online conduct that constitutes pure copyright infringement is the target of this Article, as the author recognizes the lawful validity and importance of fair use of copyrighted material. *See* 17 U.S.C. § 107 (2006). The reform strategy that is advanced in this piece does not include the proposition that user agreements should incorporate contractual provisions that conflict with this important ideal. *See, e.g.*, Bradley E. Abruzzi, *Copyright, Free Expression, and the Enforceability of "Personal Use-Only" and Other Use-Restrictive Online Terms of Use*, 26 SANTA CLARA COMPUTER & HIGH TECH. L.J. 85, 87–88 (2010) (discussing the types of user agreements that "essentially allow private parties to override, unilaterally and in their favor, the careful balance U.S. copyright law strikes between proprietary rights and public privileges").

19. Throughout this Article, "DMCA safe harbor-related litigation" will refer to cases that are brought against Internet or online service providers; that are precipitated by user-generated copyright infringement; and that involve a determination as to whether the Internet or online service provider qualifies for DMCA safe harbor protection.

20. Indeed, the original intent of the enactment of OCILLA within the DMCA was to provide clarification to the "[d]ifficult and controversial questions of copyright liability in the online world." Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004).

21. *See* 17 U.S.C. § 512(i)(1)(A) (2006).

22. *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81, 83 (2010) (discussing how past efforts to curb online copyright infringement have not "made much of a dent" in this tortious behavior).

23. *See* Lateef Mtima, *Whom the Gods Would Destroy: Why Congress Prioritized Copyright Protection over Internet Privacy in Passing the Digital Millennium Copyright Act*, 61 RUTGERS L. REV. 627, 637 (2009) (discussing the substantial number of direct copyright infringement lawsuits that have been filed since the 1990s).

24. *See id.* at 638 (citing "the growing number of quasi-anonymous (and often judgment proof) individual infringers" as one reason why copyright owners started to sue Internet and online service providers for user-generated infringing content).

user agreements.[25] This type of contractual deterrence strategy would require modifications to the status quo of transactional practices within the Internet industry. Fortunately, the Internet allows for relatively swift and easy changes on the part of service providers.[26] Specifically, this approach could be accomplished through changes to the model of user agreements that would require more evidence of users' assent to the agreements and increased security measures for identity verification. In addition to these model changes involving contract formation, this approach would require robust contractual drafting with the inclusion of remedies for users' infringing conduct that are more stringent than the current provisions addressing termination of user accounts. Further, this approach would require actual enforcement of the user agreement when there is a breach by a user posting infringing content. Finally, Internet and online service providers would need to adopt integrated marketing campaigns to increase the transparency of their efforts to curb cyberharms that are perpetrated via their services.

The adoption, enforcement, and publication of contractual deterrent measures would result in manifold benefits for Internet and online service providers. This approach would demonstrate the good faith of these entities by reinforcing the culpability of the infringer, rather than the electronic forum provider. Further, adopting this approach would carry with it a pragmatic benefit. Essentially, if these contractual deterrents are an effective means to curb online copyright infringement (the root harm at issue in DMCA safe harbor-related litigation), then these measures could commensurately curb the number of copyright infringement lawsuits that are filed against service providers.

In summary, Part II of this Article briefly introduces the present state of the law involving DMCA safe harbor eligibility through the lens of the *Viacom* case. In addition to providing the relevant background for this Article, this Part specifically explores the account termination policy requirements under the DMCA and how they have been construed. This Part concludes by examining the reasons why Internet and online service providers should do more than meet the basic requirements for DMCA safe harbor eligibility. Part III provides a practical approach, via contract formation, drafting, and enforcement, for increased deterrence of copyright infringement by online service users. This Part advocates for the implementation of stronger user agreements by Internet and online service providers. By analyzing the terms of use that are currently employed by these entities, this Part recommends integrated reforms to online ac-

25. *See generally* Jane C. Ginsburg, *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 579 (2008) (suggesting that the Internet industry may start to adopt "proactive avoidance measures" as a way to protect businesses from liability for user-generated copyright infringement).

26. *See* William R. Mills, *The Decline and Fall of the Dominant Paradigm: Trustworthiness of Case Reports in the Digital Age*, 53 N.Y.L. SCH. L. REV. 917, 929 n.49 (2009) (describing the nature of most websites as "constantly changing, [and] evolving").

count creation, maintenance, and termination. Specifically, this approach advocates for (1) increased mechanisms to evidence assent by the user to the user agreement; (2) additional security measures for identity verification in account creation; (3) more transparent provisions on account termination; (4) the inclusion of liquidated damages clauses; (5) the open enforcement of current indemnification provisions and other remedial provisions; and (6) increased marketing of these efforts.

Such an approach would preserve the flourishing of Internet freedom,[27] thereby insulating commercial and speech protections, while contemporaneously allowing for increased safeguarding of intellectual property rights.[28] Additionally, by curbing user-generated copyright infringement, such an approach could lead to a reduction in the number of lawsuits that are filed against service providers where the causes of action are premised on this type of user behavior.[29] It is this pragmatic reasoning that should provide Internet and online service providers with the impetus to adopt, enforce, and market stronger user agreements.

II. WHY INTERNET AND ONLINE SERVICE PROVIDERS SHOULD DO MORE TO DETER USER-GENERATED COPYRIGHT INFRINGEMENT THAN MEET THE DMCA'S THRESHOLD REQUIREMENTS FOR SAFE HARBOR ELIGIBILITY

A. *VIACOM INTERNATIONAL INC. V. YOUTUBE, INC.*

On June 23, 2010, a groundbreaking decision was issued by the United States District Court for the Southern District of New York in *Viacom International Inc. v. YouTube, Inc.*[30] In this $1 billion copyright infringement case,[31] Viacom sought to hold YouTube and Google liable for the

27. This is an important and valuable aspect of advances in digital technology. The intent of this Article is not to paint Internet and online service providers as being bad actors, but rather to investigate how these entities can contribute to the deterrence of online copyright infringement. Inarguably, these entities provide considerable benefits to millions of people. *See, e.g.*, Nadia L. Luhr, Note, *Iran, Social Media, and U.S. Trade Sanctions: The First Amendment Implications of U.S. Foreign Policy*, 8 FIRST AMEND. L. REV. 500, 511 (2010) ("Because of these tools [Twitter, Facebook, and YouTube], news consumers were able to learn of the events taking place [in the 2009 Iranian elections and their aftermath] from sources other than heavily censored or state-sponsored media and were able to engage in open communication with those undertaking a massive civil rights movement against a repressive regime.").

28. These types of contractual avoidance measures would help ease the significant concerns that have been stressed in discussion of the DMCA safe harbor provisions. *See, e.g.*, Ludwig, *supra* note 12, at ¶¶ 1–2.

29. *See, e.g.*, Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment on Liability and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense at 1-4, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103) (premising claims of liability on the foundation of user copyright infringement).

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

31. *See* First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial at 19-29, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103).

unauthorized user-posting of thousands of Viacom's copyrighted works to YouTube's website.[32] The defendants moved for summary judgment, claiming that they qualified for DMCA safe harbor protection pursuant to 17 U.S.C. § 512.[33] Viacom contested this assertion in its cross-motion for summary judgment.[34]

Although the court stated that "a jury could find that the defendants not only were generally aware of, but welcomed, copyright-infringing material being placed on their website,"[35] it ultimately granted the defendants' motion for summary judgment on all claims of direct and secondary copyright infringement based on a finding of DMCA safe harbor protection.[36] At the heart of this finding was a statutory construction of 17 U.S.C. § 512(c)(1), which provides:

> (1) A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), 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—
>
> (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) 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
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[37]

For the court, the key issue was whether the language in § 512(c)(1)(A)(i) and (ii) "mean[s] a general awareness that there are infringements (here, claimed to be widespread and common), or rather mean[s] actual or constructive knowledge of specific and identifiable infringements of individual items."[38]

---

32. *See id.* at 9, 20–29 (providing that Google owns YouTube, Inc.); Defendants' Answer to First Amended Complaint and Demand for Jury Trial at 5, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103) (providing that "Google acquired YouTube, Inc. for $1.65 billion in a transaction announced on October 9, 2006 and closed on November 13, 2006").

33. *Viacom*, 718 F. Supp. 2d at 516.

34. *See id.*

35. *Id.* at 518.

36. *See id.* at 529 (granting defendants' motion for summary judgment and denying plaintiffs' motion for summary judgment).

37. 17 U.S.C. § 512(c)(1) (2006).

38. *Viacom*, 718 F. Supp. 2d at 519.

Prior to resolving this central question, the court made some preliminary determinations outlining the applicability of the DMCA safe harbor provisions to the defendants. After finding that YouTube met the DMCA safe harbor definition of a service provider "as 'a provider of online services or network access, or the operator of facilities therefor,'"[39] the court also determined that YouTube had complied with the DMCA notice and takedown provisions.[40] With these initial findings in place, the court proceeded to interpret 17 U.S.C. § 512(c)(1). Relying largely on the legislative history of the DMCA, the court determined "that the phrases 'actual knowledge that the material or an activity' is infringing, and 'facts or circumstances' indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough."[41]

Consequently, the court determined that YouTube had complied with the requirements of the statute and was therefore entitled to safe harbor protection.[42] In issuing its opinion, the court stressed that, absent an online service provider's "knowledge of specific and identifiable infringements of particular individual items,"[43] which necessitates removal of the infringing material, copyright owners have the burden to identify infringement to online service providers.[44] The court made clear that "[g]eneral knowledge that infringement is 'ubiquitous' does not impose a duty on the service provider to monitor or search its service for infringements."[45]

In a concluding section of the opinion, the court also briefly addressed Viacom's argument that YouTube was not subject to DMCA safe harbor protection as it had not adopted and implemented a reasonable policy for the termination of accounts of repeat infringers.[46] Under 17 U.S.C. § 512(i), in order to be eligible for safe harbor protection, a service provider must "[have] adopted and reasonably implemented, and [inform] 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

39. *See id.* at 526 (quoting 17 U.S.C. § 512(k)(1)(B) (2006)).

40. *See id.* at 524 ("[T]he present case shows that the DMCA notification regime works efficiently: when Viacom over a period of months accumulated some 100,000 videos and then sent one mass take-down notice on February 2, 2007, by the next business day YouTube had removed virtually all of them."); *see also* 17 U.S.C. §§ 512(c)(2), (3) (2006) (providing the DMCA required notification and takedown procedures).

41. *Viacom*, 718 F. Supp. 2d at 523.

42. *See id.* at 526 (reaffirming YouTube's protection under the DMCA safe harbor provisions).

43. *Id.* at 523.

44. *See id.* at 525 ("[I]f a service provider knows (from notice from the owner, or a 'red flag') of specific instances of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the infringement.").

45. *Id.*

46. *See id.* at 527–28.

system or network who are repeat infringers."[47]

YouTube's termination policy was a "three strikes" policy by which a repeat infringer's account would be terminated "after warnings from YouTube (stimulated by its receipt of DMCA notices) that the user [had] uploaded infringing matter."[48] Upon termination of the account, "YouTube remove[d] *all* of that user's videos, not merely those against which allegations of infringement have been levied, and it permanently block[ed] the account from being reestablished."[49] The court found that YouTube's policy, which counted "as only one strike against a user both (1) a single DMCA take-down notice identifying multiple videos uploaded by the user, and (2) multiple take-down notices identifying videos uploaded by the user received by YouTube within a two-hour period,"[50] qualified as a "reasonably implemented" policy that allowed YouTube safe harbor eligibility.[51]

B. DMCA Safe Harbor Eligibility Under 17 U.S.C. § 512(i)

Viacom is not the first case to address the conditions for DMCA safe harbor eligibility under 17 U.S.C. § 512(i). However, it is one of a limited number of decisions to do so, which makes the question of satisfactory adoption and implementation of account termination policies in order to qualify for safe harbor eligibility a far from settled one.[52] In order to qualify for DMCA safe harbor protection, an entity must meet the threshold account termination policy requirements of § 512(i).[53] Such a finding is an imperative prerequisite to the question of qualification within the safe harbor.[54] However, many of the key terms of § 512(i) are not defined by the statute; these terms include "reasonably imple-

47. 17 U.S.C. § 512(i)(1) (2006).

48. *Viacom*, 718 F. Supp. 2d at 527.

49. Memorandum of Law in Support of Defendants' Motion for Summary Judgment at 23, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103).

50. *Viacom*, 718 F. Supp. 2d at 527–28.

51. *See id.* at 528.

52. *See* Jonathan J. Darrow & Gerald R. Ferrera, *Social Networking Web Sites and the DMCA: A Safe-Harbor from Copyright Infringement Liability or the Perfect Storm?*, 6 Nw. J. Tech. & Intell. Prop. 1, 15, 33 (2007) (describing the case law interpreting the requirements of 17 U.S.C. § 512(i) as "sparse").

53. *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109 (9th Cir. 2007) (discussing that a threshold condition for eligibility under the DMCA safe harbor provisions is compliance with 17 U.S.C. § 512(i)).

54. *See* Ellison v. Robertson, 357 F.3d 1072, 1080–82 (9th Cir. 2004) (reversing a district court's summary judgment in favor of America Online, Inc., based on a finding of DMCA safe harbor limitation of liability due to triable facts on whether the defendant met the threshold requirements of 17 U.S.C. § 512(i), and remanding to the trial court the question of said eligibility); *see also* UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1087 (C.D. Cal. 2008) (noting that "[m]ost cases that have addressed the § 512(c) safe harbor have examined whether the defendant meets the prerequisites enumerated in § 512(c)(1)(A-C) and § 512(i)").

mented,"[55] "appropriate circumstances,"[56] and "repeat infringer."[57] Additionally, the legislative history on this subsection does not provide clear guidance as to its meaning:

> [T]he Committee does not intend this provision to . . . suggest[ ] that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing. However, those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.[58]

Given the lack of specific definitions in this subsection, especially compared to the detailed requirements of the statute as to infringement notice and takedown procedures in § 512(c), qualification for DMCA safe harbor eligibility under § 512(i) rests largely on judicial interpretation.[59] Because only a handful of courts have examined the meaning of this subsection's requirements, those decisions, like *Viacom*, are particularly valuable for this developing area of law. In fact, the case law in this area is in such an unsettled state that at least one court has denied the discretionary award of attorneys' fees pursuant to the Copyright Act to prevailing parties that have been deemed to meet the § 512(i) requirements and the remaining DMCA safe harbor conditions.[60] Consequently, it is important to discuss the approaches of the relatively few decisions, which, in examining other Internet and online service providers' account termination policies, have provided additional or differing interpretations of the requirements of 17 U.S.C. § 512(i).

The most recent circuit court examination of the meaning of this subsection took place in 2007. In *Perfect 10, Inc. v. CCBill LLC*, the United States Court of Appeals for the Ninth Circuit held "that a service provider 'implements' a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications."[61] Further, the court found that "[t]he statute

---

55. *See Perfect 10*, 488 F.3d at 1109 ("The statute does not define 'reasonably implemented.'").

56. *See id.* at 1111 ("Section 512(i) itself does not clarify when it is 'appropriate' for service providers to act.").

57. *See* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1100–01 (W.D. Wash. 2004) ("The key term, 'repeat infringer,' is not defined and the subsection never elaborates on what circumstances merit terminating a repeat infringer's access.").

58. H.R. REP. NO. 105-551, pt. 2, at 61 (1998); *see also* S. REP. NO. 105-190, at 51–52 (1998) (providing a similar discussion on this statutory provision).

59. *See Corbis*, 351 F. Supp. 2d at 1101 (discussing how the "open-ended language [of § 512(i)] contrasts markedly with the specific requirements for infringement notices and take-down procedures set forth in § 512(c)").

60. *See* UMG Recordings, Inc. v. Veoh Networks, Inc., No. CV 07-5744 AHM (AJWx), 2010 U.S. Dist. LEXIS 44430, at *5–8 (C.D. Cal. Apr. 6, 2010) (denying the prevailing party's motion for attorneys' fees as the opposing party's claims regarding a lack of DMCA eligibility were not "objectively unreasonable").

61. *Perfect 10*, 488 F.3d at 1109.

permits service providers to implement a variety of procedures, but an implementation is reasonable if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright."[62] However, the court also noted that "[t]o identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement."[63] Instead, "[a] policy is unreasonable only if the service provider failed to respond when it had knowledge of the infringement."[64]

These definitions were a central part of the holding in *Perfect 10*. In this case, "Perfect 10, the publisher of an adult entertainment magazine and the owner of [a] subscription website . . . allege[d] that CCBill and CWIE violated copyright . . . laws by providing [web hosting and paid subscription] services to websites that posted images stolen from Perfect 10's magazine and website."[65] Perfect 10, along with nonparty celebrities who had images featured in Perfect 10's venues, sent several notices of copyright infringement to the defendants' designated agent prior to filing the lawsuit.[66] The defendants claimed that they were protected by the DMCA safe harbor provisions.[67] The district court agreed, granting the defendants' motion for summary judgment.[68]

On appeal, Perfect 10 raised several errors with the trial court's decision. First, Perfect 10 argued that "there [was] a genuine issue of material fact whether CCBill and CWIE prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters."[69] The Ninth Circuit rejected this argument, refused to classify this as a substantial failure "to record webmasters associated with allegedly infringing websites,"[70] and found that the defendants' record of most (but not all) infringing webmasters "[d]id not raise a triable issue of fact that CCBill and CWIE did not implement a repeat infringer policy."[71]

Here, the Ninth Circuit distinguished the defendants' recordkeeping from that of the defendants in *Ellison v. Robertson*,[72] a case decided by the court in 2004, and the *Aimster*[73] litigation.[74] In *Ellison*, the Ninth Circuit reversed the district court's grant of summary judgment to America Online, Inc. (AOL) on a finding of § 512(i) qualification for DMCA limitation of liability based on a determination that there were triable issues of fact on the question of reasonable implementation of an

62. *Id.*
63. *Id.* at 1111.
64. *Id.* at 1113.
65. *Id.* at 1108.
66. *See id.*
67. *See id.*
68. *See id.*
69. *Id.* at 1110.
70. *Id.*
71. *Id.* at 1111.
72. Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004).
73. *See In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).
74. *See Perfect 10*, 488 F.3d at 1110.

account termination policy.[75] In that instance, AOL changed its designated copyright notice agent's email address and failed to give notice of the change to the United States Copyright Office for several months, "allow[ing] notices of potential copyright infringement to fall into a vacuum and go unheeded."[76] In the *Aimster* litigation, the Seventh Circuit affirmed the district court's determination that Aimster did not meet the DMCA threshold requirements of a reasonably implemented account termination policy under § 512(i).[77] In these cases, Aimster's encryption completely masked the identity of the file-transferring users.[78] The Seventh Circuit stressed that, rather than "discourag[ing] repeat infringers of the plaintiffs' copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement."[79] The *Perfect 10* court determined that "[u]nlike *Ellison* and *Aimster*, where the changed email address and the encryption system ensured that *no* information about the repeat infringer was collected, it is undisputed that CCBill and CWIE recorded most webmasters."[80]

In addition to its first assigned error, "Perfect 10 claim[ed] that CCBill and CWIE unreasonably implemented their repeat infringer policies by tolerating flagrant and blatant copyright infringement by its users despite notice of infringement from Perfect 10, notice of infringement from copyright holders not a party to this litigation and 'red flags' of copyright infringement."[81] With respect to Perfect 10's individual claimed notice of infringement, the Ninth Circuit affirmed the district court's finding that Perfect 10 failed to send takedown notices that substantially complied with § 512(c)(3).[82] Although the notices identified specific infringing works, they failed to include the complainant's declaration, which reads "under penalty of perjury, that he is authorized to represent the copyright holder, and that he has a good-faith belief that the use is infringing."[83] The court determined that these noncompliant communications were fatal to this assigned error, stressing the important First Amendment implications of online content takedowns.[84] The court urged that:

> This requirement is not superfluous. Accusations of alleged infringement have drastic consequences: A user could have content removed, or may have his access terminated entirely. If the content infringes, justice has been done. But if it does not, speech protected

75. *See Ellison*, 357 F.3d at 1077.
76. *Id.* at 1080.
77. *See Aimster*, 334 F.3d at 656.
78. *See id.* at 655.
79. *Id.*
80. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1110 (9th Cir. 2007) (emphasis in original).
81. *Id.* at 1111.
82. *See id.* at 1111–12.
83. *Id.* at 1112.
84. *See id.*

> under the First Amendment could be removed. We therefore do not require a service provider to start potentially invasive proceedings if the complainant is unwilling to state under penalty of perjury that he is an authorized representative of the copyright owner, and that he has a good-faith belief that the material is unlicensed.[85]

Consequently, the court found that these noncompliant communications did not raise a genuine issue of material fact of a failure to reasonably implement the defendants' account termination policy.[86] In doing so, the Ninth Circuit stressed that "[t]he DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright."[87] Furthermore, in language that is a precursor to the rationale at the heart of the *Viacom* decision, the court clearly "decline[d] to shift a substantial burden from the copyright owner to the provider."[88]

Building on this line of reasoning, the Ninth Circuit similarly rejected Perfect 10's argument that red flags in the names of websites that received services from the defendants, such as "illegal.net" and "stolencelebritypics.com," provided the defendants with "aware[ness] of apparent infringing activity."[89] The Ninth Circuit stated that it would "not place the burden of determining whether photographs are actually illegal on a service provider," and, therefore, affirmed the district court's determination on this point.[90]

Despite the strong position that the court took on most of Perfect 10's assignments of error, the Ninth Circuit did remand the case to the district court "for determination of whether CCBill and/or CWIE implemented its repeat infringer policy in an unreasonable manner with respect to any copyright holder other than Perfect 10."[91] Further, the Ninth Circuit "remand[ed] to the district court to determine whether third-party notices made CCBill and CWIE aware that it provided services to repeat infringers, and if so, whether they responded appropriately."[92] In this instance, the district court had refused to consider the evidence of the nonparty celebrities who had images featured in Perfect 10's venues and who had sent several notices of copyright infringement to the defendants' designated agent.[93] The Ninth Circuit based its remand on the statutory demands of § 512(i), which "requires an assessment of the service provider's 'policy,' not how the service provider treated a particular copyright holder."[94] Consequently, the appellate court determined that the evi-

85. *Id.*
86. *See id.* at 1113.
87. *Id.*
88. *Id.*
89. *See id.* at 1114.
90. *Id.*
91. *Id.* at 1113.
92. *Id.* at 1115.
93. *See id.* at 1113.
94. *Id.*

dence of the nonparty notices was relevant to the determination of reasonable implementation of the defendants' repeat infringer account termination policy.[95]

Perfect 10 is an important case for any study of DMCA safe harbor-related litigation, as it illustrates one of the few judicial interpretations of the meaning of § 512(i)[96] and has been used for the basis of argument in subsequent § 512(i) cases. Specifically, plaintiffs in other DMCA safe harbor-related lawsuits have attempted to expand the rationale used by the Ninth Circuit in *Perfect 10*.[97] These plaintiffs have argued that termination policies do not fall under the auspices of § 512(i) because they do not bar repeat infringers from reregistering with different contact information,[98] they do not automatically terminate accounts of users who upload content that is blocked by a filtering system,[99] and they do not automatically terminate accounts after one instance of infringement.[100] Largely, these efforts to invalidate the designation of safe harbor eligibility based on these types of account termination policies have been unsuccessful.

For example, in the 2008 *Io Group, Inc. v. Veoh Networks, Inc.*[101] case, Veoh, a software provider and website operator of an Internet television network that allowed users to upload video content, was sued for copyright infringement by a copyright holder, Io.[102] Veoh asserted in its motion for summary judgment that it was entitled to DMCA safe harbor protection.[103] Io countered in its own motion for summary judgment that Veoh did not satisfy the DMCA safe harbor eligibility conditions regarding account termination policies pursuant to § 512(i) because Veoh's policy did "not prevent repeat infringers from reappearing on Veoh under a pseudonym and a different email address."[104] Essentially, Io claimed that because there was no reasonable tracking of infringers, the "repeat infringer policy [was] tantamount to no policy at all."[105] The court rejected Io's argument, stating that Veoh met the requirements of a reasonable § 512(i) policy as defined by the Ninth Circuit in *Perfect 10* and that

95. *See id.*

96. *See* UMG Recordings, Inc. v. Veoh Networks, Inc., No. CV 07-5744 AHM (AJWx), 2010 U.S. Dist. LEXIS 44430, at *5 (C.D. Cal. Apr. 6, 2010) ("There has not been a great deal of caselaw interpreting under what circumstances a service provider's termination policies are 'reasonably implemented' (or what are the 'appropriate circumstances' for terminating a repeat infringer).").

97. *See e.g.*, UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1116 (C.D. Cal. 2009); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1103, 1110 (W.D. Wash. 2004).

98. *See Corbis*, 351 F. Supp. 2d at 1103, 1110 (finding that Amazon met the threshold requirements of § 512(i) despite the fact that "Amazon's infringement policy has not been able to prevent certain vendors from reappearing on [its] platform under pseudonyms").

99. *See UMG Recordings*, 665 F. Supp. 2d at 1116.

100. *See id.* at 1118.

101. Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

102. *See id.* at 1136–37.

103. *See id.* at 1135.

104. *Id.* at 1143–44.

105. *Id.* at 1144.

"Veoh does track content that has been identified as infringing and permanently blocks that content from ever being uploaded by any user."[106] Further, the court discarded Io's proposition that a reasonable § 512(i) policy would require Veoh "to track users by their actual names or by Internet Protocol ('IP') addresses,"[107] claiming that this would not be a "more effective reasonable means of implementation,"[108] in part, because IP addresses "do not distinguish between users."[109] Consequently, the court granted the defendant's motion for summary judgment based on a finding that Veoh qualified for safe harbor protection.[110]

Veoh was at the center of another case in which its account termination policy was challenged for falling outside of the scope of § 512(i). In *UMG Recordings, Inc. v. Veoh Networks, Inc.*, UMG argued that "Veoh's policy [was] inadequate because it [did] not automatically terminate users who upload videos that are blocked by the Audible Magic filter."[111] This proprietary filtering system provided technology intended to block the uploading of copyrighted content.[112] The court rejected UMG's argument, referencing the core of the *Perfect 10* decision:

> If, under [*Perfect 10*], a notice by a copyright holder that specific material is allegedly infringing is not a sufficient basis for terminating a user because it lacks a sworn declaration that the notifier has a good-faith belief that the material is unlicensed, then it stands to reason that Audible Magic's automated filter also cannot be a valid basis.[113]

The court supported this proposition with a focus on reliability, noting Veoh's inability to verify "the accuracy of [third-party] Audible Magic's database."[114]

From there, the court transitioned to the idea of responsibility that is an undercurrent in all DMCA safe harbor-related litigation, finding that even if Veoh did have the ability to verify the filter's accuracy, "it would be unreasonable to place that burden on Veoh."[115] The court grounded its discussion of verifiability and reliability with a pragmatic recognition of Veoh's responses to DMCA takedown notices:

---

106. *Id.* at 1145.
107. *Id.*
108. *Id.*
109. *Id.*
110. *See id.* at 1155.
111. UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1116 (C.D. Cal. 2009).
112. *See id.* at 1103; *see also Audible Magic Content Identification Services*, AUDIBLE MAGIC, http://audiblemagic.com/products-services/contentsvcs/ (last visited Jan. 15, 2011) ("Audible Magic's content recognition services ensure copyright compliance, and enable new ways to monetize music and video on the Internet. Automatically scan user-generated or user-uploaded media files, identify any copyright owners as well as their usage rules, categorize and tag the content, associate the content with revenue opportunities and empower your online business model.").
113. *UMG Recordings*, 665 F. Supp. 2d at 1117–18.
114. *Id.* at 1118.
115. *Id.*

> [a]s a practical matter, when notice of a user's alleged infringement is not reliable enough to justify terminating the user's account, a service provider's removal of the allegedly infringing material is sufficient evidence of compliance with the DMCA. In this case, when Veoh received notices of infringement it promptly removed the material identified.[116]

As a result, the court concluded that Veoh's failure to automatically terminate accounts of users who uploaded content that was blocked by the Audible Magic filtering system did not mean that its account termination policy fell outside of the requirements of § 512(i).[117]

In addition to the filtering technology argument, UMG also raised a precursive argument to the central § 512(i) claim of the *Viacom* case.[118] UMG asserted that Veoh did not comply with the DMCA account termination policy provisions based on Veoh's choice to not automatically terminate user accounts after one instance of infringement.[119] Specifically, UMG claimed that Veoh's policy was inadequate because "it does not necessarily terminate users who upload multiple videos that are identified in a single DMCA notice."[120] Veoh's procedure was to send a warning to a user who was identified in a takedown notice, even if that notice identified multiple instances of the uploading of infringing content by that user.[121] Veoh "then terminated the user's account if the user subsequently uploaded another infringing video."[122] The court was unconvinced by UMG's claim that this "two-strikes" policy failed to comply with the DMCA requirements.[123] Instead, the court found that "nothing in the statute, legislative history, or case law establish[ed] that such a policy is not reasonable or appropriate."[124] The court bolstered its conclusion by reasserting the undefined nature of the term "repeat infringer" within the statutory scheme of the DMCA and by finding that "Veoh's policy satisfies Congress's intent that 'those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.'"[125] Consequently, this case, with its finding of compliance with the DMCA § 512(i) requirements, provides another example of a court rejecting a plaintiff's attempt to stretch the *Perfect 10* rationale.[126]

The progression in this case law demonstrates the growing development of the meaning of an adopted, implemented, and publicized reason-

116. *Id.* at 1117–18.
117. *See id.* at 1116.
118. *See supra* text accompanying notes 46–51.
119. *See UMG Recordings*, 665 F. Supp. 2d at 1116.
120. *Id.*
121. *See id.*
122. *Id.*
123. *See id.* at 1118.
124. *Id.*
125. *Id.* (quoting H.R. REP. NO. 105-551, pt. 2, at 61 (1998)).
126. *See id.* at 1116 (finding that Veoh's "policy satisfies [§] 512(i)'s requirements, and achieves the provision's purpose of deterring infringement").

able policy for termination of accounts of repeat infringers as a threshold requirement for DMCA safe harbor eligibility under 17 U.S.C. § 512(i). Clearly, if an Internet or online service provider fails to designate an agent for claimed infringement notification or fails to terminate repeat infringers at all, then that provider will not qualify for DMCA safe harbor protection.[127] However, this type of clear demarcation is rarely present in DMCA safe harbor-related litigation. Conversely, in most of the relatively few cases that have examined this issue, the providers have designated an agent, adopted and implemented an account termination policy, and, pursuant to that policy, terminated some, but not all, repeat infringers.[128] Such was the case in *Viacom*.[129]

Viacom has thrust the matter of the § 512(i) threshold requirements for DMCA safe harbor eligibility into the legal limelight, with incredible stakes weighing in the balance. Given these issues, it is little surprise that Viacom swiftly announced its intention to appeal the decision.[130] Viacom filed its notice of appeal on August 11, 2010.[131] With such enormous physical and ideological costs at issue, the course of this appeal will be monitored by legions of Internet and online service providers, copyright holders, and Internet users.[132] It is unclear how the United States Court of Appeals for the Second Circuit will resolve the matter of YouTube's DMCA safe harbor status, given the various approaches that have been taken by the few courts that have addressed this issue.[133] Regardless of the ultimate decision by the Second Circuit, Internet and online service providers should do more to address the problem of online copyright infringement conducted by their users than only meet the baseline threshold requirements for DMCA safe harbor eligibility under § 512(i). A viable strategy to provide deterrence in this area is a contractual one.

---

127. *See, e.g.*, Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2010 U.S. Dist. LEXIS 85266, at *24–25 (N.D. Cal. Mar. 19, 2010) (denying a Rule 50 motion for judgment as a matter of law premised on the assertion of DMCA safe harbor protection where the defendants initially failed to have a designated agent to receive claimed infringement notices, thereafter designated an agent who admittedly did not understand the DMCA's requirements under §512(i), and failed to terminate repeat infringers).

128. *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1111 (9th Cir. 2007).

129. *See supra* text accompanying notes 46–51.

130. *See* Michael Fricklas, *Viacom Statements: The Court Ruling*, VIACOM, http://news.viacom.com/news/Pages/summaryjudgment.aspx (last visited Mar. 4, 2011); *see also* Andrew M. Harris & Donald Jeffrey, *Google's YouTube Didn't Infringe Viacom Copyrights, Judge Says*, BLOOMBERG BUSINESSWEEK (June 24, 2010, 12:04 AM), http://www.businessweek.com/news/2010-06-24/google-s-youtube-didn-t-infringe-viacom-copyrights-judge-says.html (discussing Viacom's post-decision email regarding its intent to appeal).

131. *See* Notice of Appeal at 1, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103).

132. *See* Gary Slapper, *The Battle for Copyright on YouTube; A New York Court Ruling in a Billion-Dollar Battle over Downloading Videos has Worried the Creative Industries*, TIMES (London), July 1, 2010, at 67 (discussing the case's significance for a variety of stakeholders).

133. *See supra* note 52 and accompanying text.

C. The Need for Increased Deterrence of User-Generated Copyright Infringement by Internet and Online Service Providers

A comprehensive review of all of the DMCA safe harbor-related litigation in the United States yields relatively few bright line rules, despite the congressional intention for "greater certainty" that supported the passage of this legislation.[134] Specifically, what is clear from the decisions that have interpreted the safe harbor eligibility requirements of 17 U.S.C. § 512(i) is this: in order to qualify for this eligibility, a service provider must "[have] adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[135] Although this mere recitation of the statutory requirements may seem pedantic, it is the singular consistent directive for Internet and online service providers that seek protection in the DMCA's safe harbor. There is little doubt that these requirements will gain more context with future judicial decisions and possible legislative clarification.[136] Indeed, contouring of liability and responsibility will be helpful in delineating the statutory baseline minimums for rights and duties of the stakeholders involved in DMCA safe harbor-related litigation.[137] However, it seems unlikely that this type of refinement of the DMCA will provide the necessary effect to curb the core harm of copyright infringement.[138]

In fact, somewhat ironically, one other aspect of clarity that emerges from the limited field of decisions that construe the safe harbor eligibility requirements pursuant to § 512(i) is that the existing remedies for repeated infringement, pursuant to the DMCA, are not significant or effec-

134. *See* S. REP. NO. 105-190, at 18 (1998) ("Title II [of the DMCA] preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."); *see also* H.R. REP. NO. 105-551, pt. 2, at 49–50 (1998) (same).

135. 17 U.S.C. § 512(i)(1) (2006).

136. Again, the original intent of the DMCA was to provide a balanced and clear approach to the problems of emerging technology that allowed for online copyright infringement. *See, e.g.*, Assaf Jacob & Zoe Argento, *To Cache or Not to Cache—That Is the Question; P2P "System Caching"—The Copyright Dilemma*, 31 WHITTIER L. REV. 421, 489 (2010) ("The DMCA safe harbor clauses were technology-specific amendments [that] . . . were carefully tailored to balance the interests of users, [Internet Service Providers], and rights holders."). However, this intent, as expressed in the safe harbor statutory language, needs further explanation.

137. This need for clarification has been addressed by the courts. *See, e.g.*, CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004) ("It is clear that Congress intended the DMCA's safe harbor for ISPs to be a floor, not a ceiling, of protection.").

138. *See, e.g.*, David E. Ashley, Note, *The Public As Creator and Infringer: Copyright Law Applied to the Creators of User-Generated Video Content*, 20 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 563, 574–75 (2010) (discussing extensive online copyright infringement via users despite pending litigation premised on such infringement).

tive deterrents to stop this infringing conduct.[139] Given the scale of copyright infringement in the digital medium,[140] the anonymity that the Internet provides,[141] and the ease of setting up new accounts,[142] simply terminating a user's account pursuant to a reasonably implemented § 512(i) policy is not a sufficient solution to adequately safeguard the rights of copyright holders. Further, the alternative remedy of a direct liability lawsuit against the infringer by the copyright holder proves equally unsatisfactory in many instances, especially when dealing with rampant infringement.[143] These lawsuits are often problematic due to the veil of secrecy provided by the Internet, which can escalate the violative behavior.[144] Additionally, if identity issues of the infringing parties do not arise, the costs of private litigation may be deemed economically unfeasible, as many offenders may be unable to pay any judgment for statutory damages entered against them.[145]

Consequently, it should be of little surprise that copyright holders are increasingly pursuing litigation against Internet and online service providers for user copyright infringement.[146] While direct liability suits against the perpetrators themselves make little sense given their low potential for return,[147] secondary liability lawsuits have a much greater chance for a

---

139. *See* Margaret H. Lemos & Alex Stein, *Strategic Enforcement*, 95 MINN. L. REV. 9, 51–53 (2010) (discussing the inadequacy of current controls in curbing user-generated copyright infringement).

140. *See* Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1349 (2004) (citing dramatic increases in online copyright infringement).

141. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222 (2006) (discussing the difficulty in identifying the parties who perpetrate bad acts via a cybermedium).

142. *See* Darrow & Ferrera, *supra* note 52, at 3–6 (discussing the ease in setting up new user accounts on most websites).

143. *See* Lemos & Stein, *supra* note 139, at 52–53 (describing copyright infringement as "largely undetectable" and asserting that "unscrupulous infringers of copyrighted works" take advantage of the weaknesses in the judicial system regarding enforcement and "exploit [this vulnerability] to its fullest by increasing the volume of their illicit activities.").

144. *See* Mtima, *supra* note 23, at 632 ("[T]here is no right to 'privately' break the law. Indeed, the fact that certain illegal conduct may be difficult to detect typically mandates that any pertinent privacy interests be specifically assessed against the possibility that lack of detection and concomitant legal redress may actually encourage the undesirable conduct.").

145. *See* Lynda J. Oswald, *International Issues in Secondary Liability for Intellectual Property Rights Infringement*, 45 AM. BUS. L.J. 247, 250 (2008) (discussing the "difficulty of identifying, locating, and suing each individual infringer [in direct liability copyright infringement suits for online behavior] . . . because the individual users are often judgment-proof and lack the financial resources to compensate for their infringement"). *But see* Levi Pulkkinen, *That "Free Song" Could End up Costing Thousands for Washingtonians Accused of Theft on the Net: Downloaders Face the Music Recording Industry's Focus Turns to Hunting Individuals*, SEATTLE POST-INTELLIGENCER, May 14, 2007, at A1 (discussing a recording industry strategy to sue individuals who have illegally obtained music online and who cannot afford attorneys as a way to force monetary settlements).

146. *See* Oswald, *supra* note 145, at 250 (discussing secondary liability lawsuits premised on user-generated infringement).

147. *See* Lemley & Reese, *supra* note 140, at 1349 ("The high volume of illegal uses, and the low return to suing any one individual, make it more cost-effective to aim litigation at targets as far up the chain as possible."); *see also* Martha Neil, *Music Downloader Ap-*

lucrative outcome.[148] So, while Internet and online service providers may view compliance with the threshold requirements of § 512(i) as a shield against DMCA safe harbor-related litigation and judgments for damages for copyright infringement,[149] the reality is that these defendants who are hailed into court still have to bear the brunt of a defense—both economically and reputationally[150]—despite such compliance and even if the ultimate ruling is a favorable one.[151]

A pragmatic perspective on these issues suggests that an alternative remedy would be useful to all stakeholders who are genuinely committed to reducing copyright infringement.[152] Although the infringement of these rights is not tantamount to terrorism,[153] the preservation of intellectual property rights has been a core part of American history[154] and jurisprudence.[155] Consequently, more must be done in order to continue to protect the important rights that copyright law grants to copyright holders. The DMCA should not be deemed a panacea for this type of Internet-tortious activity.[156] Instead, alternative solutions need to be explored in order to decrease the opportunities for the violation of copyright holders' rights in the online medium. Although it is unlikely that a single strategy can provide a cure-all,[157] more action needs to be taken by all of the parties who are involved in DMCA safe harbor-related litigation in furtherance of this goal of deterrence. In other words, "[c]opying

---

peals $67.5K Award, Calls It "Equally as Insane" as Earlier $675K Verdict, A.B.A. J. (Aug. 25, 2010, 5:16 PM), http://www.abajournal.com/news/article/music_downloader_appeals_67.5k_award_calls_it_equally_as_insane_as_earlier_/ (providing that a graduate student who was sued for unlawfully downloading copyrighted music would be required to file for bankruptcy if the $67,500 verdict is upheld on appeal).

148. *See* Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1384 (2010) (providing that Internet service "providers have deep pockets that greatly increase their vulnerability to lawsuits, making them scapegoats for their users' infringing activities").

149. *See, e.g.*, Joe Nocera, *Awaiting a Compromise on YouTube*, N.Y. TIMES, Mar. 17, 2007, at C1 Late Edition (quoting Google's chief executive as stating that "Google respects copyright" and that it complies with the DMCA).

150. *See, e.g.*, Andrew Morse, *Veoh Plans to Liquidate*, WALL ST. J., Feb. 12, 2010, at B6 (discussing the decision of Veoh to liquidate under bankruptcy protection due in part to "[t]he distraction of the legal battles"). Veoh was acquired by Qlipso in April 2010. *See About Veoh*, VEOH, http://www.veoh.com/corporate/aboutus (last visited Mar. 21, 2011).

151. *See* Nocera, *supra* note 149, at C1 (implying that certain copyright holders would like to "litigate YouTube off the face of the earth").

152. *See* Amanda Bronstad, *Hollywood Squares Off Against the Internet in the Second Circuit*, 244 N.Y. L.J., Dec. 16, 2010, at 5 (discussing the perspectives of several amicus brief filers in *Viacom* that both Internet service providers and copyright holders should be involved in deterring online copyright infringement).

153. *See* MARCUS BOON, IN PRAISE OF COPYING 101 (2010) ("[T]he most aggressive defenders of copyright law have done their best to link copyright breach to terrorism . . . .").

154. *See* U.S. CONST. art. I, § 8, cl. 8 (giving Congress the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and inventors the exclusive Right to their respective Writings and Discoveries").

155. *See, e.g.*, Reed Elsevier, Inc. v. Muchnick, 130 S. Ct. 1237, 1241 (2010) (framing the copyright discussion with the Copyright Clause of the United States Constitution).

156. *See, e.g.*, Ellison v. Robertson, 357 F.3d 1072, 1077 (9th Cir. 2004) ("[T]he DMCA did not simply rewrite copyright law for the on-line world.").

157. *See* Yu, *supra* note 148, at 1373 (exploring other potentially viable solutions to curb online copyright infringement via a "graduated response" strategy).

. . . is real enough, and we do not have the luxury of deciding whether we like it or not. The question . . . is how we handle it."[158]

Due to their control over the cyberforums that are at the center of DMCA safe harbor-related litigation, Internet and online service providers are actually in a unique position to help curb online copyright infringement without taking on the responsibility of increased monitoring beyond what the DMCA requires (or, to this point, has been construed to require). Further, to take advantage of this position (and explore all of the available avenues for deterrence) would reflect the professed ideology of many of these entities;[159] indeed, representatives of Internet and online service providers have publicly attested to a commitment to the protection of copyright.[160] For example, YouTube's founders have explained that "neither they nor YouTube [have] any interest in growing the company or profiting by virtue of the presence of materials on the service that infringed others' copyrights."[161]

Inarguably, Internet and online service providers already do employ a variety of methods and considerable resources to stop the use of their websites as conduits for infringing activity.[162] These methods include some user education through website guidelines, user verification through email addresses, and limited duration for content uploading.[163] However, regardless of these efforts, the frontline mechanism utilized by these entities as a means to protect copyright holders in accordance with stated ideology is compliance with the requirements of the DMCA.[164] This baseline minimum approach by service providers regarding deterrence of online copyright infringement needs conscientious revamping.

The argument advanced in this Article is that such a strategy should be sought through the utilization of stricter user agreements when persons want to access and post content to websites.[165] Specifically, this approach

158. BOON, *supra* note 153, at 234 (citing John Giorno, *Everyone Gets Lighter*, *in* SUBDUING DEMONS IN AMERICA: SELECTED POEMS, 1962–2007, 352–53 (2008)).

159. *See, e.g.*, *How to Report Claims of Intellectual Property Infringement*, FACEBOOK, http://www.facebook.com/legal/copyright.php (last visited Mar. 21, 2011) ("Facebook is committed to protecting the intellectual property of third parties.").

160. *See, e.g.*, *Berlusconi Media Firm Sues Google for Content on YouTube*, IRISH TIMES, July 31, 2008, at 11 (quoting a YouTube spokeswoman as stating "YouTube respects copyright holders and takes copyright issues very seriously").

161. Declaration of Zahavah Levine at 2, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010), (No. 1:07-cv-02103).

162. *See id.* (describing the millions of dollars and thousands of hours that many YouTube employees have expended "to minimize the incidence of unauthorized copyrighted material on the service, while ensuring that YouTube remained a vibrant platform for users around the world to share their own videos").

163. *See id.* at 2–5.

164. *See, e.g.*, *id.* at 2–11 (providing nineteen paragraphs of explanation on how YouTube complies with the provisions of the DMCA as opposed to six paragraphs on user education); *How to Report Claims of Intellectual Property Infringement*, *supra* note 159 (highlighting the DMCA notice and takedown procedures as the remedy for copyright infringement on the site).

165. Essentially, this strategy consists of an integrated approach to contract and intellectual property law, which has been proposed in other contexts as "intellectual property rights combine easily with contracts." Lorelei Ritchie, *Reconciling Contract Doctrine with*

could be accomplished through changes to the model of user agreements that would require more evidence of users' assent to the agreements and increased security measures for identity verification. Additionally, this approach would require the revision of current user agreements to include remedies for users' infringing conduct that are more stringent than the existing provisions on termination of user accounts pursuant to the DMCA. Further, this approach would require actual and open enforcement of the user agreement when there is a breach by a user in posting infringing content. Finally, these contractual changes and the enforcement of these provisions would need to be reflected in a comprehensive notice system to increase the transparency of Internet and online service providers' efforts to curb cyber-harms that are perpetrated via their services.

The adoption of this approach would be of substantial benefit to all parties who are affected by online copyright infringement—including Internet and online service providers.[166] Although this proposed strategy would require a sea change to the standard modes of Internet businesses,[167] it would be an effective and non-cost-prohibitive way to increase deterrence of online copyright infringement—a stated goal by many of these entities.[168] Further, service providers could incorporate the necessary changes in an almost instantaneous manner, given the breadth of the provisions within most extant user agreements[169] and the nature of the Internet itself.[170] The use of this approach would also help to transform the public perception that allocates blame to the online and Internet service providers as being "serial offender[s]" in the perpetration of digital copyright infringement.[171] Additionally, these good faith efforts could discourage potentially negative behavior on the part of copyright holders in stalling to report infringements.[172]

Intellectual Property Law: An Interdisciplinary Solution, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 105, 116 (2008–2009).

166. *See* Bronstad, *supra* note 152.

167. *See, e.g.*, Ty Tasker & Daryn Pakcyk, *Cyber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 79, 81 (2008) (discussing the variance in approaches to user agreements).

168. *See supra* text accompanying note 159.

169. *See, e.g.*, *Terms of Service: Community Guidelines*, YOUTUBE (June 9, 2010), http://www.youtube.com/t/terms ("YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions.").

170. *See, e.g.*, Leonard Bucklin, *More Preaching, Fewer Rules: A Process for the Corporate Lawyer's Maintenance of Corporate Ethics*, 35 OHIO N.U. L. REV. 887, 943 (2009) (discussing digital natives and their exposure to "the complexity and swift changes of information on the . . . [I]nternet").

171. *See, e.g.*, *Google Is 'Serial Offender,' Cleland Tells House Panel*, WASH. INTERNET DAILY, Sept. 17, 2010 (providing coverage of congressional testimony regarding Google and online copyright infringement).

172. *See, e.g.*, Gideon Parchomovsky & Alex Stein, *The Distortionary Effect Of Evidence on Primary Behavior*, 124 HARV. L. REV. 518, 541 (2010) (discussing how copyright law can "ha[ve] the obvious side effect of incentivizing intellectual property owners to generate evidence of continual infringement . . . [by] sit[ting] idly by and allow[ing] multiple infringements of their rights to occur").

Finally, Internet and online service providers should explore this alternative avenue for deterring online copyright infringement as a way to protect their own assets—regardless of whether they qualify for DMCA safe harbor protection. This strategy should be adopted as a way to insulate themselves from significant monetary liability in the case that a court finds noncompliance with § 512(i) provisions.[173] Of course, this strategy will also be beneficial when companies are in compliance with the DMCA. Essentially, if these contractual deterrents are an effective means to curb online copyright infringement (the root harm at issue in DMCA safe harbor related litigation), then these measures could commensurately curb the number of copyright infringement lawsuits that are filed against online service providers.[174] Given all of these factors, it is in the interest of Internet and online service providers to adopt such a pragmatic approach to reduce the number of claims and lawsuits that will undoubtedly continue to be filed by copyright holders as long as the infringing behavior has an outlet in an electronic forum.

III. DETERRENCE OF USER-GENERATED COPYRIGHT INFRINGEMENT THROUGH STRENGTHENED USER AGREEMENTS

If Internet and online service providers are truly invested in the prevention of online copyright infringement,[175] then additional measures are needed in contract formation, remedies, and enforcement within their user agreements.[176] Simply implementing a 17 U.S.C. § 512(i) account termination policy is not a sufficient means to deter infringing conduct.[177] Given the current requirements of most Internet and online service providers, there is no effective mechanism to stop a terminated account holder from simply reregistering an account with another email account

173. For example, in a recent federal district court case, the court declined to grant the defendants' motions for judgment as a matter of law and for a new trial after a jury awarded damages in the amount of $300,000 per defendant for contributory copyright infringement based on the jury finding that the defendants were not entitled to DMCA safe harbor protection. *See* Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., No. C 07-03952 JW, 2010 U.S. Dist. LEXIS 85266, at *2, *24–25, *53 (N.D. Cal. Mar. 19, 2010).

174. The potential reduction in copyright infringement lawsuits against online and Internet service providers is of considerable value, given the developing character of this area of law. *See, e.g.*, R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J.L. & ARTS 427, 443 (2009) (discussing the effect of the convergence of common law and statutory schemes of copyright infringement upon online service providers).

175. *See, e.g.*, *Veoh Copyright Policy*, VEOH, http://www.veoh.com/corporate/copyright (last visited on Mar. 21, 2011) ("Veoh takes copyright and other intellectual property rights very seriously.").

176. These user agreements may be labeled Terms of Service, Terms of Use, or other descriptions. *See* Tasker & Pakcyk, *supra* note 167, at 81 (discussing the various terminology employed by Internet and online service providers to describe user agreements). For consistency, the term "user agreements" will be utilized throughout this Part of the Article to describe the agreements that govern the relationships between Internet and online service providers and the users of their services.

177. *See* Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 270 (2006) (discussing the inadequacies of account termination policies).

and continuing this pattern of tortious activity.[178] Further, until the root harm of online copyright infringement is addressed by service providers, beyond threshold compliance with the DMCA safe harbor requirements, these entities will face continued possibilities for protracted litigation, exposing themselves to negative publicity and potential liability.[179]

The suggested revisions that are addressed in this Part of the Article would be a step forward in reducing the malignant, infringing conduct by website users that harms both copyright content owners and service providers. This Part advocates for a tripartite strategy to strengthen user agreements as a way to deter online copyright infringement, with reform needed in the main areas of contract formation, drafting, and enforcement. Specifically, this approach will advocate for (1) increased mechanisms to evidence assent by the user to the user agreement; (2) additional security measures for identity verification in account creation; (3) clearer provisions on account termination; (4) the inclusion of liquidated damages clauses; (5) the open enforcement of current indemnification provisions and other remedial provisions; and (6) increased marketing of these efforts.

This proposed strategy can be an effective way to help to curb online copyright infringement, as well as the DMCA safe harbor-related litigation that is premised on the propagation of this primary infringement.[180] Further, it can help ensure the continued viability of lawful content sharing,[181] an important component of the digital marketplace of ideas and Internet freedom. Finally, it is a strategy that can be quickly adopted and implemented by Internet and online service providers, given the fluid nature of the Internet.[182]

The Internet provides the perfect arena for swift changes like those proposed in this Article. For example, eBay has modified its user agreement to more accurately reflect the nature of the transfer of title pursuant to Uniform Commercial Code § 2-401(2) and California's codification of

178. *See id.* ("OSPs . . . might also terminate free home page accounts for any number of reasons, including outsiders' claims of copyright infringement, but little prevents a subscriber so terminated from simply establishing a new free account with the same OSP.").

179. *See, e.g.*, Don Jeffrey, *Viacom Appeals YouTube Copyright-Infringement Ruling*, BLOOMBERG (Aug. 11, 2010, 3:29 PM), http://www.bloomberg.com/news/2010-08-11/viacom-appeals-youtube-copyright-infringement-ruling.html (discussing the lengthy timeline of the case and the drop in share prices for both Google and Viacom).

180. This approach would seemingly satisfy the claim of content holders that the DMCA is "a law intended to provide safe harbor against liability where online services providers take reasonable steps to prevent infringement." *Viacom Statements: Viacom Files Brief with U.S. Court of Appeals*, VIACOM (Dec. 3, 2010), http://news.viacom.com/news/Pages/statements-viacom-files-brief.aspx.

181. *See, e.g.*, Brian Heater, *Viacom vs. Google: The Battle for YouTube*, PCMAG (Mar. 22, 2010), http://www.pcmag.com/article2/0,2817,2361617,00.asp (describing how successful DMCA safe harbor-related litigation on the part of copyright holders may lead to the demise of lawful content sharing).

182. *See* Adrian Vermeule, *Congress and the Costs of Information: A Response to Jane Schacter*, 89 B.U. L. REV. 677, 687 (2009) ("Internet technology is seemingly more fluid now than printing technology was in its era.").

these relevant sections.[183] Specifically, these provisions provide different times for passage of title in sales contracts depending upon the nature of the contract as a place of shipment or place of destination contract.[184] For the former, "title passes to the buyer at the time and place of shipment."[185] For the latter, "title passes on tender" at the place of destination.[186] However, in the eBay user agreement that became effective on August 13, 2008, the following language was provided regarding transfer of title:

> We do not transfer legal ownership of items from the seller to the buyer, and nothing in this agreement shall modify the governing provisions of California Commercial Code § 2401(2) and Uniform Commercial Code § 2-401(2), under which legal ownership of an item is transferred upon physical delivery of the item to the buyer by the seller. Unless the buyer and the seller agree otherwise, the buyer will become the item's lawful owner upon physical receipt of the item from the seller, in accordance with California Commercial Code § 2401(2) and Uniform Commercial Code § 2-401(2).[187]

The current eBay user agreement has been modified, with respect to its discussion of the governing law: "We do not transfer legal ownership of items from the seller to the buyer. California Commercial Code § 2401(2) and Uniform Commercial Code § 2-401(2) applies to the transfer of ownership between the buyer and the seller, unless the buyer and the seller agree otherwise."[188]

eBay is not the only online service provider to revise its user agreement or revamp its account creation process.[189] For example, an Internet Archive[190] search of Veoh, an online service provider that has been the subject of several DMCA safe harbor-related lawsuits,[191] demonstrated a

183. The eBay user agreement is governed by California law. *See Your User Agreement*, EBAY (Sept. 7, 2010), http://pages.ebay.com/help/policies/user-agreement.html.

184. *See* CAL. COM. CODE § 2401(2) (West 2002) ("Unless otherwise explicitly agreed title passes to the buyer at the time and place at which the seller completes his performance with reference to the physical delivery of the goods.").

185. *Id.* § 2402(2)(a).

186. *Id.* § 2402(2)(b).

187. *Your User Agreement*, EBAY (Aug. 13, 2008) (on file with author).

188. *Your User Agreement*, *supra* note 183.

189. *Compare* Declaration of Zahavah Levine at Ex. 2, Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103) (providing copies of the YouTube user agreements from December 2005 and January 2007), *with Terms of Service: Community Guidelines*, *supra* note 169 (showing some revisions from previous YouTube user agreements). An Internet Archive search was attempted to locate a screenshot of the YouTube account creation screen to determine if changes had been made to this process. However, access to the archived website for YouTube sign-up "has been blocked by the site owner." *See Internet Archive Wayback Machine*, INTERNET ARCHIVE, http://web.archive.org/web/20050428171556/http://www.youtube.com/signup.php (last visited Jan. 7, 2011).

190. *See* INTERNET ARCHIVE, http://www.archive.org/ (last visited Jan. 6, 2011) ("The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.").

191. *See supra* text accompanying notes 101–126.

much simpler account registration process on January 10, 2008, as opposed to its current registration process.[192] In fact, most of the user agreements utilized by Internet and online service providers expressly incorporate change of terms clauses that allow for such modification.[193] This characteristic of the user agreements, coupled with the fluidity of the Internet, makes the solution advanced in this Article, which requires changes to contract formation, drafting, and enforcement, viable and easily accomplishable.

A. CONTRACT FORMATION AND ACCOUNT CREATION

Generally, the websites that provide their users the opportunity to upload content, which creates the potential for online copyright infringement, utilize acceptance of user agreements as a part of the account creation process to govern the relationship between the Internet or online service provider and the user.[194] In addition to acceptance of the user agreement, account creation also typically requires the user to provide basic identification information, such as a first and last name, email address, account password, gender, and birthdate.[195] Both of these prongs of account creation should be the focus of reformation, on the part of Internet and online service providers, in an effort to curb user-generated copyright infringement and subsequent DMCA safe harbor-related litigation. Specifically, they should revise their business practices to include (1) increased mechanisms to evidence assent to the user agreement by the user who can post potentially infringing content to the website and (2) additional security measures for identity verification in account creation.

---

192. As of January 2011, Veoh's registration process requires a username, email address, password, country, gender, and birthdate. *See Create a New Veoh Account*, VEOH, http://www.veoh.com/register (last visited Jan. 15, 2011). In January 2008, only a username, email, and password were required. *See Veoh Log-in*, VEOH, http://web.archive.org/web/20071011030836rn_1/www.veoh.com/login.html?redir=1&noAction=1 (last visited Jan. 6, 2011).

193. *See, e.g.*, *Craigslist Terms of Use*, CRAIGSLIST, http://www.craigslist.org/about/terms.of.use (last visited Jan. 15, 2011) ("We reserve the right, at our sole discretion, to change, modify or otherwise alter these terms and conditions at any time. Such modifications shall become effective immediately upon the posting thereof. You must review this agreement on a regular basis to keep yourself apprised of any changes. You can find the most recent version of the TOU at: http://www.craigslist.org/about/terms.of.use.html"); *Terms of Service: Community Guidelines*, *supra* note 169 ("Although we may attempt to notify you when major changes are made to these Terms of Service, you should periodically review the most up-to-date version http://www.youtube.com/t/terms. YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions.").

194. *See, e.g.*, *Hi! Ready to Register with eBay?*, EBAY, https://scgi.eBay.com/ws/eBayISAPI.dll?RegisterEnterInfo (last visited Jan. 15, 2011) (requiring acceptance of the user agreement via a clickable icon to create an account); *Get Started with Your Account*, YOUTUBE, http://www.youtube.com/create_account?feature=idx_promo_std&next= (last visited Jan. 15, 2011) (conditioning account creation on acceptance of the Google Terms of Service and the YouTube Terms of Use).

195. *See, e.g.*, FACEBOOK, http://www.facebook.com/ (last visited Jan. 15, 2011); *Create a New Veoh Account*, *supra* note 192.

The user agreements utilized by Internet and online service providers that are most susceptible to DMCA safe harbor-related litigation are primarily browsewrap and clickwrap agreements.[196] Over the last decade, the area of jurisprudence involving these user agreements has developed rapidly.[197] Electronic standard form contracts are categorized by the type of assent that is required by the user of the website.[198] Mutual assent is an essential component of contract formation.[199] Due to the differences in the natures of browsewrap and clickwrap agreements,[200] courts have found varying levels of valid contract formation and enforceability between these two forms of user agreements.[201] Although user agreements are not treated uniformly by the courts, they share a predominant similarity in that most users never read them.[202] This characteristic is a typical one for standard form contracts, whether they are traditional

196. *See* Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 366 (E.D.N.Y. 2009) (providing that the primary forms for Internet contracting are browsewrap and clickwrap agreements); *see, e.g.*, *MySpace.com Terms of Use Agreement*, MYSPACE (June 25, 2009), http://www.myspace.com/help/terms (providing an example of a browsewrap and clickwrap user agreement with the following provisions: "By accessing and/or using the MySpace Services, you agree to be bound by this Agreement, whether you are a 'Visitor' (which means that you simply browse the MySpace Services, including, without limitation, through a mobile or other wireless device, or otherwise use the MySpace Services without being registered) or you are a 'Member' (which means that you have registered with MySpace). The term 'User' refers to a Visitor or a Member."). In order to create a MySpace account, an individual must click a button that is labeled "Sign up free." *See Sign up in Less Than 60 Seconds*, MYSPACE, https://www.myspace.com/signup (last visited Jan. 15, 2011). Above this button is the following language: "By clicking Sign up free, you agree to Myspace terms of service and privacy policy." *See id.*

197. *See* Tasker & Pakcyk, *supra* note 167, at 82 (stating that in the early 2000s, "the development of a body of applicable case law [regarding the enforceability of online user agreements] is in its infancy, with very few published rulings on point before the year 2000, and the availability of such authorities did not become substantial until around 2003"). *See also* Juliet M. Moringiello & William L. Reynolds, *Survey of the Law of Cyberspace: Electronic Contracting Cases 2007–2008*, 64 BUS. LAW. 199, 218 (2008) (claiming the maturity of the law of Internet contracts).

198. *See* Juliet M. Moringiello & William L. Reynolds, *Electronic Contracting Cases, 2009–2010*, 66 BUS. LAW. 175, 176 (2010) (discussing the differences between browsewrap and clickwrap agreements for standard form electronic contracts).

199. *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 464–65 (2006) (discussing the fundamental nature of assent in contracting and how this element gives contracts legitimacy).

200. Although most courts apply a different analysis for what they deem to be browsewrap and clickwrap agreements, some courts have "recognized that whether terms are presented as clickwrap terms or browsewrap terms has no bearing on enforceability; rather, the relevant inquiry is whether the terms were reasonably communicated to the website user." Moringiello & Reynolds, *supra* note 198, at 178.

201. *See generally* Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405 (2010) (discussing enforceability of browsewrap and clickwrap agreements); Mo Zhang, *Contractual Choice of Law in Contracts of Adhesion and Party Autonomy*, 41 AKRON L. REV. 123, 173 (2008) (discussing judicial treatment of these agreements).

202. *See* Lydia Pallas Loren, *Slaying the Leather-Winged Demons in the Night: Reforming Copyright Owner Contracting with Clickwrap Misuse*, 30 OHIO N.U. L. REV. 495, 503 (2004) (stating that it is "common knowledge that the vast majority of individuals do not, in fact, read the shrinkwrap and clickwrap agreements").

or online agreements.[203]

Although browsewrap agreements appear online in many different forms, they generally bind the user to the agreement based on the mere use or browsing of the website or online services.[204] Consequently, browsewrap agreements do not require any type of express manifestation of assent to the agreement.[205] Instead, assent is premised on use of the website or services alone.[206] The terms of browsewrap user agreements are typically accessible via a hyperlink on the homepage.[207] Although some courts have upheld the formation and enforceability of browsewrap agreements,[208] other courts have refused to do so.[209] Despite the ultimate holding, when faced with the question of formation and enforceability of browsewrap agreements, the majority of courts focus on the issue of notice to the user[210]—specifically, "whether the website user 'has actual or constructive knowledge of a site's terms and conditions prior to using the site.'"[211]

Due to the nature of browsewrap agreements, which claim acceptance of their terms premised on mere use, most websites that allow users to upload content require the creation of an account via acceptance of a clickwrap agreement.[212] As opposed to browsewrap agreements, click-

203. *See* Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1313 (2005) (noting that few people read standard form contracts); Nishanth V. Chari, Note, *Disciplining Standard Form Contract Terms Through Online Information Flows: An Empirical Study*, 85 N.Y.U. L. REV. 1618, 1626 (2010) (stating that "[Law and Economics] scholars generally agree that most buyers do not read SFCs at the time of purchase").

204. *See* United States v. Drew, 259 F.R.D. 449, 462 n.22 (C.D. Cal. 2009) ("Browsewraps can take various forms but basically the website will contain a notice that-by merely using the services of, obtaining information from, or initiating applications within the website-the user is agreeing to and is bound by the site's terms of service.").

205. *See* Sw. Airlines Co. v. BoardFirst, L.L.C., No. 3:06-CV-0891-B, 2007 WL 4823761, at *4 (N.D. Tex. Sept. 12, 2007) ("A defining feature of a browsewrap license is that it does not require the user to manifest assent to the terms and conditions expressly-the user need not sign a document or click on an 'accept' or 'I agree' button.").

206. *See id.* ("A party instead gives his [or her] assent simply by using the website.").

207. *See, e.g.*, *Terms of Use*, VEOH (Jan. 21, 2009), http://www.veoh.com/corporate/termsofuse (The following sample of a browsewrap agreement can be accessed by a hyperlink from the website's main page: "By accessing or using the Veoh Service, you ('You' or 'Your' as applicable) are bound by the notices, terms and conditions in these TOU and, as applicable, elsewhere on www.veoh.com (including but not limited to our Privacy Policy and Copyright Policy, which are incorporated by reference).").

208. *See, e.g.*, *Sw. Airlines Co.*, 2007 WL 4823761, at *5 (upholding the enforceability of a browsewrap agreement).

209. *See, e.g.*, Specht v. Netscape Comms. Corp., 306 F.3d 17, 31–32 (2d Cir. 2002) (refusing to enforce a browsewrap agreement where the terms of the agreement were only available on a scroll-down through another screen apart from the screen where a download was offered via a click of a button).

210. *See* Moringiello & Reynolds, *supra* note 198, at 178–79 (discussing the contractual idea of notice as the essential inquiry for assent in contract formation in browsewrap enforceability cases).

211. Snap-on Bus. Solutions Inc. v. O'Neil & Assocs., Inc., 708 F. Supp. 2d 669, 681 (N.D. Ohio 2010) (quoting *Sw. Airlines Co.*, 2007 WL 4823761, at *5).

212. *See, e.g.*, *Create a New Veoh Account*, *supra* note 192 (requiring account creation via acceptance of a clickwrap agreement, as evidenced by clicking a "Sign up" icon which demonstrates the user's agreement to the hyperlinked Terms of Service, in order to

wrap agreements require an express manifestation of assent to the agreement by affirmatively clicking on a box or icon designating such agreement.[213] Some of these clickwrap agreements will feature the user agreement via a hyperlink next to the clickable icon,[214] while others will feature a scroll-through textbox on the same page as the clickable icon.[215] Courts have routinely upheld the formation and enforceability of clickwrap agreements,[216] including situations involving online and Internet service providers that allow users to upload content.[217]

Despite the judicial trend of increasing enforcement of clickwrap agreements,[218] Internet and online service providers should introduce increased mechanisms to evidence assent to the user agreement by the user who can post potentially infringing content to the website. In order to deter online copyright infringement effectively, more is needed from these entities than baseline compliance with the DMCA or with what has been upheld as sufficient evidence of assent for a finding of an enforceable user agreement by past courts. Essentially, more is needed than just a clickable icon with a hyperlink to the user agreement on the account creation page[219] for Internet and online service providers to truly respect

---

"upload videos of any run length"). *See also Terms of Use*, *supra* note 207 ("Registration is not required to view most User and Video Content provided as part of the Veoh Service. However, You are required to register if You wish to post a comment or upload a video, download the Veoh Client or view certain User Material and Video Content.")

213. *See* United States v. Drew, 259 F.R.D. 449, 462 n.22 (C.D. Cal. 2009) ("Clickwrap agreements require a user to affirmatively click a box on the website acknowledging awareness of an agreement to the terms of service before he or she is allowed to proceed with further utilization of the website."); Moringiello & Reynolds, *supra* note 198, at 176 (discussing the express manifestation of assent that is tied to clickwrap agreements). *See, e.g.*, *Hi! Ready to Register with eBay?*, *supra* note 194 (requiring users to click a box that signifies that "I agree that: I accept the User Agreement and Privacy Policy" for account creation).

214. *See id.* (featuring hyperlinks to the User Agreement and Privacy Policy, underneath the clickable box of acceptance of the agreement).

215. *See, e.g.*, *Get Started with Your Account*, *supra* note 194 (providing a scroll-through textbox of the Google Terms of Service and the YouTube Terms of Use on the same page as the clickable icon, "I accept" box, as well as hyperlinks in the following language that precedes the clickable icon: "By clicking 'I accept' below you are agreeing to the YouTube Terms of Use, Google Terms of Service and Privacy Policy.").

216. *See* Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513, at *2–3 (E.D. Mo. Mar. 6, 2009) (noting that district and circuit courts routinely uphold the enforceability of clickwrap agreements and finding that the clickwrap agreement at issue in the case was enforceable).

217. *See, e.g.*, Riggs v. MySpace, Inc., No. 3:2008-247, 2009 WL 1203365, at *1–5 (W.D. Pa. May 1, 2009) (enforcing the MySpace clickwrap agreement); Feldman v. Google, Inc., 513 F. Supp. 2d 229, 235 (E.D. Pa. 2007) (finding the enforceability of Google's clickwrap agreement).

218. *See* Abruzzi, *supra* note 18, at 112 ("A user's click-through is usually adequate to establish that the user and the website proprietor formed a 'contract' that incorporates the terms of use.").

219. *See* Francis J. Mootz III, *After the Battle of the Forms: Commercial Contracting in the Electronic Age*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 271, 284 (discussing the favorable treatment by courts of pure clickwrap contracts that present a clickable icon with a hyperlink to the user agreement).

copyright.[220]

Internet and online service providers have a variety of options that can be used to implement an approach of increased mechanisms to evidence assent to user agreements. At a minimum, these providers should incorporate a scroll-through textbox that includes the entire user agreement on the account creation screen with a clickable icon that cannot be clicked until the user completely scrolls through the entire document.[221] A much better mechanism, which would especially fit with the services provided by a website that allows users to upload content, would be the requirement that each user view a video reading, with subtitles, of the user agreement in its entirety before having the ability to click on an icon that represents agreement with the terms. To further improve this approach, user agreements should be revised into plain language—as most of these agreements are overly lengthy documents,[222] which tends to discourage users from actually reading them.[223] In the video presentation, the copyright provisions of the user agreement should be explained in clear, direct language. These provisions should include a discussion of the notice and takedown procedure as it protects the rights of copyright holders;[224] the counter-notification and replacement of removed material procedure as it protects the rights of the user against abusive takedown notices and allegations of repeat infringement;[225] and the account termination procedure for repeat infringers as it protects the rights of the Internet and online service providers to be entitled to DMCA safe harbor status.[226]

Additionally, entities that allow users to upload content on their website should implement an actual, or "knowing,"[227] assent mechanism to

220. *See, e.g.*, *Metacafe: Usage Rules*, METACAFE, http://wikicafe.metacafe.com/en/Metacafe:Usage_Rules (last visited Jan. 15, 2011) ("Metacafe respects the intellectual property rights of others, and requests you to do the same.").

221. Some websites' account creation pages already do feature a scroll-through textbox with the user agreement contained therein. *See, e.g.*, *Get Started with Your Account*, *supra* note 194.

222. For example, to create a YouTube account, a user must agree to the YouTube Terms of Use, the YouTube Privacy Policy, the Google Terms of Service, and the YouTube Community Guidelines. *See id.* Together, these user agreements and policies are over 10,000 words long. *See Google Terms of Service*, GOOGLE (Apr. 16, 2007), https://www.google.com/accounts/TOS?loc=US&hl=en; *Terms of Service: Community Guidelines*, *supra* note 169; *YouTube Community Guidelines*, YOUTUBE, http://www.youtube.com/t/community_guidelines (last visited Jan. 15, 2011); *YouTube Privacy Policy Notice*, YOUTUBE (Dec. 8, 2010), http://www.youtube.com/t/privacy.

223. *See* Michael I. Meyerson, *The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 U. MIAMI L. REV. 1263, 1269–70 (1993) ("[C]onsumers do not read form contracts both because it is unreasonable to do so and because businesses do not want consumers to read them prior to signing.").

224. *See* 17 U.S.C. §§ 512(c)(2), (3) (2006) (providing the DMCA requirements for a valid notice and takedown procedure).

225. *See id.* § 512(g) (2006) (providing the DMCA requirements for counternotification and replacement of removed materials).

226. *See id.* § 512(i) (2006) (providing the DMCA requirements for a valid account termination policy for repeat infringers).

227. *See* Edith R. Warkentine, *Beyond Unconscionability: The Case for Using "Knowing Assent" As the Basis for Analyzing Unbargained-for Terms in Standard Form Con-*

demonstrate explicit agreement with the copyright provisions within the user agreement (through the incorporation of an "I agree" clickable icon or an "I do not agree" clickable icon for the specific provisions dealing with intellectual property).[228] Finally, Internet and online service providers should require users to answer a short series of questions regarding the user agreement correctly prior to the conclusion of account creation in order to evidence awareness and understanding of the contract that is being formed.

The incorporation of these types of mechanisms would bolster a showing of manifestation of assent to the user agreement (and specifically to the copyright provisions contained within it). As such, it would demonstrate the willingness of Internet and online service providers to take proactive steps towards the deterrence of online copyright infringement—steps above the floor of requirements for assent that most courts now find.[229] Additionally, it would streamline the process of clickwrap agreement formation by providing the most basic terms in a consumer-friendly presentation.[230] Further, it would provide a solid foundation to refute any type of assertion of inadvertent or mistaken clicking on the part of the user.[231] The mechanisms also would provide evidence of user culpability when that user chooses to violate the user agreement by posting infringing content after being required to respond to these increased assent measures in account creation. Essentially these mechanisms, if adopted, would concretely demonstrate how the copyright provisions were bargained-for sections of the user agreement.[232]

---

tracts, 31 SEATTLE U. L. REV. 469, 473 (2008) ("Knowing assent requires the following: (1) that the unbargained-for term be conspicuous; (2) that the importance of that term be explained so that the adhering party understands its significance; and (3) that the adhering party objectively manifests its assent to that term separately from its manifestation of assent to undertaking a contractual obligation.").

228. *See* Nancy S. Kim, *Clicking and Cringing*, 86 OR. L. REV. 797, 803 (2007) (advocating for actual assent for specific provisions in software licensing agreements).

229. *See, e.g.*, Lemley, *supra* note 199, at 465 ("But in today's electronic environment, the requirement of assent has withered away to the point where a majority of courts now reject any requirement that a party take any action at all demonstrating agreement to or even awareness of terms in order to be bound by those terms.").

230. *See* Kim, *supra* note 228, at 829–30 ("Contract drafters faced with the requirement of calling out affirmative obligation provisions will either modify their contracts if the provision is considered important enough (i.e., if it is part of what is being bargained for), or they will drop the provision as unnecessary, thus streamlining and facilitating the contracting process. . . . Currently, the overwhelming verbiage presented in form agreements makes it difficult to distinguish innocuous provisions from those requiring more scrutiny and contemplation.").

231. *See* Tasker & Pakcyk, *supra* note 167, at 116 (discussing the possibility that "computer users may have indicated their assent, or acceptance of particular terms, by inadvertence, such as by a premature click on a form submission button").

232. *See* Kim, *supra* note 228, at 830 ("A requirement of manifestation of consent to an affirmative obligation term attracts the consumer's attention and requires the consumer to consider whether the proposed transaction in fact is what she or he had bargained for. . . . The consumer faced with such a decision may not be enthusiastic about the available options, but at least he or she is made aware of the consequences of engaging in the transaction. The act of assenting forces the consumer to acknowledge the existence of a particular term.").

In addition to adopting these revised systems to evidence user assent, Internet and online service providers should implement additional security measures for identity verification in account creation. Although some of these providers require the provision of detailed information in the account creation process,[233] others still only require minimal information, like a username, password, and email address, to create an account.[234] Because of the vast differences in the requirements of email account creation[235] and because of the availability of public computers in the United States that would not tie users to a specific IP address,[236] Internet and online service providers that require only minimal information will have few or no means to identify the user who chooses to infringe upon others' intellectual property rights.

In order for strengthened user agreements to effectively deter online copyright infringement, these entities should implement additional security measures for identity verification in account creation. Like the needed reforms regarding user assent, these changes are not a requirement in order to claim safe harbor under the DMCA.[237] Indeed, the subpoena provisions of the DMCA regarding the responsibilities of Internet and online service providers to respond to subpoenas to identify infringers illustrate this very notion.[238] However, improving identity verification is a vital part of the strategy for service providers to take proactive

233. *See, e.g.*, *Hi! Ready to Register with eBay*, *supra* note 194 (requiring a name, street address, telephone number, email address, date of birth, user name, password, and entry of a verification code, as well as acceptance of the user agreement via clickable icon, in order to create an account).

234. *See, e.g.*, *Sign up for a Personal Account*, VIDDLER, http://www.viddler.com/signup/personal/ (last visited Jan. 15, 2011) (requiring a username, password, and email address, along with acceptance of the user agreement via clickable icon, to create an account that allows a user to upload video content to the website).

235. *Compare Create an Account*, GMAIL, https://www.google.com/accounts/NewAccount?service=mail&continue=http://mail.google.com/mail/e-11-1c5fae25d43bf12b3ad7503 13d8e96-8eada2b39a294aae9e0182c56e3d42cbfbc7e9c5&type=2 (last visited Jan. 15, 2011) (requiring a full name, username, password, optional alternate email address, country location, birthday, word verification, and acceptance of terms of service via clickable icon to create an account), *with New Secure Email Account*, HUSHMAIL, https://www.hushmail.com/signup/ (last visited Jan. 15, 2011) (requiring only the requested email address, password, number verification, and acceptance of the user and security agreements via clickable icons to create an account).

236. Courts in DMCA safe harbor-related lawsuits have rejected the idea that an IP address will always provide a valid identification of an infringing user. *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008) ("There is no material dispute that, while IP addresses identify a particular computer connected to the Internet, they do not distinguish between users (e.g., family members) who may share the same computer.").

237. *See id.* (finding that "tracking (or verifying) users' actual identity or . . . blocking their IP addresses" is not a requirement of a § 512(i) account termination policy under the DMCA).

238. *See* 17 U.S.C. § 512(h)(3) (2006) ("The subpoena [to identify the infringer] shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.").

steps to deter user-generated copyright infringement and subsequent DMCA safe harbor-related litigation.

A continuum of possibilities is present with respect to additional security measures for identity verification. As a baseline minimum, Internet and online service providers should require users to provide a full name, physical address, email address, date of birth, user name, password, and entry of a verification code (in addition to the increased assent acceptance of the user agreement) in order to create an account that allows uploading user content.[239] In order to curb the use of their services by individuals who provide false information, providers should also require the user to respond online to a physical mailing that contains a security code, thereby making the early period of account creation conditional upon this response. During this time, users should not have the ability to upload content. This would be a precautionary measure to aid in identity verification for the purposes of copyright infringement deterrence.

Alternatively, Internet and online service providers should consider the implementation of an account creation requirement of a verified credit card or PayPal account that is linked to a bank account for those users who wish to have the ability to upload content.[240] This would allow for the introduction of a sliding-scale-tiered system, which would remain free for most users but require more identity verification measures for those users who want more access. Such a mechanism would help to balance the important ideals of Internet freedom and access[241] with the protection of intellectual property by taking away the veil of anonymity that currently protects many infringing users.[242]

Admittedly, some of the suggested reform mechanisms with respect to identity verification will require more effort and expenditure by these

239. A few providers require this level of detail. *See supra* text accompanying note 233. However, most providers do not require this amount of information in order to create an account. *See, e.g.*, *Create Your Metacafe Account*, METACAFE, https://secure.metacafe.com/account/login/?token=a289b0b09985b0347a1eca8bcaa3cbb7&action=register (last visited Jan. 15, 2011) (requiring an email address, nickname, password, birthdate, postal code, and acceptance of user agreement via clickable icon to create an account).

240. Multiple state officials have requested that Internet and online service providers require this type of information as part of the account registration process in an effort to protect minors from unlawful conduct that results from online use. *See, e.g.*, Notice of Removal, Tab F, Exs. B & D, Doe v. MySpace, Inc., 629 F. Supp. 2d 663 (E.D. Tex. 2008) (No. 4:08-CV-00140) (providing letters from the Ohio and Texas Attorney Generals requesting that MySpace and other online service providers require the entry of a verifiable credit card or bank account information in order to set up accounts as an effort to prevent the abuse and exploitation of minors).

241. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 851–53 (1997) (discussing the vast advantages of Internet access).

242. Interestingly, a review of the user agreements and policies of certain online service providers reveals that at least one of these entities may be considering the implementation of such measures. *See, e.g.*, *Privacy Policy*, MYSPACE (Dec. 7, 2010), http://www.myspace.com/Help/Privacy (discussing how MySpace, which does not currently require credit card information for account creation, can use personal information, including credit card information, obtained during the registration process).

providers.[243] However, many technology experts are already calling for these types of redesigns.[244] By taking these proactive steps, Internet and online service providers can demonstrate their ability to innovate in the competitive marketplace. Indeed, making voluntary changes to the existing business model for formation of most user agreements (as opposed to a court-ordered or case-driven change) will require a significant shift in the practices of most Internet and online service providers.[245] This is especially the case given that most courts find user assent to, and valid formation of, clickwrap agreements[246] despite the fact that most users do not read them.[247] However, if industry leaders voluntarily incorporate these changes, then it is likely that other entities that are prone to DMCA safe harbor-related litigation will follow suit.[248] Because the Internet allows for such swift changes, modifying user agreement and identity verification policies would be a cost-efficient and relatively easy reformation to the account creation and contract formation processes between Internet and online service providers and their users.

Consequently, Internet and online service providers should make strides towards a more uniform approach to account creation and contract formation for those users who have the ability to upload content to their websites.[249] Just as threshold compliance with the DMCA is not enough to provide a significant deterrent to online copyright infringe-

243. Of course, all of these measures would be unnecessary if use of the Internet required registration with an independent identity verification service. *See* Scott Ness, *The Anonymous Poster: How to Protect Internet Users' Privacy and Prevent Abuse*, 2010 DUKE L. & TECH. REV. 8, 52–56 (2010) (advocating for the creation of a mandatory, independent identity verification system for Internet use). However, the creation of such an innovation seems to be unlikely in the near future.

244. *See, e.g.*, Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 706 (2010) (discussing how leading technologists are advocating for the redesign of the Internet to improve security and identity verification).

245. *See, e.g.*, David F. Scranton, *"Clickwrap" or "Browsewrap": Enforceable Website Agreements*, 119 BANKING L.J. 290, 291 (2002) (advocating, after a court refused to enforce a browsewrap agreement, that "financial institutions should [promptly reevaluate] their Web sites to be sure that any terms, conditions or agreements that are intended to be binding upon a visitor are implemented with a 'click-through' type mechanism to verify that the visitor is aware of them and agrees to them").

246. *See* Hartzog, *supra* note 201, at 433 (describing courts as "almost uniformly enforc[ing] clickwrap agreements" as validly formed contracts).

247. *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 33 (2009) (stating that judicial decisions on clickwrap agreements typically "[echo] the long-held acknowledgement that consumers generally do not read form contracts, yet are still bound to the terms of the agreement").

248. *See* Chari, *supra* note 203, at 1619–20 (providing this summary of the dominant position of Law and Economics scholars: "'To what extent will firms include the most onerous possible clauses [in standard form contracts]?' Scholarly responses to this question have taken various shapes, but the dominant position today is . . . 'Only so far as competitive pressures fail to discipline firms into offering fair and efficient clauses.'").

249. Most reviews of user agreements denote significant differences and a general lack of uniformity. *See* Sharon K. Sandeen, *The Sense and Nonsense of Web Site Terms of Use Agreements*, 26 HAMLINE L. REV. 499, 501–02 (2003) (discussing the differences between user agreements).

ment,[250] Internet and online service providers' current practice of meeting the minimum requirements for formation and enforceability of their clickwrap agreements does not sufficiently address the problem of users misusing these services to infringe upon the intellectual property rights of others. Implementing increased mechanisms to evidence user assent, along with additional security measures to verify the identity of users in the account creation process, will reaffirm the good faith of Internet and online service providers and their commitment to the protection of copyright. Further, this reformation in contract formation is a necessary prerequisite for the remaining two prongs of the strategy advanced in this Article, which include revisions to the practices of contract drafting and enforcement. Together, these three prongs carry the potential to decrease online copyright infringement, which would commensurately curb DMCA safe harbor-related litigation.

B. Contract Drafting: DMCA Account Termination Policies and Other Remedial Provisions in User Agreements

The suggested revisions for modification in the formation of user agreements are steps in the right direction for Internet and online service providers who want to show a good faith effort towards minimizing online copyright infringement. However, these entities should also examine their current drafting practices for these types of contracts and should consider making revisions to these practices to combat illegal conduct. Changes to the drafting process, specifically through the use of clearer provisions on account termination for infringing activity and through the inclusion of liquidated damages clauses, are an important part of an integrated strategy that service providers should use to stop the tortious activity that may take place through their forums (as well as limiting the type of litigation and negative publicity that is premised upon this type of activity). The success of these changes depends upon an adherence to the plain language approach that was mentioned in Part III.A of this Article.[251] With the increased mechanisms for assent and identity verification in place, these revised drafting provisions will be much more effective when enforced by the providers.

Most user agreements currently employ language regarding account termination that is reflective of the DMCA's requirements for such policies.[252] Unfortunately, many of the key terms of § 512(i) are not defined,

250. *See* Bridy, *supra* note 22, at 83 (discussing how past efforts to curb online copyright infringement have not "made much of a dent" in the tortious behavior).

251. *See supra* Part III.A.

252. *Compare* 17 U.S.C. § 512(i)(1)(A) (2006) ("The limitations on liability established by this section shall apply to a service provider only if the service provider has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."), *with Facebook Statement of Rights and Responsibilities*, Facebook (Oct. 4, 2010), http://www.facebook.com/terms.php?ref=pf ("If you repeatedly infringe other people's intellectual property rights, we will disable your account when ap-

and without these definitions there is almost no clear statutory direction regarding the requirements of these account termination policies.[253] Further, the litigation that has involved the DMCA account termination policies has not provided much more clarity beyond the fact that implementation of such a policy is a threshold condition for safe harbor status.[254] As a result, most Internet and online service providers incorporate a broad, generalized provision regarding account termination that does not fully encapsulate the providers' practices in enforcing such policies.

For example, during the *Viacom* case it was revealed that YouTube utilized a "three-strikes" policy, premised on YouTube's warnings that the user had uploaded infringing material that was initiated by DMCA take-down notices, in the enforcement of its repeat infringer account termination policy.[255] The court determined that this policy, which counted "as only one strike against a user both (1) a single DMCA take-down notice identifying multiple videos uploaded by the user, and (2) multiple take-down notices identifying videos uploaded by the user received by YouTube within a two-hour period,"[256] qualified as a "reasonably implemented" policy that allowed YouTube safe harbor eligibility.[257] However, this level of detail regarding actual policy enforcement is visibly missing in the drafted provisions of the user agreement, which provide only that "YouTube will terminate a user's access to the Service if, under appropriate circumstances, the user is determined to be a repeat infringer."[258]

Although not required by the DMCA,[259] more detailed specificity in drafting the account termination policies within user agreements would significantly benefit users, as it would provide an actual notice of the triggers for account termination that is currently missing in most user agreements. Educating users in this way can prospectively stop users from posting infringing content without the awareness that it is infringing—a goal that some Internet and online service providers have already publicly articulated.[260] Further, it would demonstrate the service providers' transparency of operation, which would be of significant benefit to disprove wrongdoing in a DMCA safe harbor-related lawsuit. Although In-

---

propriate.") *and Vimeo Terms of Service*, VIMEO (Jan. 7, 2011), http://vimeo.com/terms ("VIMEO may, in appropriate circumstances and at its discretion, terminate the accounts of users who infringe the intellectual property rights of others.").

253. *See supra* text accompanying notes 55–59.

254. *See supra* Part II.B.

255. *See* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 527 (S.D.N.Y. 2010).

256. *Id.* at 527–28.

257. *See id.* at 528.

258. *Terms of Service: Community Guidelines*, *supra* note 169.

259. *See, e.g.*, Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004) (finding that a service provider need not reveal its internal "decision-making criteria to the user" in order to have a valid § 512(i) policy).

260. *See, e.g.*, Declaration of Zahavah Levine at 2, Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 1:07-cv-02103) ("A key component of YouTube's approach to protecting copyright holders is to educate its users.").

ternet and online service providers may hesitate to increase the transparency of their operations in an environment of uncertainty regarding future holdings on the reasonableness of § 512(i) policies, these norms will likely soon be established by judicial arbiters.[261] Once these norms are established in a user agreement's operative jurisdiction, there will be little reason to sustain the current practice of broad generalities as to account termination if the providers are truly invested in the deterrence of online copyright infringement.

This increased transparency could also be accomplished via revisions to the other relevant DMCA remedial provisions within these user agreements. Specifically, Internet and online service providers can clarify the account termination policy if the DMCA notice and takedown procedures, as well as the counter-notification and put-back provisions, are stated clearly and with sufficient detail.[262] Further, these entities should monitor the pending *Lenz v. Universal Music Corp.* case to determine if they should draft user agreement language to specifically reflect the requirement that a copyright owner must first determine if the use of copyrighted work is fair use before filing a DMCA takedown notice.[263] The inclusion of such language would assist in providing a balance for the rights of all stakeholders within these types of intellectual property disputes and would assist in the deterrence of abusive takedown notices.

The impetus to reform DMCA account termination and other related provisions in user agreements requires the internal motivation of Internet and online service providers to be proactive in stopping illegal conduct. Like contract formation mechanisms, these service providers should implement stronger account termination provisions than what are required for baseline compliance with the DMCA in order to actively deter copyright infringement. By reforming these provisions, Internet and online service providers can provide a clear warning to the user who might contemplate this tortious activity and can provide evidence of their good faith efforts to prevent these actions from occurring.

Further, all of these providers should contemplate the inclusion of liquidated damages clauses within their user agreements as a remedy for a breach, such as use of a website or Internet service to post infringing content. Currently, most Internet and online service providers have indemnification provisions for the losses that might result due to a breach of the

261. The impending decision in the *Viacom* case will set a significant precedent in establishing these norms. *See* Fricklas, *supra* note 130 (noting that the case provides the parties with an accelerated timeframe to have appellate courts resolve the issues related to the applicability of DMCA safe harbor eligibility).

262. *See* 17 U.S.C. §§ 512(c)(2), (3) (2006) (providing the DMCA requirements for a valid notice and takedown procedure); *id.* § 512(g) (2006) (providing the DMCA requirements for counter-notification and replacement of removed materials).

263. *See* Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1154 (N.D. Cal. 2008) ("[I]n order for a copyright owner to proceed under the DMCA with 'a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law,' the owner must evaluate whether the material makes fair use of the copyright.").

user agreement;[264] yet only relatively few provide for the collection of liquidated damages.[265] The uniform drafting of reasonable liquidated damages clauses for user copyright infringement, premised on an adjudication of infringement or knowledge of actual infringement,[266] could provide a viable means to deter this type of user conduct. Given the high stakes of secondary infringement litigation and the insolvency of many users, it seems unlikely that an Internet or online service provider would be fully indemnified by a user who breached the agreement in a way that generated the subsequent DMCA safe harbor-related litigation. However, such an entity may be able to recover a reasonable amount of liquidated damages from such a breaching user.[267] This type of small—but actual[268]—recovery could have an equally actual deterrent effect on digital copyright infringement.

If Internet and online service providers adopt these proposed changes and institute drafting practices that are reflective of these suggestions, these entities must ensure that the end result reflects plain language that is accessible to the user. The efficacy in enforcement of these provisions will decrease if they are couched in "convoluted legalese."[269] The strength of these contractual requirements can only be fully realized if the typical consumer user can understand the language after having actually read it or been exposed to it via the suggested revisions for contract for-

264. *See, e.g., Facebook Statement of Rights and Responsibilities*, *supra* note 252 ("If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim."); *Terms of Service: Community Guidelines*, *supra* note 169 ("To the extent permitted by applicable law, you agree to defend, indemnify and hold harmless YouTube, its parent corporation, officers, directors, employees and agents, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney's fees) arising from: (i) your use of and access to the Service; (ii) your violation of any term of these Terms of Service; (iii) your violation of any third party right, including without limitation any copyright, property, or privacy right; or (iv) any claim that your Content caused damage to a third party. This defense and indemnification obligation will survive these Terms of Service and your use of the Service.").

265. *See, e.g., Craigslist Terms of Use*, *supra* note 193 (providing a tiered structure of liquidated damages (ranging from $25 to $3,000) for various types of breach of the user agreement); *Vimeo Terms of Service*, *supra* note 252 (providing for the collection of liquidated damages, if actual damages cannot be established, for the use of the service to distribute unsolicited bulk email).

266. This is the standard advanced by Professor Nimmer as a definition for "repeat infringer" under the DMCA. *See* 3 MELVILLE NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.10(B)(3) (Matthew Bender ed., 2010).

267. *See* Gregory Scott Crespi, *Measuring "Actual Harm" for the Purpose of Determining the Enforceability of Liquidated Damages Clauses*, 41 HOUS. L. REV. 1579, 1579–80 (2005) ("A contractual provision stipulating a sum of money to be paid as damages in the event of breach will be enforced as a valid liquidated damages clause in most U.S. jurisdictions if, among other minimal requirements that are usually satisfied, it sets forth an amount that is 'reasonable in the light of the anticipated or actual harm caused by the breach.'").

268. Courts have enforced liquidated damages clauses pursuant to breaches of user agreements. *See infra* text accompanying notes 274–76.

269. Tasker & Pakcyk, *supra* note 167, at 144–45 ("A very large percentage of contracts found on the Internet contain convoluted legalese and long, compound sentence structures that are difficult to comprehend, even for experienced judges or counsel.").

mation. With these conditions in place, courts will be more likely to enforce them.[270] Consequently, the use of plain language throughout the entirety of the user agreement is an essential part of an effective adoption of the strategy advanced in this Article.[271] This idea connects all of the proposed changes to contract formation, drafting, and enforcement together.

C. The Open Enforcement of Contractual Provisions in User Agreements

In addition to the implementation of revisions to the contract formation and drafting processes, open enforcement of indemnification and other remedial provisions, as well as increased marketing of these efforts, by Internet and online service providers will be necessary to complete an integrated copyright infringement deterrence strategy. Although these entities may be somewhat reticent to enforce their user agreements,[272] especially in the area of intellectual property disputes,[273] this is an essential component of prospective dissuasion of online copyright infringement and DMCA safe harbor-related litigation. Further, the implementation of the suggested changes to contract formation and drafting will likely help these providers in seeking assistance from courts in enforcement of the user agreements.

Courts have enforced user agreements' remedial provisions—specifically in the form of liquidated damages.[274] Several of these decisions

---

270. *See id.* at 143 ("Attorneys, while drafting extreme Internet agreements to zealously advocate protection for their clients, may have collectively and unintentionally created a catalyst for an upcoming backlash of unfavorable law from the courts and legislative bodies.").

271. Some Internet and online service providers have attempted to transform their user agreements into contracts that are readable and understandable by its users, but this needs to become a uniform and integrated practice. *See, e.g.*, *Vimeo Terms of Service*, *supra* note 252 (providing sideline "Vimeo-speak" explanations as a guide to the terms of service, but noting that "While we've endeavored to make these Terms of Service easier to read and understand by providing the 'Vimeo-speak' explanations, please note that it is the 'Lawyer-speak' section that comprises the actual, legally-binding Terms of Service. As such, the 'Vimeo-speak' section should be seen as a guide or overview only.").

272. *See* Abruzzi, *supra* note 18, at 137–38 ("Unlike digital rights management and copy-protection technologies, which automatically lock down content to prevent privileged and lawful reproduction and further dissemination of content, TOU require attentive policing, and they admit the possibility that a site owner will exercise its judgment and conclude that a certain use is or ought to be tolerated. And indeed, to this point the law reporters have recorded very few instances in which content purveyors have litigated to hold users to the terms of website TOU.").

273. *See, e.g.*, *BuzzMedia Copyright & Intellectual Property Policy*, BuzzMedia (Apr. 2010), http://www.buzz-media.com/copyright/ ("Claimants and users must understand that we are not an intellectual property tribunal. While we and our Designated Copyright Agent may in our discretion use the information provided in order to decide how to respond to infringement claims, we are not responsible for determining the merits of such claims.").

274. *See* Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1064–65 (N.D. Cal. 2010) (awarding Craigslist liquidated damages for the breach of its user agreement); MySpace, Inc. v. TheGlobe.com, Inc., No. CV 06-3391-RGK (JCx), 2007 WL 1686966, at *10 (C.D. Cal. Feb. 27, 2007) (awarding liquidated damages for the distribution of unsolicited email via the forum in violation of the user agreement).

have involved Internet or online service providers that are most prone to DMCA safe harbor-related litigation, such as Craigslist[275] and MySpace.[276] Given this emerging precedent, these entities should vigorously pursue the recovery of liquidated damages for the breach of their user agreements in the form of digital copyright infringement. If an Internet or online service provider has implemented the requirement of a credit card or PayPal account as an identity verification measure in the contract formation process,[277] then this will assist in the collection of these damages after adjudication.

Although the judicial trend is to find valid formation and enforceability of clickwrap user agreements,[278] a few courts have refused to enforce certain provisions in these user agreements against consumers under the theory of unconscionability.[279] These provisions include arbitration provisions[280] and choice of forum clauses.[281] Some courts have also expressed unease with respect to change of terms clauses.[282] However, significant examples exist of contrary holdings that reject the proposition that user agreement clauses are unconscionable and therefore unenforceable.[283] These latter cases appear to represent the future of enforcement of the types of online user agreements that govern the relationship between an Internet and online service provider and a user who can upload

275. *See Craigslist*, 694 F. Supp. 2d at 1064–65.

276. *See MySpace*, 2007 WL 1686966, at *10.

277. *See supra* text accompanying notes 240–42.

278. *See* Abruzzi, *supra* note 18, at 115 ("As time passes and more sites adopt this convention [of clickwrap and browsewrap agreements], and the links subsist on these sites for a longer time, a user's argument that he or she did not know where to find the term will become less supportable. What a court rules, on balance, to be 'sufficiently conspicuous' today may not even require the balancing tomorrow. If the history of shrinkwrap agreements is any guide, browsewrap [and clickwrap] TOU will overcome the skepticism of courts by sheer persistence: it is far safer, jurisprudentially, to ratify widespread business practices than to invalidate them.").

279. *See* Lemley, *supra* note 199, at 462–63 (discussing the trends regarding enforceability of clickwrap agreements).

280. *See, e.g.*, Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 611 (E.D. Pa. 2007) (finding that the arbitration clause in the clickwrap user agreement for Second Life, an online virtual world, is procedurally and substantively unconscionable and refusing to enforce it against a consumer user of the website).

281. *See, e.g.*, Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1177 (N.D. Cal. 2002) (concluding that the PayPal user agreement, including the arbitration clause and choice of forum clause, is substantively unconscionable and refusing to enforce the agreement against a consumer). *See generally* J. Brian Beckham, *Forum Selection Clauses in Clickwrap Agreements*, 14 U. BALT. INTELL. PROP. L.J. 151 (2006) (discussing cases that found enforceability and lack of enforceability of forum selection clauses in clickwrap agreements).

282. *See, e.g.*, Universal Grading Serv. v. eBay, Inc., No. 08-CV-3557 (CPS), 2009 WL 2029796, at *9 n.8 (E.D.N.Y. June 10, 2009) (declining to determine if a subsequent unilateral modification to the user agreement, pursuant to a change of terms clause, properly superseded an earlier version of the user agreement based on a finding that the earlier version contained the same clause at issue).

283. *See* Tricome v. eBay, Inc., No. 09-2492, 2009 WL 3365873, at *3 (E.D. Pa. Oct. 19, 2009) (finding that the eBay "forum selection clause is not substantively unconscionable because it is not so unduly one-sided so as to shock the conscience"); Harold H. Huggins Realty, Inc. v. FNC, Inc., 575 F. Supp. 2d 696, 708 (D. Md. 2008) (finding the validity of a unilateral modification of a user agreement pursuant to a change of terms clause, which resulted in the superseding of a prior agreement).

content to the service.[284]

Given this movement toward enforcement of clickwrap user agreements, as well as the examples of enforcement of liquidated damages clauses for other breaches, Internet and online service providers should seek judicial support for the enforcement of the provisions suggested in Part III.B of this Article.[285] However, these providers also need to shoulder certain responsibilities in marketing these efforts by giving both prospective and retrospective notice to their users. Publicizing these policies and their enforcement is an essential part of the strategy to deter digital copyright infringement.[286]

With respect to prospective notice of intentions to enforce their agreements, Internet and online service providers should first provide notification whenever they institute revisions to the user agreement. Currently, many Internet and online service providers assert that users are bound to the most current user agreement, as posted on the providers' websites, regardless of the nature of the agreement at the time of the original account creation and contract formation.[287] Although at least one court has found that a user is bound by a subsequently posted user agreement when the original contract provided that continued use after some notice of the change in provisions constituted agreement with the revised user agreement,[288] an email notification of all revisions to the user agreement would be another proactive step to deter online copyright infringement and to shield providers against lawsuits that stem from such tortious conduct. This notification should not consist only of cursory notice of the revisions,[289] but it should present these changes in the forms recommended

284. *See supra* text accompanying note 283.

285. *See supra* Part III.B.

286. *See* NIMMER & NIMMER, *supra* note 266, at § 12B.10(f) (discussing how Internet and online service providers should publicize DMCA account termination policies).

287. *See, e.g.*, *Terms of Service: Community Guidelines*, *supra* note 169 ("Although we may attempt to notify you when major changes are made to these Terms of Service, you should periodically review the most up-to-date version http://www.youtube.com/t/terms. YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions."); *Terms of Use*, *supra* note 207 ("Veoh shall have the right to modify these TOU at any time, which modification shall be effective upon posting the new TOU on the Terms of Use page of the Veoh Website. We recommend that You check the Veoh website regularly for any such changes. Your use of the Veoh Service following such posting shall be deemed to constitute Your acceptance of such modification."). *But see MySpace.com Terms of Use Agreement*, *supra* note 196 ("MySpace reserves the right to modify this Agreement at any time and from time to time, and each such modification shall be effective upon posting on the MySpace Services. All material modifications will apply prospectively only. Your continued use of the MySpace Services following any such modification constitutes your agreement to be bound by and your acceptance of the Agreement as so modified. It is therefore important that you review this Agreement regularly. If you do not agree to be bound by this Agreement and to abide by all Applicable Law, you must discontinue use of the MySpace Services immediately.").

288. *See* TradeComet.com LLC v. Google, Inc., 693 F. Supp. 2d 370, 375–76 (S.D.N.Y. 2010).

289. *See, e.g.*, Sawyer v. Bill Me Later, Inc., No. CV 10-04461 SJO JCGX, 2010 WL 5289537, at *2 (C.D. Cal. Oct. 4, 2010) (finding that a revised agreement bound a user who had received "electronic notice via e-mail, announcing changes to the Original Agreement

for increased assent mechanisms as discussed in Part III.A of this Article.[290] This type of notice would demonstrate the willingness of providers to be transparent in their operations with respect to the unauthorized posting of copyrighted content, as it is unreasonable for users to have to compare two user agreements. Such a process might even be impossible if the old user agreement becomes no longer accessible via the website.

Additionally, Internet and online service providers should provide information through their services about their efforts to enforce user agreements against those users who post infringing content. Most of these entities already provide their users with guidelines that intend to provide education.[291] Providing awareness to these users that they will seek to collect reasonable liquidated damages for the breach of contract that occurs when a user infringes upon another's intellectual property rights via the electronic forum will serve as an additional measure to dissuade this unlawful conduct. This type of openness in enforcement is an important final step in achieving an integrated strategy of digital copyright infringement deterrence.

IV. CONCLUSION

The user agreements that are currently utilized by the Internet and online service providers that are most likely to be defendants in DMCA safe harbor-related litigation are "not a substitute for intellectual property protection."[292] Neither is the threshold compliance with the DMCA's requirements for account termination by Internet and online service providers. Instead, alternative steps need to be taken by these entities to help curb online copyright infringement.[293] One of these steps should be the adoption of the three-part user agreement strategy advanced in this Article.

By adopting this modest yet effective and cost-efficient approach, Internet and online service providers can help copyright holders as well as themselves. Without tortious activity that is violative of copyright law, DMCA safe harbor-related litigation itself could become a nullity.[294] It is a solution that is reflective of both the innovative business practices that

---

and the effective date of those changes," that included a hyperlink to the revised agreement).

290. *See supra* Part III.A.

291. *See, e.g.*, *YouTube Community Guidelines*, *supra* note 222.

292. Sandeen, *supra* note 249, at 553.

293. For example, there have been arguments for the creation of a system of online dispute resolution for certain Internet transactions. *See* Fred Galves, *Virtual Justice As Reality: Making the Resolution of E-Commerce Disputes More Convenient, Legitimate, Efficient, and Secure*, 2009 U. ILL. J.L. TECH. & POL'Y 1, 6 (2009) (advocating for Online Dispute Resolution for e-commerce disputes). Perhaps, much of the unlawful conduct that is associated with online copyright infringement could be resolved in this type of forum. However, without such a forum in place, Internet and online service providers must take action now to contribute to curbing this tortious activity of its users.

294. *See, e.g.*, Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment on Liability and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense at 1-4, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514

can be utilized in the digital arena and a commitment to safeguarding rights that extend back to the origins of American democracy. Further, it is a solution that combines the normative values of contract and intellectual property law, as it allows for an accord between the stakeholders who are affected by online copyright infringement.[295] Finally, it is a pragmatic step toward limiting exposure to liability that could result in losses of billions of dollars.[296]

(S.D.N.Y. 2010) (No. 1:07-cv-02103) (premising claims of liability on the foundation of user copyright infringement).

295. *See* Ritchie, *supra* note 165, at 115-16 ("[Intellectual property and contract law] share the general value of satisfying the reasonable expectations of the parties involved, as well as a balancing of interests between the relevant stake holders, including the public. Moreover, intellectual property rights, like contract rights, are primarily commercial.").

296. *See supra* text accompanying note 31.