The (Im)possibility of "Standard Technical Measures" for UGC Websites

Lauren G. Gallo[*]

INTRODUCTION

In today's highly litigious legal landscape, one might doubt that there could ever be an "open, fair, voluntary" agreement between copyright owners and service providers to police infringement.[1] Congress nevertheless envisioned such a consensus when it developed § (i) of the Digital Millennium Copyright Act (DMCA): "Conditions for [Safe Harbor] Eligibility."[2] An often-overlooked provision of the DMCA, § 512(i) directs right holders and Internet service providers to work together and agree on "standard technical measures" to "identify or protect copyrighted works."[3] In addition to being the product of consensus, these measures must be "available . . . on reasonable and nondiscriminatory terms" and also "not impose substantial costs . . . or substantial burdens."[4] Although ostensibly thorough, these guidelines are too imprecise and elusive to actually guide service providers and right holders toward a consensus; the term "standard technical measures" remains undefined and possibly undefinable more than a decade after passage.

However, right holders and user-generated content sites (UGCs)—the group of DMCA "service providers" that pose the greatest problems for copyright enforcement—already employ audio and video fingerprinting technology as a standard measure to police infringement.[5] Both groups employ this technology both to conduct general policing and also to operate repeat infringer policies, which are separately mandated by § 512(i).[6] Already, fingerprinting technology is fundamental to the protection of copyrighted works on the Internet.[7]

---

[*] J.D. Candidate 2011, Columbia Law School; B.A. Rhetoric and English, University of California—Berkeley. Many thanks to Professor Jane Ginsburg for her helpful input and feedback. Thanks also to Stanley Pierre-Louis, Sean Varah and Fred von Lohmann for their suggestions. Finally, many thanks to Timothy A. Cohan, Shanti E. Sadtler and the staff of the Columbia Journal of Law & the Arts for their excellent editorial contributions.

1. 17 U.S.C. § 512(i)(2)(A) (2006).
2. *Id.*
3. *Id.* § 512(i)(2).
4. *Id.* § 512(1)(2)(B)–(C).
5. *Content Management Overview*, YOUTUBE, http://www.youtube.com/t/content_management (last visited Oct. 21, 2010) ("Hundreds of media companies have signed up [for Audio ID and Video ID fingerprinting] already.").
6. 17 U.S.C. § 512(i)(1).
7. *See Content Management Overview*, *supra* note 5. *See also* Catherine Applefield Olson,

In light of the widespread use of this successful technology and Congress's mandate that the term "standard technical measures" be developed "expeditiously," individual or infrequent holdouts should not obstruct the consensus necessary to define the term.[8] Although Congress expected that a standards development organization would be the key to establishing consensus, no such organization has arisen, and parties remain free to agree independently on such measures.[9]

This Note will argue that fingerprinting technology should qualify as "standard technical measures" under § 512(i), so that right holders and service providers may be on notice of their statutory obligations and may continue to develop "best practice" applications for that technology.

Part I will briefly introduce the reader to fingerprinting technology and to the general scope and purpose of § 512. Part II will then expand this general discussion to describe how—and whether—§ 512 has come to be understood to include UGCs within its scope while right holders continue to accuse UGCs of enabling widespread copyright infringement online.[10] In response to this insecurity, and in an effort to preserve its eligibility, the UGC industry has developed sophisticated, technological practices for identifying and protecting copyrighted works.[11] This Note will argue that, by its widespread use, fingerprinting technology satisfies the qualifications for "standard technical measures" set out in § 512(i).[12] Part III will then uncover legislative history and analogous technological and legal developments in an effort to better illuminate the definition of "standard technical measures" in light of this existing technology. Finally, Part IV concludes with a hypothesis of what "standard technical measures" might usefully look like.

I. THE LEGAL BACKGROUND: "STANDARD TECHNICAL MEASURES" AND WHAT § 512 WAS MEANT TO DO

A. FINGERPRINTING TECHNOLOGY: A STANDARD TECHNICAL MEASURE?

At present, the predominant mechanism for digital copyright enforcement of audio, visual and audiovisual works depends on the application of digital

Audible Magic's Capabilities May Charm the Industry, BILLBOARD, Jan. 11, 2003.

8. At the time of passage, Congress mandated that these measures be developed "expeditiously." S. REP. NO. 105-190, at 52 (1998).

9. *Id.* ("The Committee anticipates that these provisions could be developed both in recognized open standards bodies or in ad hoc groups.").

10. *See* Viacom Int'l Inc. v. YouTube Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (granting YouTube's motion for summary judgment on the grounds that it qualifies for safe harbor immunity under the DMCA and is not secondarily liable for user-generated infringement).

11. *See Content Management Overview*, *supra* note 5.

12. Of course, should the Second Circuit determine that YouTube does not qualify as a service provider within the scope of § 512, UGCs' compliance with the "standard technical measures" provision will be irrelevant. *See* 17 U.S.C. § 512(i) (providing requisite "Conditions for eligibility" for service providers to acquire and preserve safe harbor protection from liability).

"fingerprints" of those works.[13] These fingerprints contain unique, identifying information about copyrighted works including tempo, tone, pitch and color, depending on the nature of the content.[14] Once generated and incorporated into an expansive database, filtering technology will then filter or scan online content by running algorithmic comparisons against works within its referent database.[15] Though imperfect, this "content-based classification" is much more effective than simple search term filtering, which would not match infringing content unless the file name for the content was titled the same as the file name of the copyrighted work. Versions of this technology vary in their ability to match sound or video content that is modified or short in duration, but all perform essentially the same function: scanning the Internet for audiovisual content and comparing that content against a database of copyrighted works in search of matches or incidents of infringement.[16]

Although there is currently no explicit consensus on the application of this technology, all major right holders and UGCs apply it in some form.[17] This universal utilization should be taken to amount to a "broad consensus," required by

13. *See* Mark Holden, *ASCAP's MediaGuide: Will it Identify Your Music?*, FILM MUSIC MAG. (Apr. 11, 2006), http://www.filmmusicmag.com/?p=653.

14. *See, e.g.*, *Audio Fingerprinting*, MUSIC TRACE, http://www.musictrace.de/technologies/fingerprinting.en.htm (last visited Nov. 30, 2010).

15. *See, e.g.*, Stan Z. Li, *Content-Based Audio Classification and Retrieval Using the Nearest Feature Line Method*, 8 IEEE TRANSACTIONS ON SPEECH & AUDIO PROCESSING 619 (Sept. 2000); *Audio Fingerprinting*, *supra* note 14; *Audiomatic Identification (AudioID) Via Acoustic Fingerprints*, FRAUNHOFER IDMT, http://www.idmt.fraunhofer.de/eng/research_topics/ audioid.htm (last visited Nov. 3, 2010); *Auditude's Content ID Indexing System*, AUDITUDE, http://www.auditude.com/products/ (last visited Nov. 3, 2010).

16. *See supra* note 15. Another similar technology, digital watermarking, "involves embedding cryptographic information derived from frames of digital video [or audio] into the video itself." *Digital Video Watermarking: Technical Overview*, MICROSOFT, http://download.microsoft.com/download/d/6/b/d6bde980-5568-4926-8c71-dea63befed64/video_watermk.doc (last visited Oct. 21, 2010). For the moment, the cost and burden of implementing this technology has prohibited its adoption. *Id.* Watermarking will affect the quality of audio or video content ("[a] more secure watermark distorts the original video more than a less secure watermark"), demand a massive overhaul of all existing nonwatermarked content and demand implementation of a separate filtering system to locate this content. *Id.*; David Kravets, *DRM is Dead, But Watermarks Rise From Its Ashes*, WIRED (Jan. 11, 2008), http://www.wired.com/print/entertainment/music/news/2008/01/sony_music ("[W]atermarking is likely to produce fresh, empirical data that copyright material is ping-ponging across peer-to-peer sites—data the industry would use in its ongoing bid to tighten copyright controls, and to browbeat internet service providers to implement large-scale copyright-filtering operations."). Major right holders such as Viacom, Inc. argue that watermarking should supplement fingerprinting technology, enabling right holders to automatically identify their content, and negating the need for a notice-and-takedown system altogether. *See, e.g.*, Jack Balkin, *The Real Issues in* Viacom v. YouTube, BALKINIZATION (June 25, 2010), http://balkin.blogspot.com/2010/06/real-issues-in-viacom-v-youtube.html. Watermarking would provide another line of defense against copyright infringement in addition to fingerprinting. *See, e.g.*, *Audio Fingerprinting*, *supra* note 14. However, watermarking is not currently implemented on as wide a scale as fingerprinting. *See supra*, Balkin. Furthermore, it would require greater cost and proactivity on the part of service providers. *Id.* As such, it does not currently warrant serious consideration as a "standard technical measure[]," developed pursuant to a "broad consensus," available "on reasonable and nondiscriminatory terms" and without "substantial costs . . . or substantial burdens" to service providers. 17 U.S.C. § 512(i)(2)(A)–(C).

17. *See infra* Parts II.C–D.

subsection (2)(A), if only implicitly.[18] Furthermore, the technology's widespread use should serve as prima facie evidence that it is both "available to any person on reasonable and nondiscriminatory terms" and does "not impose substantial costs . . . or substantial burdens" on service providers, consistent with subsections (2)(B) and (C).[19]

Fingerprinting technology appears to satisfy the statutory definition, which Congress provided in anticipation that technology would "be the solution to many of the issues facing copyright owners and service providers in this digital age."[20] However, interested parties continue to dispute the appropriate application of the technology, thus impeding its definitive characterization as a "standard technical measure" in satisfaction of § 512.[21] These unsurprising disagreements should not eclipse the potential importance of fingerprinting technology to resolving the uncertainty of service provider's "Conditions for eligibility," and particularly UGCs' eligibility for DMCA safe harbor immunity. [22]

B. SECTION 512: A COMPLICATED COMPROMISE

Congress enacted 17 U.S.C. § 512 via the DMCA in the wake of a suite of litigation that sought to determine the liability of Internet service providers (ISPs) for vicarious and contributory copyright infringement.[23] ISPs sought, among other things, immunity from, or at least clarification of, their liability to copyright owners for the generation of copies often incidental to their many operations: providing connections and transmissions, storing data, caching and indexing or linking content.[24] The resulting statute carved out exceptions or "safe harbors" from liability for digital copies generated by and through the Internet.[25] As conceived by Congress, limiting ISP liability would ensure "that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet

18. 17 U.S.C. § 512(i)(2)(A).

19. *Id.* § 512(i)(2)(B)–(C).

20. S. REP. NO. 105-190, at 52 (1998).

21. *See, e.g.*, UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1105 (C.D. Cal. 2009) (arguing that Veoh did not meet the requirements set forth in 17 U.S.C. § 512(i)).

22. 17 U.S.C. § 512.

23. In *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), the court held that defendant repair person's incidental upload of plaintiff's copyrighted operating system into a computer's random access memory (RAM) constituted infringement. Subsequently, in *Religious Technology Center v. Netcom On-Line Communication Services*, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995), the district court distinguished *MAI* according to defendants' relative voluntariness. *Id.* at 1368. Because Netcom did not take any affirmative action, the copies at issue were noninfringing because incidental to Netcom's working transmission system. *Id. See also* Digital Millennium Copyright Act of 1998 (DMCA), sec. 202, Pub. L. No. 105-304, 112 Stat. 2860, 2877 (codified at 17 U.S.C. § 512).

24. *See generally* DMCA, 112 Stat. at 2860. *See also* Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004) (stating that Title II of the DMCA "endeavors to facilitate cooperation among Internet service providers and copyright owners").

25. The safe harbors provided by Congress in § 512 include: (a) Transitory digital network communications, (b) System caching, (c) Information residing on systems or networks at the direction of users and (d) Information location tools. 17 U.S.C. § 512(a)–(d).

will continue to expand."[26]

Conditional to those exemptions, the DMCA provides three affirmative steps to ensure that it will benefit only "innocent" service providers: those who neither promote, nor have "actual or constructive knowledge" of infringement facilitated by their transmission or other services.[27] First, under § 512(c), service providers must comply with a notice-and-takedown procedure, whereby copyright holders are charged with actively locating and notifying service providers of infringing material so that the service providers will then "remove or disable access to" that infringing material.[28] The statute describes the requisite elements of these notices, as well as procedures for responding and objecting to them.[29] This particular provision has garnered substantial attention in the courts, in academia and throughout the public, particularly in the blogosphere.[30] Though the provision remains controversial and the legal standards regulating it are by no means fixed, debate and discussion have initiated some momentum toward consistent application of these conditions.[31]

Affected parties have accepted the basic legal framework and their relative burdens, and have instead focused their disputes on the standards informing that procedure, in particular the requisite good faith necessary to issue a takedown notice, and the level of knowledge service providers demand before assuming their obligation to remove content.[32] But as of October 2010, at least one major right holding party has challenged this basic safe harbor framework as applied to

26. S. REP. NO. 105-190, at 8 (1998).

27. ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) (noting that "immunity . . . is not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement").

28. 17 U.S.C. § 512(c)(1)(A).

29. *Id.* § 512(c)(3) (prescribing the "Elements of Notification" for issuing a takedown notice), (f) (imposing liability for "Misrepresentations" in violation of subsection (c)(3)), (g) (prescribing procedures for "Replacement of Removed or Disabled Material and Limitation on Other Liability").

30. *See, e.g.*, Rossi v. Motion Picture Ass'n of Am., 391 F.3d 1000 (9th Cir. 2004) (holding that § 512(c)(3)(A)(v) imposes a standard of *subjective* good faith on the part of copyright holders issuing takedown notices); *ALS Scan*, 239 F.3d 619; Lenz v. Universal Music Grp., 572 F. Supp. 2d 1150, 1156 (N.D. Cal. 2008) (denying a motion to dismiss in light of requirement that copyright holders consider fair use before issuing takedown notices); Jerome H. Reichman, Graeme B. Dinwoodie & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981 (2007); Emily Zarins, *Notice Versus Knowledge Under the Digital Millennium Copyright Act's Safe Harbors*, 92 CAL. L. REV. 257 (2004); Balkin, *supra* note 16; *Deeplinks Blog*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/deeplinks/archive (last visited Oct. 21, 2010); Liz Gannes, *Would Filtering YouTube Make It More Liable?*, GIGAOM.COM, http://gigaom.com/video/would-filtering-youtube-make-it-more-liable/ (last visited Nov. 3, 2010).

31. *See, e.g.*, *Rossi*, 391 F.3d 1000 (holding that the "good faith belief" in infringement contained in a takedown notice be measured under a subjective standard); *Lenz*, 572 F. Supp. 2d at 1156 (ruling that some consideration of fair use is required prior to issuing a takedown notice under § 512(c)); Michael Warnecke, *DMCA's False Notification Provision Gains Traction in Complaints, Case Law*, 12 ELECTRONIC COM. & L. REP. (BNA) 73 (2007) (describing cases invoking § 512(f)).

32. *See supra* notes 27–31 and accompanying text. *See, e.g.*, Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1104–05 (W.D. Wash. 2004) (stating that "knowledge of blatant copyright infringement" minimally requires that service providers receive notice of infringement and "be able to tell merely from looking at the user's activities . . . that copyright infringement is occurring").

UGCs.[33] In its summary judgment motion against YouTube, Viacom alleged that the UGC giant's direct financial benefit and ability to control infringement disqualify it from safe harbor eligibility.[34] This argument constitutes a significant challenge to presently accepted safe harbor coverage.[35] For the moment, the challenge has not succeeded in narrowing the scope of safe harbor eligibility.

Judge Louise Stanton in the Southern District of New York granted YouTube's summary judgment motion, denying Viacom's claims of vicarious and contributory infringement against it.[36] Judge Stanton reasoned that YouTube lacked specific knowledge of "particular case[es]" of infringement and otherwise satisfied the eligibility requirements laid out in § 512(c).[37] Rejecting this statutory interpretation, Viacom maintains that its arguments have "always been about whether intentional theft of copyrighted works is permitted under existing law" and has appealed the district court's interpretation of § 512(c) to the Second Circuit Court of Appeals.[38] Should Viacom's ensuing challenge garner judicial support at the appellate level, its claim would not only invalidate generally accepted safe harbor eligibility for UGCs, but also would undermine the presumption of innocence fundamental to safe harbor immunity at large.[39]

For the moment, and assuming that the Second Circuit will not reverse the district court's determination that YouTube does qualify as a "service provider" under § 512, UGCs must also satisfy two conditions for eligibility specified in § (i) to qualify for safe harbor eligibility.[40] They must adopt and implement repeat infringer policies, and must further "accommodate[] and . . . not interfere with standard technical measures."[41] The extent to which covered service providers currently comply with these requirements remains unknown, even to the providers themselves, because the requirements lack a solid definition. As of yet, these requirements have not enjoyed nearly the level of controversy or litigious attention of the notice-and-takedown provisions of § 512(c) and remain almost entirely indeterminate.[42] This uncertainty leaves service providers free to articulate novel legal standards on one hand, and vulnerable to challenges to their safe harbor

33. *See* Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment on Liability and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense, Viacom Int'l Inc. v. YouTube Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 07 Civ. 2103 (LLS)), 2010 WL 1004561 [hereinafter Viacom Summary Judgment Motion].

34. *Id.* at 56–61.

35. *See also* Balkin, *supra* note 16 (arguing that Viacom's real argument is that YouTube should implement watermarking technology so that Viacom may automatically trace its content on YouTube's server).

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

37. *Id*. at 526–27.

38. Michael Fricklas, *Viacom Statements: The Court Ruling*, VIACOM, http://news.viacom/news/Pages/summaryjudgment.aspx (last visited Nov. 3, 2010).

39. Covered by subsection § 512(c), "Information residing on systems or networks *at the direction of users*." 17 U.S.C. § 512(c) (2006) (emphasis added).

40. *Id.* § 512(i).

41. *Id.* § 512(i)(1)(A)–(B).

42. *See infra* Part III.

eligibility on the other.[43]

Because they pose a considerable threat to copyright holders' exclusive rights and are already foremost in content owners' sights as targets of litigation, UGCs have the greatest incentive to formulate repeat infringer policies and standard technical measures, whether or not their safe harbor immunity is revoked.[44] If a court removes immunity for a particular UGC or for a type of UGC service, repeat infringer policies and standard technical measures may prevent infringement and thus minimize actual causes of action against the sites. But although UGCs have incentives to comply with these two provisions whether or not safe-harbor immunity is found to apply, a Second Circuit reversal in *Viacom v. YouTube* would negate the UGCs' obligation to collaborate in forming a definition of "standard technical measures," as well as their statutory obligation to accommodate and not interfere with those measures.

At present, to counter the rapid reproduction and distribution enabled by such UGC sites, both sites and copyright owners employ technological measures to curtail infringement at a parallel pace.[45] Though the entire industry appears to employ a variety of substantially similar fingerprinting mechanisms, this technology has yet to be explicitly deemed adequate, much less in compliance with § 512(i).[46]

The following section will explore the nature of the fingerprinting technology that is widespread among UGCs and right holders with a lens toward determining whether this technology could, or does, meet the statutory requirements of development pursuant to a broad consensus, with reasonable availability and without substantial cost.[47] In particular, this Note will focus on the first of these requirements—development pursuant to a broad consensus—as this appears to present the greatest barrier to meeting the statutory definition.[48]

43. Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 262 (2009) ("[T]he DMCA safe harbors should be interpreted to promote clarity for private planning. An unclear 'safe harbor' is self-defeating and of no practical use because it cannot guide people in how to avoid liability.") (citing Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275, 1314–16 (2002)).

44. *See, e.g.*, Complaint for Declaratory and Injunctive Relief and Damages, Viacom Int'l Inc. v. YouTube Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 07 Civ. 2103 (LLS)), 2007 WL 775611 [hereinafter Viacom Complaint 1]; *see also* Matt Williams, *The Truth and the "Truthiness" About Knowing Material Misrepresentation*, 9 N.C. J.L. & TECH. 1, 5 n.20 (2007) ("There are strong arguments that YouTube does not qualify for this safe harbor because, inter alia, it is engaged in far more than 'storage' and YouTube receives direct financial benefit from infringing material that it could control.").

45. *See supra* Part I.A.

46. *Id.*; 17 U.S.C. § 512(i)(2).

47. 17 U.S.C. § 512(i)(2).

48. *See, e.g.*, 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.02[B][3][b] (2008) ("Given the incentives of the various parties whose consensus is required before any such technical measures can win adoption, it seems unlikely . . . that the need for any such monitoring will eventuate.").

II. WEB 2.0 TECHNOLOGY: WHAT IT DOES, HOW IT WORKS AND WHY IT MATTERS TO COPYRIGHT

While it was probably not the original intent of the legislation, Web 2.0 sites and UGCs are now generally accepted as falling within the scope of the DMCA.[49] These sites are particularly troubling for copyright holders because users can (and do) upload infringing material faster than content owners can find it and demand that it be taken down pursuant to § 512(c).[50] In response to this unforeseen expansion of copyright infringement online, right holders have repeatedly targeted UGCs in litigation.[51] At present, courts have accepted the safe harbor eligibility of UGCs under § 512(c), which covers "Information residing on systems or networks *at the direction of users*."[52] Right holders have instead focused their disputes on whether UGCs comply with the notice-and-takedown procedure and otherwise meet the statute's prescribed conditions for eligibility.[53] Given the nature of Web 2.0 technology, UGC sites' ability to comply with the conditions for eligibility set forth in § 512(c) and § 512(i) is uncertain.[54]

The DMCA takedown system has been an ineffective method of policing infringement, not to mention a source of possible privacy and First Amendment violations. Therefore, content owners and UGCs have begun to develop policies and devices for curtailing infringement currently outside the reach of the law.[55] Chief among these are the Principles for User Generated Content Services, which explicitly incorporate an expectation that fingerprinting technology will be used to

49. *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 38 (D.D.C. 2003) (quoting Brief of Amici in Support of Verizon's Opposition to RIAA's Motion to Enforce at 6, *In re Verizon*, 240 F. Supp. 2d 24 (No. CIV.A.02-MS-0323(JDB)), 2002 WL 32387949 (describing Web 2.0 world as "not even a glimmer in anyone's eye" at the time of passage)), *rev'd sub nom.* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003); *see also* Viacom Summary Judgment Motion, *supra* note 33, at 61 (arguing that the infringement on leading UGC site YouTube does not result from any of the specified core functions—transmission, caching, storage and linking—to which the DMCA applies); Viacom Int'l Inc. v. You Tube Inc., 718 F. Supp. 2d 514, 527–29 (S.D.N.Y. 2010) (holding that YouTube satisfies the safe harbor eligibility requirements under § 512).

50. *See, e.g.*, Viacom Complaint 1, *supra* note 44, at 23.

51. *See, e.g.*, *id.*; UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1105 (C.D. Cal. 2009).

52. 17 U.S.C. § 512(c) (emphasis added).

53. *Id.*

54. *See infra* Part II.A.

55. 17 U.S.C. § 512(c); *see* Online Policy Grp. v. Diebold, 337 F. Supp. 2d 1195, 1203 (N.D. Cal. 2004) (explaining that "[i]t is hard to imagine a subject the discussion of which could be more in the public interest," than the use of a copyrighted email archive to inform the public about the problems associated with electronic voting machines, which a DMCA takedown notice targeted); Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effect"? Take-down Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006) (reporting on findings from an empirical study of takedown practice and concluding that overbroad takedown notices pose policy concerns for the system as a whole); PRINCIPLES FOR USER GENERATED CONTENT SERVICES, http://www.ugcprinciples.com (last visited Nov. 25, 2010) [hereinafter UGC PRINCIPLES] (providing a leading example of a voluntary agreement between and among copyright owners and UGC services for how to limit copyright infringement beyond the notice-and-takedown system).

police copyright.[56] At present, every major right holder and UGC applies fingerprinting technology because it is capable of quickly identifying and locating infringing content.[57] As Congress predicted, "technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age."[58]

To describe how, and whether, technology has met Congress's expectation, this section will begin by providing a brief illustration of what UGCs do and how they operate. Part B will then discuss how UGCs have come to be considered eligible for DMCA safe harbor protection by various district courts, despite Viacom's recent challenge.[59] Next, Part C will introduce a recent "best practice" initiative to redistribute the burden for policing infringement between copyright owners and UGC sites. "The Copyright Principles for UGCs" arguably signifies the closest available opportunity for a "broad consensus."[60] Finally, Part D will examine the actual operation of fingerprinting measures widely used throughout the industry to police and prevent copyright infringement.

A. OVERVIEW OF WEB 2.0 TECHNOLOGY AND UGCS

"Web 2.0" refers to web applications and services that facilitate interactive online participation through information sharing, collaboration and interoperability, as distinguished from noninteractive sites where users are restricted to passive ingestion of information.[61] Common examples are collaborative information resources, such as Wikipedia.com, and file-sharing sites, such as YouTube.com and Vimeo.com. Web 2.0 technology combines user- and server-side software, such that users can input keyword searches, trail information via hyperlinks and contribute original audio, visual and/or literary material.[62] These capabilities were anticipated long before the advent of the Internet. In his 1948 essay, "As We May Think," Vannevar Bush predicted that we would one day no longer be restricted to the associations our authors provide for us, but could, and would, choose our own paths.[63] In his 1968 essay, "The Death of the Author," Roland Barthes described writing as "a multi-dimensional space in which a variety of writings, none of them

56. UGC PRINCIPLES, *supra* note 55.

57. *See, e.g.*, *id.*; *see also Content Management Overview*, *supra* note 5.

58. S. REP. NO. 105-190, at 52 (1998); *see also About Our Company and Industry*, MEDIADEFENDER, http://www.mediadefender.com/aboutUs.html (last visited Oct. 21, 2010) ("Internet-piracy-prevention (IPP) technologies are an emerging means to successfully thwart Internet-based piracy and are critical enablers of the distribution of digitized content through legitimate channels.").

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

60. 17 U.S.C. § 512(i)(2)(A).

61. Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY (Sept. 30, 2005), http://www.www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

62. *See, e.g.*, Andrew P. McAfee, *Enterprise 2.0: The Dawn of Emergent Collaboration*, 47 MIT SLOAN MGMT. REV. 3, 21–28 (2006).

63. Vannevar Bush, *As We May Think*, LIFE, Sept. 10, 1945, at 112–24 (originally published in THE ATLANTIC MONTHLY, July 1945).

original, blend and clash."[64] Today, users interact with and alter the text of others by following hyperlinks, participating in online message boards and even by composing e-mail.[65] Web 2.0 resources have indisputably altered our social, political and economic world.[66] They have facilitated cross-global collaboration and education, enabling users to share artwork and experiences with persons otherwise entirely unconnected to the users themselves.[67] However, Web 2.0 devices have likewise provided a mechanism for the rapid and unauthorized exchange of copyrighted works.[68]

In particular, the species of Web 2.0 applications that accommodate user-generated and user-uploaded content (UGCs) has enabled an unforeseen expansion of copyright infringement.[69] Because infringing content is uploaded at the direction of users at large, right holders must either police a highly diffuse target or police those sites that facilitate the users' individual infringements. As a matter of policy, it has proven exceedingly difficult and politically unpopular to contain widespread infringement by targeting individual users.[70] However, because many of those sites are substantially used for noninfringing purposes, UGCs' liability for indirect infringement remains unclear even after the enactment of the DMCA, which was intended to resolve many of these issues.[71] Copyright owners and UGCs have consequently recognized the need to resolve the uncertainty of such liabilities.[72] In particular, UGCs characterize themselves as service providers within the statutory definition of the DMCA and therefore eligible for safe harbor eligibility and partially insulated from infringement liability.[73]

B. SAFE HARBOR ELIGIBILITY FOR USER-GENERATED CONTENT SERVICES

The DMCA broadly defines "service provider" as "a provider of online services or network access, or the operator of facilities therefor."[74] Much has been written

64. ROLAND BARTHES, *The Death of the Author*, *in* IMAGE—MUSIC—TEXT 146 (Stephen Heath trans., 1977).

65. *See, e.g.*, GEORGE P. LANDOW, HYPERTEXT 2.0, at 80 (2d ed., Johns Hopkins Univ. Press 1997).

66. *See, e.g.*, Tom W. Bell, *The Specter of Copyism v. Blockhead Authors: How User-Generated Content Affects Copyright Policy*, 10 VAND. J. ENT. & TECH. L. 841 (2008) (predicting that UGCs will drive down costs and increase accessibility and availability for creative content).

67. *See e.g.*, WEOWNTV, http://www.weowntv.org (last visited Nov. 3, 2010).

68. *See* Scott Karp, *A Lot of User-Generated Content Is Really User-Appropriated Content*, PUBLISHING 2.0 (Nov. 18, 2006), http://www.publishing2.com/2006/11/18/a-lot-of-user-generated-content-is-really-user-appropriated-content/.

69. *Id.*; *see also* Bell, *supra* note 66.

70. *See, e.g.*, Jonathan Saltzman, *BU Student Admits Illegal Downloads*, BOSTON.COM (July 31, 2009), http://www.boston.com/news/local/massachusetts/articles/2009/07/31/bu_students_admission_of_illegal_downloads_may_cost_him_45m/.

71. *See* Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417 (1984).

72. *See generally*, UGC PRINCIPLES, *supra* note 55.

73. *See, e.g.*, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010); UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1105 (C.D. Cal. 2009).

74. 17 U.S.C. § 512(k)(1)(B) (2006). This definition includes, but is separate from, those entities covered in § 512(a) and (b): Internet access providers such as Netcom, which communicate material through automatic and transitory processes, without selecting, directing or modifying that material. *See*

about the scope of eligibility for DMCA safe harbors in light of this definition.[75] For example, Professor Jane C. Ginsburg posits facetiously that the term "could mean any services offered online, including the services of making copyrighted works available to the public."[76] The statute's legislative history reveals that Congress only anticipated web-specific services widely used in the mid- and late-1990s. The House Report, for example, provides specific examples limited to "providing server space" for traditional online activities such as e-mail and chat rooms.[77] However, the House Report also indicates that though a traditional media operation would not be specifically covered, it would be "to the extent it performs functions covered by (j)(1)(B)."[78] This clarification seems to foresee the probable expansion of DMCA safe harbor coverage to Web 2.0 technologies, even though at the time the DMCA was enacted, the Web 2.0 world was "not even a glimmer in anyone's eye."[79] In light of the limited online operations in existence at the time of enactment, many scholars doubt not only whether the DMCA *should* include UGCs within the term of "service providers," but also whether it was ever meant to.[80]

Courts have repeatedly construed the very general statutory definition of "service providers" to apply to Web 2.0 sites.[81] As a leading example, in *UMG Recordings, Inc. v. Veoh Networks Inc.*, the plaintiff right holder did not dispute that video sharing site Veoh is a "service provider" within the scope of that definition.[82] Nonetheless, UMG claimed that Veoh was not "innocent" with respect to copyright infringement because the UGC did not meet the requirements set forth in § 512(c) and (i) of the Act.[83]

H.R. REP. NO. 105-551, pt. 2, at 50 (1998) ("Subsection (a) applies to service providers transmitting, routing, or providing connections for material, and some forms of intermediate and transient storage of material in the course of performing these functions."); *see also id.* at 52 ("Subsection (b)(1) provides that the material must be transmitted to subsequent users without modification to its content.").

75. *See, e.g.*, NIMMER & NIMMER, *supra* note 48, § 12B.04[A][2][b] (suggesting that DMCA safe harbors only exclude from immunity a limited set of vicarious liability cases of "direct financial benefit," narrower than the common law scope of vicarious liability, which includes indirect benefits); Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 233–69 (2009) (commenting on the ongoing uncertainty over DMCA safe harbors and suggesting guiding principles to clarify and update them); Tim Wu, *Does YouTube Really Have Legal Problems*, SLATE (Oct. 26, 2006, 4:28 PM), http://www.slate.com/id/2152264/ (noting that YouTube is protected by a notice-and-takedown system, but that YouTube's legal status "might not be 100-percent airtight").

76. 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, 593 (2008).

77. *Id.* at 594, n.70 (citing H.R. REP. NO. 105-551, pt. 2, at 53).

78. H.R. REP. NO. 105-551, pt. 2, at 64.

79. *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 38 (D.D.C. 2003) (quoting Brief of Amici in Support of Verizon's Opposition to RIAA's Motion to Enforce at 6, *In re Verizon*, 240 F. Supp. 2d 24 (No. CIV.A.02-MS-0323(JDB)), 2002 WL 32387949), *rev'd sub nom.* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

80. Ginsburg, *supra* note 76, at 593.

81. *See, e.g.*, *In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003); *see also* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

82. UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1105 (C.D. Cal. 2009).

83. *Id.* (citing ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) (stating that "immunity . . . [is] granted only to 'innocent' service providers")); *see also* 17 U.S.C. § 512(c), (i) (2006); Viacom Summary Judgment Motion, *supra* note 33, at 56.

These sections direct service providers to "remove, or disable access to, the material that is claimed to be infringing," to adopt and implement a policy that appropriately terminates the subscriptions of "repeat infringers," and to "accommodate and . . . not interfere with standard technical measures."[84] The extent to which Web 2.0 services have successfully complied with these affirmative obligations is the subject of ongoing debate.[85] In general, UGCs comply with the specific notice-and-takedown process detailed in § 512(c).[86] However, the repeat infringer and standard technical measure requirements in § 512(i) have yet to be conclusively defined, perpetuating the uncertainty of whether UGCs can (or do) comply with the DMCA safe harbor prerequisites.[87]

C. THE UGC PRINCIPLES

In 1997, a group of major commercial copyright owners and web services providing user-uploaded audio and visual content collaborated to establish "Principles for User Generated Content Services."[88] These principles were intended to "foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners."[89] In particular, many of the principles are intended to shift the burden of policing infringement from the Copyright Owners alone to be shared with the UGCs.[90] The Principles take the DMCA safe harbor requirements as their starting point, incorporating requirements such as a "good faith belief" in infringement on the part of copyright owners and "expeditious" removal of allegedly infringing content.[91] A substantial portion of this agreement also calls for the use of "effective content identification technology," that is "highly effective . . . in achieving the goal of eliminating infringing content."[92] Though this technology is not specifically identified, the Principles provide a detailed description of how this technology should function to filter out potentially infringing content *before* the fact.[93]

Initially, the copyright owners must provide UGC sites with "Reference

84. 17 U.S.C. § 512(c)(1)(C), (i)(1)(A)–(B).

85. *See, e.g.*, Viacom Int'l Inc. v. YouTube, Inc., 518 F. Supp. 2d 514 (S.D.N.Y. 2010); *Veoh*, 665 F. Supp. 2d 1099.

86. *See* sources cited *supra* Part I.B.

87. 17 U.S.C. § 512(i)(1)(A)–(B).

88. UGC PRINCIPLES, *supra* note 55. The initial signatories include the major television studios (CBS, Disney, Fox, NBC-Universal and Viacom), and some UGC sites (Myspace, Veoh, Daily Motion and SoapBox). *Id.* Google (YouTube) is notably absent. *Id. See also* Alan N. Braverman & Terri Southwick, *The User-Generated Content Principles: The Motivation, Process, Results and Lessons Learned*, 32 COLUM. J.L. & ARTS 471, 471–80 (2009) (noting that "[t]he hope behind the Principles was that if the rhetoric could be reduced and trust could be built (however slowly), rights owners and UGC platforms should be able to find a shared interest in forging a workable solution").

89. UGC PRINCIPLES, *supra* note 55.

90. Braverman & Southwick, *supra* note 88.

91. 17 U.S.C. § 512(c)(3)(A)(v), (c)(1)(C). For example, under Principle 8, participating UGCs agreed to facilitate the notice and takedown process by expeditiously removing content. UGC PRINCIPLES, *supra* note 55, ¶ 8.

92. UGC PRINCIPLES, *supra* note 55, ¶ 3.

93. *Id.*

Material," which should include the data required to establish a match between the copyrighted work and user-uploaded content, instructions regarding how those matches should be treated and a representation of the owner's authority to exercise rights with respect to those works.[94] This system depends on copyright owners creating digital "fingerprints" of their audio and visual works, which can then be used to target matches or infringing copies online.[95] UGCs are essentially required to participate in this matching process by using the reference material to "filter" or scan user-uploaded content before that content is made available on its service.[96] The Principles accept as their underlying objectives the legitimate interests in "(1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use."[97] With particular attention to the first of these objectives, the Principles provide that the default treatment of content matches should be to block, rather than to allow, notify or license potentially infringing content.[98] Though not enforceable obligations, the Principles provided an informal deadline for UGCs to implement technology by the end of 2007.[99]

These principles merely represent an unenforceable agreement based on best practice and the leading UGC site, YouTube.com, did not sign on. Nevertheless, all major right holders and all major UGCs, including YouTube and other nonsigners like GoFish and Break.com, employ some form of the fingerprinting technology proposed by the UGC Principles.[100] On its face, the extent to which this filtering scheme meets the three-prong definition of "standard technical measures" seems clear. Still, parties dispute the application and effectiveness of fingerprinting technology, obscuring its satisfaction of a "broad consensus."[101]

94. *Id.* ¶ 3(a). Note that "reference material" may include watermarks, but not necessarily. *See supra* note 16; *see also* Bill Rosenblatt, *Video Content Owners and User Generated Content Sites Agree on Filtering Principles*, DRM WATCH (Oct. 25, 2007), http://www.drmwatch.com /watermarking/article.php/3707261 ("Content owners agree to provide information to UGC sites that enables them to use the technology—*such as watermarks*, or copies of content for fingerprinting purposes." (emphasis added)). However, major UGCs party to the Principles, such as Veoh, do not implement this more sophisticated (and burdensome and expensive) technology. *See, e.g.*, Solveig Singleton, *Veoh Wins Copyright Infringement Case*, DRM WATCH (Sept. 11, 2008), http://www.drmwatch.com/legal/article.php/3771041 ("The ruling that equates 'control' with prescreening ability is likely to prove more difficult . . . . [D]oes it simply put more pressure on the content side to step up with technology such as watermarking that would enable such control?").

95. UGC PRINCIPLES, *supra* note 55, ¶ 3(a)–(i).

96. *Id.*

97. UGC PRINCIPLES, *supra* note 55, ¶ 3(d), (f).

98. *Id.* ¶ (3)(a).

99. *Id.* ¶ 3.

100. GoFish.com provides online games, created and rated by users. GOFISH, http://gofish.com/ (last visited Oct. 4, 2010). Break.com provides humorous online videos and video clips, which can be uploaded and ranked by users. BREAK, http://www.break.com/ (last visited Oct. 4, 2010); s*ee also Press Release: Audible Magic Licenses Digital Filtering Technology to Break.com*, AUDIBLE MAGIC (Mar. 15, 2007), http://www.audiblemagic.com/news/press-releases/pr-2007-03-15.asp; *Press Release: GoFish Partners with Audible Magic*, AUDIBLE MAGIC (Mar. 7, 2007), http://www.audiblemagic.com/ news/press-releases/pr-2007-03-07.asp..

101. 17 U.S.C. § 512(i)(2)(A) (2006).

D. TECHNOLOGY USED IN PRACTICE

Fingerprinting measures satisfy the UGC Principles, but do not meet unreasonably high right holder expectations. Right holders such as Universal Music Group (UMG) employ the same technology themselves and furthermore deem the technology sufficient to identify infringers and implement aggressive repeat infringer policies.[102] Nevertheless, right holders are dissatisfied with the current application of fingerprinting technology.[103] But despite their hold-out posture, and despite YouTube's absence from the UGC Principles, parties on both ends of the digital infringement dilemma, including YouTube, rely on fingerprinting technology to regulate infringement. Absent more specific instructions about the terms of the "open, fair, and voluntary" agreement necessary to establish "standard technical measures," widespread fingerprinting technology should satisfy the term.[104]

Despite proprietary variations, fingerprinting technology is widespread among UGCs.[105] Even YouTube, the most notable absentee from the Principles agreement, takes proactive steps to prevent copyright infringement with fingerprinting technology.[106] A party's particular protocol with respect to its fingerprinting identification is not publicly available information. For instance, whether a given right holder or UGC decides to block, tag or do nothing when its program turns up is a matter of "best practice," which varies according to a party's operating system and according to the quality or type of match.[107] However, the general framework and operability of these programs can be readily understood.

YouTube describes its ContentID system as "an advanced set of copyright policies and content management tools to give rights holders control of their content."[108] This system has two different methods of operation: the Content Verification Program and Audio ID and Video ID.[109] The Verification Program tool "assists copyright owners in searching for material that they believe to be infringing, and provid[es] YouTube with information reasonably sufficient to . . . locate that material."[110] Audio ID and Video ID, by comparison, include more technologically sophisticated protection mechanisms.[111] They operate by comparing uploaded YouTube videos against reference files provided by content

102. UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1103, 1116 (C.D. Cal. 2009).

103. *Id.* at 1103 n.6.

104. 17 U.S.C. § 512(i)(2)(A).

105. *See, e.g.*, UGC PRINCIPLES, *supra* note 55.

106. *Content Management Overview*, *supra* note 5.

107. Telephone Interview with Stanley Pierre-Louis, Vice President & Assoc. Gen. Counsel for Intellectual Prop., Viacom Inc. (Jan. 14, 2010) [hereinafter Viacom Interview].

108. *Audio ID and Video ID*, YOUTUBE, http://www.youtube.com/t/contentid (last visited Oct. 21, 2010).

109. *Id.*

110. *Content Verification Program*, YOUTUBE, http://www.youtube.com/t/copyright_program (last visited Oct. 21, 2010).

111. *Audio ID and Video ID*, *supra* note 108.

owners.[112] This comparison process can identify user-uploaded videos comprised entirely or partially of copyrighted content.[113] Once a match occurs, YouTube then implements one of three treatments, depending on the right holder's instruction: "monetize, track, or block."[114] The inner workings of YouTube's identification technology are not publicized, and are unlikely to be revealed, now that Judge Stanton has denied Viacom's motions to compel production of that and similar information.[115] But at face value, it appears that YouTube is employing a device functionally identical to those preferred by the UGC Principles and adopted throughout the industry. Furthermore, many prominent cyber-copyright scholars and practitioners argue that these devices may even go too far.[116]

A recent decision of the U.S. District Court for the Central District of California describes several technological methods that the UGC site Veoh (a party to the UGC Principles) utilizes to prevent copyright infringement.[117] For example, since 2006, Veoh has used "hash filtering" software that "automatically disables access to any identical video and blocks any subsequently submitted duplicates."[118] In addition, since October 2007, Veoh has adopted a third party device from a company called "Audible Magic."[119] As understood by the court, "Audible Magic's product works by taking an audio 'fingerprint' from video files and comparing it to a database of copyrighted content that is provided by content holders."[120] The company's website describes the process, enabled by their "Patented CopySense" identification techniques, as "highly immune to compression or distortion, and . . . indifferent to codec, file type or streaming format."[121] These capabilities are particularly well suited to detect digital files. MP3 files remove imperceptible bits of information, altering the binary encoding of audio files without affecting their sound, in order to store and convey those files in condensed formats.[122] Digital video files can assume various file types, such as .avi, .mov and .flv, requiring a technological device that can detect content matches in a variety of formats.[123] Audible Magic is arguably the industry leader for digital fingerprinting, maintaining a content registry of over six million works.[124] This

112. *Id.*

113. *See Content Management Overview*, *supra* note 5.

114. *Id.*

115. Viacom Int'l Inc. v. YouTube Inc. 253 F.R.D. 256 (S.D.N.Y. 2008).

116. Richard Koman, *EFF's von Lohmann: YouTube Worse Than DMCA for Fair Use*, ZDNET (Apr. 7, 2009), http://government.zdnet.com/?p=4570 ("Under the current process, we make YouTube aware of WMG content. Their content ID tool then takes down all unlicensed tracks, regardless of how they are used." (quoting Will Tanous, Warner Music Grp. Spokesperson)).

117. UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1103 (C.D. Cal. 2009).

118. *Id.*

119. *Id.* at 1103.

120. *Id.*

121. *Content Identification Services*, AUDIBLE MAGIC, http://audiblemagic.com/products-services/contentsvcs (last visited Nov. 3, 2010).

122. *How MP3 Files Work*, HOW STUFF WORKS, http://howstuffworks.com/mp31.htm (last visited Dec. 1, 2010).

123. *Video File Types*, FILEINFO.COM, http://www.fileinfo.com/filetypes/video (last visited Dec. 1, 2010).

124. *Content Identification Services*, *supra* note 121.

database, along with others, supplies a bulk of the reference material, which Veoh and other file-sharing sites use to compare against their user-uploaded files.[125]

This fingerprinting filtering process, anticipated by the UGC Principles described above, has become an industry standard among both copyright holders and UGC sites.[126] For example, major right holder Viacom employs a similar company, Auditude, among others, to imprint its own copyrighted works and search for infringing matches.[127] Similar to Audible Magic, Auditude's Content ID indexing system claims to "fingerprint[] over 100 channels of TV every second every day and applies the right metadata (show name, episode, air date, etc)," at speeds "thirty to 300 times faster than the rest of the industry."[128] According to Sean Varah, CEO of MotionDSP, yet another company producing fingerprinting software, the technology is capable of performing algorithmic matches down to thirty seconds for audio and video content.[129] In other words, the technology can identify a thirty-second clip of a two-hour movie or a thirty-second clip from a four-minute song.[130] The matches are essentially binary, although Viacom describes its matching process on a scoring basis from one to one hundred, such that only matches above a certain score will be deemed positive matches.[131] The program analyzes online audio and video data against a library of copyrighted content and then determines a match by comparing variations in color composition, light, volume, pitch, etc. So, a match of fifty or even seventy-five may not constitute an infringing "match," but one over ninety, or ninety-five, probably would.[132] Once a match is made according to its individual standard, a company then determines treatment instructions based on its best practice—which is not publicly available information and varies from company to company—and then either blocks, tags or does nothing with the matched, and possibly infringing, content.[133]

These mechanisms facially comply with the "content identification technology" practices described by the UGC Principles.[134] However, UMG, Viacom and other right holders insist that these mechanisms, including their own, are insufficient as

125. *Press Release: Dailymotion Selects Audible Magic's Fingerprinting Solution for Detecting Copyrighted Video*, AUDIBLE MAGIC (May 10, 2007), http://www.audiblemagic.com/news/press-releases/pr-2007-05-10.asp; *Press Release: Microsoft Selects Audible Magic's Digital Fingerprinting Technology as Filtering Solution for Soapbox Video Site*, AUDIBLE MAGIC (Mar. 26, 2007), http://www.audiblemagic.com/news/press-releases/pr-2007-03-26.asp.

126. *See supra* Part I.A. *See also* UGC PRINCIPLES, *supra* note 55.

127. Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 260 n.2 (S.D.N.Y. 2008) (quoting Housley Decl. ¶ 2).

128. *Products*, AUDITUDE, http://www.auditude.com/products (last visited Nov. 3, 2010). In contrast, Audible Magic's technology does not use metadata.

129. E-mail from Sean Varah, CEO & Founder, MotionDSP, to author (Nov. 23, 2009, 03:06 EST) (on file with author).

130. *Id.*

131. Viacom Interview, *supra* note 107.

132. *Id.*

133. *Id.*; *see also Audio ID and Video ID*, *supra* note 108.

134. UGC PRINCIPLES, *supra* note 55, ¶ 3.

currently employed by UGCs.[135] Despite removing the "vast majority" of identified copyrighted works, the District Court for the Central District of California found that Veoh's efforts were incomplete: "[E]ven the Audible Magic filter had failed to identify as infringing hundreds of these allegedly infringing videos."[136] Arguably, because of this general dissatisfaction, fingerprinting technology, by definition, cannot meet the broad consensus for "standard technical measures" required by the DMCA.[137] On the other hand, Congress may not have intended unanimity or even near unanimity to qualify as a "broad consensus." In light of the controversies prompting the passage of § 512, it is unlikely that Congress intended to create such a large obstacle in the way of satisfying the safe harbor condition. Because many right holders and UGC sites have already accepted, if not formally agreed to, the use of fingerprinting technology, it is currently the best candidate for fulfilling the terms of the statutory provision.

Relatedly, UMG contends that Audible Magic's matching system should be used to implement the second prong of § 512(i)'s eligibility requirement: the repeat infringer policy.[138] Though the filtering system is not 100 percent effective at identifying its fingerprinted works, UMG reasons that its identifications should nonetheless form a sufficient basis for terminating users.[139] The right holder expects that users whose content is matched through fingerprinting technology should be automatically blocked from accessing the UGC in the future, even though the right holder considers the same technology ineffective in the context of automatically removing infringing content.[140] The District Court for the Central District of California disagreed: "[H]owever beneficial the Audible Magic technology is in helping to identify infringing material," the court reasoned, "it does not meet the standard of reliability and verifiability required . . . to justify terminating a user's account."[141]

The court extended the knowledge standard of § 512(c)(1)(A)—good faith—to repeat infringer termination policies.[142] Thus, the technical measures enabled by Audible Magic, Auditude and MotionDSP "cannot be a valid basis" for terminating a user because the UGC site "has no way of verifying the accuracy of Audible Magic's database, and even if it did, it would be unreasonable to place that burden on [the UGC site]."[143] In other words, in order to allege a good faith belief in infringement, whether on the part of the right holder demanding takedown or on the part of the UGC site terminating repeat infringers, the party must perform some minimal human review and cannot rely solely on technological detection.[144]

135. *See, e.g.*, UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099 (C.D. Cal. 2009); Viacom Complaint 1, *supra* note 44.

136. *Veoh*, 665 F. Supp. 2d at 1104.

137. 17 U.S.C. § 512(i)(1)(B) (2006).

138. 17 U.S.C. § 512(i)(1)(A).

139. *Veoh*, 665 F. Supp. 2d at 1116.

140. *Id.*

141. *Id.*

142. *Id.* at 1117–18 (citing Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1105 (9th Cir. 2007)).

143. *Id.* at 1118.

144. Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1155 (N.D. Cal. 2008) ("The DMCA

This case upheld second-warning termination policies conditional on sworn declarations of good-faith belief in infringement.[145] The court broadened the level of knowledge required for legal action under subsection (c)—"good faith belief"—to encompass subsection (i)—"Conditions for Eligibility."[146]

Though it does not say so explicitly, this holding also sheds light on the "standard technical measures" requirement. First, the court implicitly upheld the Audible Magic filtering process as applied to the vicarious liability described in § 512(c)(1)(B).[147] Second, the court indicated that other, more precise, subsections of § 512 can be extended to interpret the more opaque requirements in 512(i).[148] Although the court did not agree that fingerprinting technology, without more, could authorize a repeat infringer termination, its decision underscores the dissension between UGCs and right holders regarding "standard technical measures." Affected parties universally implement filtering technology as the principal measure for identifying infringing content, but none can reconcile that technology with the statutory requirements of § 512(i).[149]

III. DEFINING "STANDARD TECHNICAL MEASURES": THE INTENT AND THE TECHNOLOGY

Despite the relatively lengthy statutory definition of the term, the phrase "standard technical measures" has yet to attach to any existing technology. Nevertheless, the text hints at the sort of measures the drafters had in mind.[150] The three requisite characteristics—broad consensus, availability and low cost—evoke standards development organizations (SDOs), such as the DVD Copy Control Association (DVD CCA), which have been successful in other areas of legal development.[151] Indeed, the legislative history even anticipates that standard technical measures "could be developed both in recognized open standards bodies or in ad hoc groups," provided the process is consistent with that prescribed by § 512(i)(2)(A).[152]

However, ten years after passage, no SDOs have emerged to resolve the definition. Nor have the courts been any help. Interpreting § 1201, the United

already requires copyright owners to make an initial review of the potentially infringing material . . . indeed it would be impossible to meet any of the requirements of Section 512(c) without doing so."); s*ee also*, Rossi v. Motion Picture Ass'n of Am. Inc., 391 F.3d 1000, 1003–05 n.7 (9th Cir. 2004) (grounding its decision on the minimal review that MPAA agents did employ, although not reaching the issue of human review because MPAA employees reviewed the site); Viacom Interview, *supra* note 107 (indicating that Viacom reviews allegedly infringing material before issuing takedown notices).

145. *Veoh*, 665 F. Supp. 2d at 1117–18.

146. *Id.*

147. *Id.* at 1113.

148. *Id.* at 1117–18.

149. *See supra* Part I.A.

150. 17 U.S.C. § 512(i)(2) (2006).

151. *See id.*; *see also, e.g.*, *All Standards and Drafts*, WORLD WIDE WEB CONSORTIUM (W3C), http://www.w3.org/TR (last visited Dec. 1, 2010) (naming Hypertext Transfer Protocol, Hypertext Markup Language and the World Wide Web as examples of successful SDOs).

152. S. REP. NO. 105-190, at 52 (1998) (noting also: "A number of recognized open standards bodies have substantial experience with Internet issues.").

States District Court for the Eastern District of Pennsylvania stated in dicta that the Robots Exclusion Protocol (robots.txt) could possibly qualify as a "standard technical measure," though it was probably not intentionally developed "to identify or protect" copyrighted works.[153] Automated Content Access Protocol (ACAP) is currently being developed to supplement robots.txt with the express purpose of controlling content use and display and thus expressly meeting the statutory requirement "to identify and protect" copyrighted works.[154] However, ACAP's ability to garner a "broad consensus" is doubtful because it would impose an exceedingly high burden on UGCs and other site hosts to limit the length, type and display settings for user-uploaded and -generated content, compromising their services' appeal and operability.[155] Given the inactivity by SDOs and the courts and the obstacles to the adoption of potentially qualifying robots.txt and ACAP, already-adopted fingerprinting technology may be the best candidate to meet the statutory definition.

Part A of this section will parse the statutory definition by examining the legislative history underlying § 512 and the DMCA generally. Part B will then take a closer look at SDOS, which Congress expected to be the source of reconciling the statutory definition. Finally, Part C will introduce a variety of possible "standard technical measures" considered by the courts to meet the terms of § 512.[156] While these legislative intentions and judicial developments help to illustrate a prediction of what "standard technical measures" should or might have once looked like, all fall short of establishing an appropriate solution.

A. CLUES FOR INTERPRETING § 512(i)(2): THE WHOLE ACT AND THE TEXT

The DMCA, through its notice-and-takedown regime, unmistakably places the burden on right holders to police their own content.[157] Furthermore, UGC technology does not currently support a business model that includes substantial effort at policing infringement by their users. With its passage, § 512 took into account the automated nature of providing many online services, the likelihood of technology to solve copyright problems posed by technology and the probability that standards development organizations would be the source of that technical solution.[158] These considerations are evident in both the language and structure of

153. 17 U.S.C. § 512(i)(2); Healthcare Advocates, Inc. v. Harding, 497 F. Supp. 2d 627, 643 (E.D. Pa. 2007).

154. 17 U.S.C. § 512(i)(1)(B); Gavin O'Reilly, *Solutions to Address the Challenges of Communicating Digital Rights and Permissions*, ACAP: MAKING COPYRIGHT WORK ON THE WEB, http://www.the-acap.org/ (last visited Dec. 1, 2010).

155. *See* Ryan Paul, *A Skeptical Look at the Automated Content Access Protocol*, ARS TECHNICA (Jan. 13, 2008, 11:58 PM), http://arstechnica.com/business/news/2008/01/skeptical-look-at-acap.ars [hereinafter ACAP Ars Technica]; *see also* 17 U.S.C. § 512(i)(2)(C) (requiring that standard technical measures "not impose substantial costs on service providers *or substantial burdens on their systems or networks*." (emphasis added)).

156. 17 U.S.C. § 512(i)(1)(B).

157. Digital Millennium Copyright Act § 202, 17 U.S.C. § 512 (2006); *see also* 17 U.S.C. § 512(m).

158. S. REP. NO. 105-190, at 52 (1998).

the Act itself, which allocates primary responsibility for policing content on the party with the greatest interest in protecting copyrighted work: the right holders themselves.

Apart from their affirmative duty to comply with the takedown requests issued by right holders, UGCs are also responsible, under § 512(i)(1) for "accommodat[ing] and . . . not interfer[ing] with standard technical measures."[159] This language implies that UGCs are not obligated to implement such measures independently, but only that they must "accommodate" them.[160] Based on its plain meaning, this provision can be interpreted to require that UGCs passively tolerate or become compatible with standard technical measures.[161] For example, UGCs might be compelled to allow right holders access to their sites to independently police infringement, but not to perform any affirmative obligation beyond responding to resulting takedown notices.[162] As it stands, this is already more than some UGCs have agreed to.[163]

Under a more exacting interpretation, the provision may require that UGCs actively employ protective measures similar or identical to those employed by right holders on behalf of their copyrights. At least one canon of judicial interpretation—avoidance of redundancy—supports the premise that subsection (i) requires something different from or additional to the previous subsections, which allow service providers to sit and wait for right holders to issue takedown notices.[164]

However, the countervailing canons of statutory interpretation, coupled with existing practice, probably favor a more passive approach to compliance with § 512(i)(2). Under *noscitur a sociis*, for example, "accommodate" would mean "not interfere with," and thus support a passive reading of noninterference.[165] The Whole Act Rule lends support to this approach, given that the DMCA was constructed to *limit* liability of service providers through passive obligations, and in

159. 17 U.S.C. § 512(i)(1)(B). UGC sites also cannot receive direct financial benefit attributable to infringing activity, and must adopt and reasonably implement a repeat infringer policy. 17 U.S.C. § 512(c)(1)(B), (i)(1)(A).

160. 17 U.S.C. § 512(i)(1)(B). The explicit language in § 512(i)(2), which specifies "standard technical measures means technical measures *that are used by copyright owners*," affirms that this requirement is not proactive. 17 U.S.C. § 512(i)(2) (emphasis added).

161. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 11 (4th ed. 2006) (defining "accommodate" as "to make suitable or consistent; adapt;" also, "to have or make room for").

162. By allowing right holders access to identify and locate infringing content, UGCs would simply enable § 512(c) procedure to be consistent with standard open access Internet protocol. 17 U.S.C. § 512(c); *see also id.* § 512(m) (clarifying that service providers have no duty to monitor or affirmatively seek facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i)). At present, because no standard technical measures have been established, this could be simplified to relieve service providers of *any* duty to monitor or affirmatively seek infringing activity beyond the requirements in § 512(c).

163. *See* Viacom Complaint 1, *supra* note 44 (alleging that user privacy settings prevent them from effectively identifying infringing content).

164. *See, e.g.*, Circuit City Stores, Inc. v. Adams, 532 U.S. 105, 121 (2001).

165. *Noscitur a sociis* translates as "by which words are known by their companions." *See, e.g., Circuit City*, 532 U.S. at 115.

light of the limiting language in the Protection of Privacy provision in § 512(m).[166]

The text of § 512(i) also provides a definition of the term "standard technical measures," but this definition has caused more obstacles than clarifications.[167] Subsections (B) and (C) mandate realistic cost and widespread access: straightforward counterparts to the broad consensus requirement of (A).[168] However, in light of the adversarial relationship between service providers and right holders, the broad consensus provision is worrisome.

Though a large section of the industry has arguably demonstrated its willingness and ability to work together in an "open, fair, voluntary, multi-industry standards process," at least in the informal context of the developing the UGC Principles, any broader or legally enforceable collaboration appears at present to be nearly impossible to achieve.[169] Right holders and UGCs have unmistakably competing interests: the former to protect copyright and the latter to attract web traffic, including by reproducing and displaying popular, sometimes copyrighted works. Furthermore, the nature of UGC technology, by which the sites provide and organize a platform for user-uploaded material, does not currently support a business model that includes substantial effort at policing infringement.[170] And the DMCA endorses this inactivity, at least to some degree.

The Act specifies in § 512 (m) that a service provider has no duty to monitor or "affirmatively seek[] facts indicating infringing activity, e*xcept to the extent consistent with a standard technical measure complying with the provisions of subsection (i).*"[171] This limitation is consistent with the underlying purpose of the Act: to enable routine service activities without risking liability and without any obligation to routinely track user activities that may constitute copyright infringement.[172] The Ninth Circuit asserted this principle succinctly: "[t]he DMCA notification procedures place the burden of policing copyright

166. *See* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010); *see, e.g.*, 17 U.S.C. § 512(c)(1)(C) ("*[U]pon notification* of claimed infringement . . . [the service provider] *responds* expeditiously to remove, or disable access to, the material that is claimed to be infringing." (emphasis added)); *Id.* § 512(m) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i).").

167. 17 U.S.C. § 512(i)(2).

168. *Id.* § 512(i)(2)(B), (i)(2)(C), (i)(2)(A). Common sense suggests that any technology developed in an "open, fair, voluntary, multi-industry standards process" would more likely than not be reasonably available and would not impose substantial costs or burdens. These subsections are probably meant to ensure that the "broad consensus" should not be limited to industry leaders, but should include input from startup, independent and nonprofit interests as well.

169. *See, e.g.*, UGC PRINCIPLES, *supra* note 55.

170. Indeed, one could characterize the current fingerprinting technology employed by UGCs as more of a quick fix than a viable solution. *See, e.g.*, Michael S. Sawyer, *Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA*, 24 BERKELEY TECH. L.J. 363, 395 (2009) ("Because it is an automated system, it will capture fair use as well as infringement.").

171. 17 U.S.C. § 512(m)(1) (emphasis added).

172. *See supra* Part I.B. Neither can service providers be "aware of facts or circumstances from which infringing activity is apparent." 17 U.S.C. § 512(c)(1)(A)(ii). The courts have interpreted this "apparent" standard as a very high threshold or "red flag" standard. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).

infringement . . . squarely on the owners of the copyright."[173] This distribution of responsibility supports interpreting the requirement that service providers "accommodate" standard technical measures concurrently with the "complying" language in this subsection. Service providers are therefore probably not obligated to monitor user activity by independently *supplying* technical measures, but should once again oblige and assist the policing goals of right holders through technical measures. This textual interpretation sheds light on what "standard technical measures" might look like by excluding the possibility of a device that would place the responsibility for copyright control entirely in the hands of the UGCs.

On a broader scale, Professor Sonia K. Katyal notes that the phrase "standard technical measures" is "notoriously difficult to define in the wake of changing norms of technology and surveillance."[174] Rapid technological development disturbs the very notion of "standard," which, combined with competing interests in policing enforcement and protecting privacy, has significantly encumbered the process of development. Sites are simultaneously under attack for compromising user privacy, while fielding demands that they keep track of user activity to better monitor for infringement.[175] And, for better or worse, this dilemma does not appear to have been anticipated by the enacting legislature.

In its report on the passage of the DMCA, the Senate Judiciary Committee asserted that technology would solve the problems facing copyright holders and service providers.[176] The report indicates that the "standard technical measures" provision was "intended to encourage appropriate technological solutions to protect copyrighted works."[177] Given the now thirteen-year delay, the Committee foresaw that such a collaborative agreement would be unlikely without legislative backing.[178] However, the legislature did propose one solution, speculating that "these provisions could be developed . . . in recognized open standards bodies," in light of the success of those groups in other realms.[179]

B. LEGISLATIVE INTENT AND THE HOPE FOR STANDARDS DEVELOPMENT ORGANIZATIONS

Open standards bodies, or "Standards Development Organizations," have considerable experience with developing Internet and digital legal management issues.[180] According to the International Telecommunications Union (ITU-T), a

173. *CCBill*, 488 F.3d at 1113.

174. Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 275 (2005).

175. *See, e.g.*, Ryan Paul, *Epic Fail: Google Faces FTC Complaint over Buzz Privacy*, ARS TECHNICA (Feb. 17, 2010, 8:12 AM), http://www.arstechnica.com/security/news/2010/02/epic-fail-google-faces-complaint-over-buzz-privacy-issues.ars; Viacom Complaint 1, *supra* note 44.

176. S. REP. NO. 105-190, at 52 (1998).

177. *Id.*

178. *Id.* ("The Committee strongly urges all of the affected parties expeditiously to commence voluntary, interindustry discussions to agree upon and implement the best technological solutions available to achieve these goals.").

179. *See* UGC PRINCIPLES, *supra* note 55.

180. S. REP. NO. 105-190, at 52.

specialized agency of the United Nations, "Open Standards" are "standards made available to the general public and . . . developed (or approved) and maintained via a collaborative and consensus driven process" to "facilitate interoperability and data exchange among different products or services and . . . intended for widespread adoption."[181] One of the best known examples of this open standards development is the Content Scramble System (CSS), developed by the DVD Copy Control Association (DVD CCA).[182] According to some, the DVD CCA offers the best model for developing "standard technical measures" consistent with the statutory definition.[183]

In 2003, Professor Pamela Samuelson proposed an open standards solution similar to the DVD CCA in response to proposed additional legislative encouragement to produce "standard technical measures."[184] The motion picture industry and other groups of copyright owners collaborated to encourage members of Congress to introduce the Consumer Broadband and Digital Television Promotion Act (CBDTPA).[185] According to Samuelson, the Act "would give representatives of technology companies, copyright holders, and consumer groups 12 months to agree on such 'standard technical measures,'" and would further require FCC rulemaking to require embedding in "every digital media device," arguably including even "general-purpose computers."[186] Samuelson suggests that this legislation would overly tax existing technological freedoms and discusses a better alternative, already anticipated by § 512(i):

> Universal adoption of standard technical protection measures could also come through standards-setting by industry groups. This would have virtually the same effect in the marketplace as a legislative mandate, but happen without input from consumers. For instance, the motion picture and consumer electronics industries reached agreement in 1995 on the content scramble system (CSS) as a standard technical protection measure for DVD discs and players.[187]

The DVD CCA describes itself as a "not-for-profit corporation with responsibility for licensing CSS . . . to manufacturers of DVD hardware, discs and related products."[188] The corporation was formed pursuant to authority granted by the National Cooperative Research and Production Act of 1993, which was designed to clarify the application of antitrust laws and provide shelter to standards

181. *Definition of Open Standards*, ITU-T, http://www.itu.int/ITU-T/othergroups/ipr-adhoc/openstandards.html (last visited Nov. 2, 2010).

182. *Content Scramble System (CSS)*, DVD COPY CONTROL ASS'N, http://www.dvdcca.org/css/ (last visited Dec. 1, 2010).

183. Pamela Samuelson, *The Congressional Corral: The Future of Digital Technology Is in the Hands of the U.S. Congress*, IEEE SPECTRUM, May 2003, at 33, 33–34.

184. *Id.*

185. Declan McCullagh, *Anti-Copy Bill Slams Coders*, WIRED (Mar. 22, 2002), http://www.wired.com/politics/law/ news/2002/03/51274.

186. Samuelson, *supra* note 183, at 33.

187. *Id.* at 34.

188. *Frequently Asked Questions (FAQ)*, DVD COPY CONTROL ASS'N, http://www.dvdcca.org/faq.html (last visited Nov. 2, 2010).

development organizations that follow NCRP procedures.[189] The DVD CCA notice provides that "[t]he nature and objectives of the venture are to provide an encryption technology designed to prevent unlawful or unauthorized copying by encrypting digital files."[190] The cited consensus includes an expansive group of International media companies, including Intel Corporation, LG Electronics and Metro-Goldwyn-Mayer Studios, and since has been widely accepted as the standard technical measure for protecting copyrighted works.[191]

Support for the view that Congress had CSS-type "standard technical measures" in mind may also be found in the anticircumvention provisions of the DMCA, already referenced in the context of robots.txt approval.[192] In § 1201(a)(3), the statute provides illustrative examples of what "technological measure[s] that effectively control[] access to a work protected under [the Copyright Act]" would look like.[193] The subsection includes measures such as "scrambling, encrypting . . .

189. The National Cooperative Research and Production Act of 1993 was subsequently amended by the Standards Development Organization Advancement Act of 2004, sec. 103, § 2 , Pub. L. No. 108-237, 118 Stat. 661, 663 (codified at 15 U.S.C. § 4301 (2006)). The amendment defined "standards development organization" as:

> a domestic or international organization that plans, develops, establishes, or coordinates voluntary consensus standards using procedures that incorporate the attributes of openness, balance of interests,due process, an appeals process, and consensus in a manner consistent with the Office of Management and Budget Circular Number A-119, as revised February 10, 1998.

Id.

190. Notice Pursuant to the National Cooperative Research and Production Act of 1993, 66 Fed. Reg. 40,727-01 (Aug. 3, 2001).

191. *Id.* DeCSS circumvention technology has undermined the effectiveness of CSS, and its legality in light of 17 U.S.C. § 1201 remains subject to debate. *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (holding that Congress can legitimately regulate the "functionality" of DeCSS code). *But see* DVD Copy Control Ass'n v. Bunner, 113 Cal. Rptr. 2d 338 (Ct. App. 2002) (holding that DeCSS is "pure speech" that must not be subjected to prior restraint under the trade secret laws), *rev'd*, 75 P.3d 1 (Cal. 2003), *remanded to*, 10 Cal. Rptr. 3d 185 (Ct. App. 2004) (ruling that the preliminary injunction was not warranted on the grounds that there was no evidence that the Content Scrambling System (CSS) encryption technology used in DVD movie disks was still a trade secret by the time that Bunner posted DeCSS code on his website, so the preliminary injunction was an unconstitutional restriction on his right to free speech). *See also* ROBERT S. THAU & BRYAN TAYLOR, "AUTHORITY OF THE COPYRIGHT OWNER" IN 1201(A), AND FIRST SALE 13 (Aug. 4, 2000), *available at* http://www.ntia.doc.gov/ntiahome/occ/dmca2000/ThauTaylor.pdf.

192. *See supra* note 153 and accompanying text. Like § 512(c), the anticircumvention provision in § 1201 has been hotly contested and hotly litigated. 17 U.S.C. § 1201 (2006). Generally, this provision prohibits breaking or bypassing technical measures in place to protect copyrighted works. *Id.* However, § 1201(a) and (b) vary in scope, the former dealing with both circumventing and trafficking in circumvention tools related to *accessing* copyrighted works, the latter dealing only with trafficking of circumvention tools related to *copying* works already accessed. *Id.* § 1201(a), (b). The scope of § 1201(a) has met challenges as it impliedly extends the scope of copyright to include the right to control access to copyrighted works. *See, e.g.*, 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D.Cal. 2004). On the other hand, § 1201(c) explicitly provides that nothing in § 1201 "shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use." *Id.* § 1201(c). The Federal and Second Circuits have split in their various interpretations to this section. *Compare* Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004), *with* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001). *See generally* 17 U.S.C. § 1201 (2006).

193. 17 U.S.C. § 1201(a)(1)(A).

[or] treatment such as password protection."[194] Such measures include CSS, fingerprinting, robots.txt and other web-crawling protocols: all candidates to hold the title of "standard technical measures." Although the anticircumvention provisions are clearly separate from the liability limitations of § 512, the simultaneous passage of these sections may shed further light on what Congress had in mind when it provided for "standard technical measures" in both sections.

As demonstrated by this and other successful applications of standard development groups, the kind of standard setting envisioned by § 512(i)(2)(A) is feasible despite the adversarial relationship between interested parties. And, if achieved in a manner that does not require significant affirmative obligations on the part of UGCs, it would both satisfy the Protection of Privacy requirement in § 512(m) and not overly burden any of the participating parties. The CBDTPA's FCC rulemaking proposal is unlikely to pass consistently with the DMCA, given the DMCA's requirement that standard technical measures be developed in an "open, fair, *voluntary*, multi-industry standards process."[195] Yet, this proposal serves as an indication that these measures are forthcoming, and that interested parties, at least on one side of the spectrum, are eager for their development and establishment. Until then, the courts have characterized, or come close to characterizing, some technologies as "standard technical measures."[196] However, as discussed below, these are unlikely to garner widespread acceptance by right holders and service providers in satisfaction of the statute.

C. POTENTIALLY QUALIFYING "STANDARD TECHNICAL MEASURES" ACCORDING TO THE COURTS

The robots exclusion standard (robots.txt) is the only arguably qualifying "standard technical measure" identified by the judiciary.[197] Consistent with the statutory definition, the system was initially devised through an open collaborative effort in 1994, and is regarded as the "de-facto standard" for Web publishers to "control the way search engines access and display their content."[198] Leading

194. *Id.* § 1201(a)(3)(A)–(B).

195. *Id.* § 512(i)(2)(A) (emphasis added).

196. *See infra* Part III.C.

197. In *Healthcare Advocates, Inc. v. Harding*, 497 F. Supp. 2d 627 (E.D. Pa. 2007), the District Court for the Eastern District of Pennsylvania considered whether the Robots Exclusion Protocol (robots.txt) satisfied the statutory requirement. Healthcare Advocates placed a robots.txt file on its website "as a means of preventing the public from accessing archived screenshots of [the company's website]." *Id.* at 631. The plaintiff characterized this file use as a "digital padlock," to which only defendant's personnel had the key, such that another's access would be infringing under 17 U.S.C. § 1201(a)(1)(A). *Id.* at 632. The court agreed, reasoning that because a robots.txt file worked to block access to copyrighted images, and because only the website owner could remove the file, it "qualifies as a technological measure effectively controlling access to the archived copyrighted images." *Id.* at 643. In this limited scenario, interpreting another provision of the DMCA, which also anticipates "standard technical measures," the court definitively characterized robots.txt as such. *Id.* Still, the court specified that its holding "should not be interpreted as a finding that a robots.txt file universally qualifies" as a standard technical measure. *Id.*

198. ACAP Ars Technica, *supra* note 155; *A Standard for Robot Exclusion*, WEB ROBOTS PAGES, http://www.robotstxt.org/orig.html (last visited Nov. 2, 2010) (noting that the standards "represent[] a

search engines run by Microsoft, Yahoo and Google all implement robots.txt in some form.[199] Site operators use robots.txt to guide and instruct Web crawling software, which automatically browses the World Wide Web, copying and indexing visited pages to update search engine data.[200] The instructions provided by robots.txt specify files and data that should or should not be accessed by crawling bots.[201] Usefully, these instructions prevent harvesting of personal identifying information for privacy purposes and prevent access to copyrighted works for purposes of copyright protection.[202] At the same time, robots.txt can also be used to enable infringement with the proper instructions.

It is not clear whether robots.txt was intended to "identify or protect copyrighted works," so a court might not find that this technology could qualify as a standard technical measure under § 512(i).[203] At the same time, the statute does not specify that "standard technical measures" must have been developed solely, or even partly, to identify and protect copyrighted works. It may be enough that a broad consensus now exists among copyright owners and service providers who do in fact use robots.txt for the purpose of identifying and protecting copyrighted works.[204] Viewed in this light, robots.txt meets the three-pronged definition: it was developed through an open collaborative effort and is entirely voluntary; it is reasonably available to any person; and it does not impose substantial costs or burdens.[205] However, given its potential infringing uses on one hand and changing technology on the other, robots.txt may soon outlive its usefulness as a "standard technical measure."

Currently, Internet publishers have been devising a similar but more expansive system called the Automated Content Access Protocol (ACAP), which will supplement the Robots Exclusion Protocol with more specific instructions to guide Web crawling software and "dictate the terms under which [written] content can be used and displayed."[206] Specifically, ACAP can:

> describe restrictions on the number of words that third parties are permitted to display in a text snippet, prohibit annotations like user ratings or tags, prohibit conversion to alternate formats like PDF, limit the use of typographical style and formatting changes, restrict translation, [and] insist that the content can only be displayed in a

consensus on 30 June 1994 on the robots mailing list (robots-request@nexor.co.uk), between the majority of robot authors and other people with an interest in robots"); Rick DeJarnette, *Robots Exclusion Protocol: Joining Together to Provide Better Documentation*, BING COMMUNITY (June 3, 2008, 12:00 PM), http://www.bing.com/community/blogs/webmaster/archive/2008/06/03/robots-exclusion-protocol-joining-together-to-provide-better-documentation.aspx.

199. DeJarnette, *supra* note 198.

200. *Id.*

201. *Id.*

202. ACAP Ars Technica, *supra* note 155.

203. 17 U.S.C. § 512(i)(2) (2006).

204. *See* DeJarnette, *supra* note 198. In fact, as may have been the case in *Perfect 10, Inc. v. CCBill LLC*, 481 F.3d 751 (9th Cir. 2007), robots.txt could be used to instead facilitate infringement. Robots.txt metatags can be set to "don't crawl," such that Web crawlers searching for infringing works will bypass the site or sites where infringing work is located.

205. 17 U.S.C. § 512(i)(2)(A)–(C).

206. ACAP Ars Technica, *supra* note 155.

frame that replicates the exact conditions of the original source.[207]

Though the system is entirely voluntary, consistent with the § 512(i)(2)(A) requirements, it may nonetheless prove unduly burdensome to agree upon in practice. The sophisticated metadata restrictions would impose a huge number of restrictions on search engines, limiting whether and how certain materials can be copied and displayed, without regard for the actual, often fair, use of those materials.[208] More recently, Jon Stokes, also of *Ars Technica*, characterized ACAP as "a bit like robots.txt—but on illegal steroids that cause anger management issues and can precipitate bouts of violence and heart problems."[209] Furthermore, ACAP has yet to be endorsed by any mainstream search engine companies, running far afoul of the central criteria that the measures be "developed pursuant to a broad consensus of copyright owners *and service providers*."[210]

Google has also introduced its own metadata standards: "Rich Snippets," which will collect and apply information like user ratings, content samples and other data that publishers are willing to share.[211] Unsurprisingly, Google's modus operandi is to collect more information in order to improve search engine function and use, rather than to limit collected information in the interests of privacy or copyright protection.[212]

The Associated Press and Media Standards Trust have introduced a third new text-based metadata format: "Value Added News," which operates somewhere between the reader friendly Rich Snippets and right holder friendly ACAP scale, attaching both rights information and snippets of text to copyrighted works.[213]

These protocols are limited to print media, as they attach to text and not audio, visual or audiovisual works.[214] Thus, while Value Added News might address the concerns of news publishers—the print media group hardest hit by the digital age—the relevant protocols will not appease the UMGs and Viacoms of the world and will doubtfully garner a broad enough consensus to satisfy the statutory requirements for "standard technical measures."[215] Although Congress probably did not contemplate universal satisfaction when it mandated an "open, fair and

207. *Id.*

208. *Id.*

209. Jon Stokes, *European Publishers Want a Law to Control Online News Access*, ARS TECHNICA (July 10, 2009, 3:45 PM), http://arstechnica.com/media/news/2009/07/european-publishers-want-news-access-controls-legislated.ars. Ryan Paul of *Ars Technica* supposes that the burden of implementation costs and use limitations of ACAP will prevent its implementation by most search engines. ACAP Ars Technica, *supra* note 155.

210. 17 U.S.C. § 512(i)(2)(A) (emphasis added).

211. *Introducing Rich Snippets*, GOOGLE (May 12, 2009), http://googlewebmastercentral.blogspot.com/2009/05/ introducing-rich-snippets.html.

212. *Id.*

213. Stokes, *supra* note 209.

214. *ACAP Executive Summary*, ACAP (June 2008), http://www.the-acap.org/Files/25/25c1462a-b7c8-44bb-997f-be53e5ed73ed.pdf (noting that "[i]n future it will be extended to cover other types of . . . content (including video and audio).").

215. Stephanie Chen, *Newspapers Fold as Readers Defect and Economy Sours*, CNN (Mar. 19, 2009), http://articles.cnn.com/2009-03-19/us/newspaper.decline.layoff_1_newspaper-industry-tucson-citizen-journalism?_s=PM:US.

collaborative" agreement, it probably did expect measures that would rectify copyright infringement of audio and visual works in addition to written works.

This is not to dismiss these developments as fruitless. The statute does provide for "standard technical measures," not a singular measure.[216] There will likely need to be multiple technologies to address the multiple needs of multiple industries. Internet publishers are alone in developing open standards for this purpose. The film, television and music production industries have not taken affirmative steps to develop an "ACAP equivalent" to use in concert with UGCs and other service providers. Unlike Web publishers, production companies cannot embed rights information into already published content.[217] More importantly, these parties continue to dispute the efficiency of protective technology measures that currently do exist.[218] Arguably, in light of these conflicting interests and technological limitations, any resolution of "standard technical measures" to protect audiovisual copyrighted works may be impossible without FCC rulemaking, despite its incongruity with the statutory requirement for voluntariness.[219]

But neither "voluntary" nor any other statutory requirement in § 512(i)(2) has garnered any definitive legal definition. For example, in *Perfect 10, Inc. v. CCBill LLC*, the Ninth Circuit was unable to determine whether preventing access to a website interfered with a "standard technical measure" within the meaning of the statute.[220] In that case, CCBill blocked Perfect 10's access to CCBill affiliated websites, claiming that Perfect 10 had ceased to pay for access.[221] Unable to determine whether accessing a website is a "standard technical measure" satisfying the requirements of § 512(i)(2), the court remanded to the district court to determine first, whether the ability to access websites is a standard technical measure with which CCBill interfered, and second, whether CCBill blocked access because Perfect 10 had previously reversed subscription charges or because CCBill wanted to interfere with Perfect 10's ability to police for infringement.[222] Because Perfect 10 needed to view the website in order to properly "identify or protect [their] copyrighted works," the argument proceeded, this ability constitutes a

216. 17 U.S.C. § 512(i)(1)(B) (2006) (emphasis added).

217. On the other hand, audio and video "watermarking" embeds preproduction digital audio files with a unique identifier or "signature" such that the files can be traced to their source if they are later found in a torrent stream or other unauthorized location. *What it Does and Who it Is For*, AUDIOWATERMARKING.INFO, http://audiowatermarking.info (last visited Nov. 3, 2010); *see also*, Balkin, *supra* note 16 ("Viacom can digitally watermark its video content (and does so) so that Google can filter any Viacom clips uploaded to YouTube, identify them as Viacom files and block them. In other words, instead of using individual notice and takedown, the entire system can be automated using watermarking plus filtering.").

218. *See, e.g.*, Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 260 (S.D.N.Y. 2008) ("If there is a way to write a program that can identify and thus control infringing videos, plaintiffs are free to demonstrate it, with or without reference to the way [YouTube's] Video ID program works.").

219. *See supra* notes 202–04 and accompanying text.

220. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1115 (9th Cir. 2007).

221. *Id.*

222. *Id.*

standard technical measure within the meaning of the statute.[223] On remand, the court would have determined whether granting free access to copyright owners would constitute a "substantial cost" on service providers and therefore was outside the proscribed definition of a "standard technical measure."[224] But the Supreme Court denied certiorari, so this question remains unresolved.[225]

The court in *CCBill* did, however, rule on the "reasonableness" required for implementing repeat infringer termination policies required by § 512(i)(1)(A) "by borrowing the knowledge standard of § 512(c)(1)(A)."[226] The court held that, absent declarations under penalty of perjury that Perfect 10's agent had a "good faith belief" that the user was infringing, their notices of infringement did not provide a valid basis for terminating users.[227] This interpretive tactic may provide the closest approximation of how courts will continue to apply § 512(i)(2)(A) as well. The courts should determine that the "open, fair, voluntary, multi-industry standards process" required by the statute should also be governed by a good faith requirement. In this way, a holdout party would have to show a good faith effort to avoid "substantial costs" and "substantial burdens," rather than simply asserting either one or refusing to participate in a consensus.[228] At a minimum, Congress must have anticipated some mechanism for developing these standards without the help of SDOs or unanimous agreement between all of the widely dispersed, affected parties. Politics aside, one should not assume that Congress deliberately created a statutory "filibuster" for limiting the development of standard technical measures for digital copyright infringement.

IV. WHAT "STANDARD TECHNICAL MEASURES" MIGHT LOOK LIKE

Section 512(i) provides "Conditions for Safe Harbor Eligibility."[229] Though not mandatory per se, these requirements provide the quid pro quo for service providers to operate despite user copyright infringements enabled by their services. Like the

223. 17 U.S.C. § 512(i)(2) (2006); *CCBill*, 488 F.3d at 1115.

224. 17 U.S.C. § 512(i)(2)(C); *CCBill*, 488 F.3d at 1115.

225. Perfect 10, Inc. v. CCBill, 552 U.S. 1062 (2007) (denying petition for writ of certiori). For another application of this argument, see, e.g., Viacom Complaint 1, *supra* note 44 (alleging that YouTube interferes with standard technical measures by allowing users to restrict access to their posted content through privacy settings) (cited by Brandon Brown, *Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World*, 23 BERKELEY TECH. L.J. 437, 460 (2008)). As Brown acknowledges, these decisions are closely related to user privacy and site functionality. Brown, *supra* at 460–61. A ruling that they "interfere with standard technical measures" would compel UGCs to eliminate fundamental privacy features, compromising user rights, in order to remain eligible for safe harbor protection. Brown, *supra* at 462. These allegations remain in Viacom's amended complaint. First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial at 5, Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256 (S.D.N.Y. Apr. 24, 2008) (No. 07-CV-02103), 2008 WL 2062868 ("YouTube allows its users to make the hidden videos available to others through other YouTube features like the 'embed,' 'share,' and 'friends' functions.").

226. *CCBill*, 488 F.3d at 1115.

227. *Id.* at 1114.

228. 17 U.S.C. § 512(i)(2)(C).

229. *Id.* § 512(i).

notice-and-takedown provisions of § 512(c), which require that the service provider respond to right holder notifications of infringement, § 512(i)(1)(B) requires that the service providers "accommodate and not interfere with standard technical measures . . . that are used by copyright owners to identify or protect works."[230] This accommodation constitutes a passive obligation on the part of service providers. The right holders, not the service providers, are expected to implement and apply these measures.[231] However, service providers are expected to participate in an "open, fair, voluntary, multi-industry standards process" in order to develop and establish them.[232] As discussed above, this agreement has not been forthcoming among audio and visual right holders and service providers.[233]

While the ideal option is probably to establish a standards development organization in the vein of the DVD CCA, as Congress anticipated and as Professor Samuelson espouses, these conversations have yet to begin more than a decade after passage of the statute.[234] Pending these discussions, ad hoc groups will most likely assume responsibility for establishing "standard technical measures" consistent with the statute.[235] The most prominent of these groups—the parties behind the UGC Principles—hold significant bargaining power in this process. In light of their posture and their existing practice, the fingerprinting technology widely used throughout the industry will provide the most likely resolution to the statutory uncertainty behind § 512(i). Nonetheless, the technology remains imperfect.

Fingerprinting technology meets the statute's four requirements.[236] First, it is used to identify and, most often, to protect copyrighted works.[237] Second, it is supported by the UGC Principles, which name all of the major broadcast networks and many of the major UGC sites as supporters and therefore have garnered a fairly large consensus.[238] Third, the technology is already widely used and at least one fingerprinting producer, Audible Magic, offers free identification technology to smaller UGCs.[239] Last, the widespread use of the technology, and its free availability, probably mitigates the additional burdens of licensing and implementation costs.

Congress conceded that the development of standard technical measures could occur through ad hoc groups, provided the process was open, fair, voluntary and multi-industry.[240] An open standards body is therefore not required to satisfy the

230. *Id.* § 512(c), (i)(2).

231. *Id.* § 512(i)(1)(B); *see also id.* § 512(c), (m).

232. *Id.* § 512(i)(2)(A).

233. As discussed, ACAP probably presents the best solution for text based media protection, though it has yet to attract the requisite broad consensus. *See supra* Part II.

234. S. REP. NO. 105-190, at 52 (1998); Samuelson, *supra* note 183, at 34.

235. 17 U.S.C. § 512(i)(1)(B).

236. Sawyer, *supra* note 170, at 396–97.

237. *See supra* Part I.

238. *See* UGC PRINCIPLES, *supra* note 55.

239. *Press Release: Audible Magic Broadens Reach with Free Service for UGC Websites*, AUDIBLE MAGIC, (Apr. 8, 2008), http://www.audiblemagic.com/news/press-releases/pr-2008-04-08.asp.

240. S. REP. 105-190 (1998).

first of the three § 512(i)(2) requirements.[241] The second and third requirements—availability and minimal burden—are probably conditional on satisfying the first.[242] Thus, one cannot reasonably predict whether technical measures are available on "nondiscriminatory terms" and without "substantial burden" or "substantial cost" until this initial qualification is met. The arrangement and juxtaposition of these requirements suggests that the multi-industry participants themselves will be responsible for determining what constitutes a "discriminatory term" and a "substantial cost."

The UGC Principles serve as a collaborative statement among leading copyright owners and service providers of audio and video content.[243] As such, their endorsed technology, "Identification Technology," may satisfy the first of the three § 512(i)(2) requirements.[244] Though the leading UGC, YouTube, is notably absent from the agreement, this single holdout should not be dispositive. "Broad consensus" does not mean, and could not reasonably be interpreted to mean, "unanimous consensus." Rather, the plain meaning of "broad" definitively excludes this reading.[245] Even if YouTube were to induce an open standards filibuster, its holding out would not disqualify fingerprinting technology from being a "standard technical measure." YouTube, after all, employs fingerprinting technology of its own.[246]

This is the problem with fingerprinting: the disagreement lies not in the nature of the technology, but in its protocol. Fingerprinting technology is not used consistently between or among service providers or right holders. In some instances, the matches are used to filter content and thus act on it before it becomes available.[247] In other instances, the matches occur after user uploading, and are used to facilitate the notice-and-takedown process.[248] Furthermore, what constitutes a "match" for either purpose remains uncertain and likely inconsistent. What Viacom considers a "match," for instance, probably significantly differs from what YouTube deems a "match."[249] Finally, the actions taken once a match is made—blocking, removing access, licensing use, sending notification or doing nothing—also vary.[250] These decisions remain "best practice" determinations.[251] A "standard technical measure" would require some consensus regarding application in addition to technical platform; though the technology may already exist, the terms of its use in policing infringement may create the greatest source of controversy.

241. 17 U.S.C. § 512(i)(2)(A)–(C) (2006).
242. *Id.* § 512(i)(2)(B)–(C).
243. *See* UGC PRINCIPLES, *supra* note 55.
244. *Id.*
245. AMERICAN HERITAGE COLLEGE DICTIONARY 177 (3d ed. 1993) (defining "broad" as "wide in extent from side to side" and "covering a broad scope; general").
246. *Audio ID and Video ID*, *supra* note 108.
247. *See, e.g.*, *id.*; *see also* Viacom Interview, *supra* note 107.
248. *Audio ID and Video ID*, *supra* note 108; Viacom Interview, *supra* note 107.
249. Viacom Complaint 1, *supra* note 44.
250. *See Audio ID and Video ID*, *supra* note 108; Viacom Interview, *supra* note 107.
251. Viacom Interview, *supra* note 107

Berkeley fellow Michael S. Sawyer has argued that filtering fingerprinting technology used to block content identifications would come at too high a price to fair use.[252] He argues that the technical content identification process prevents a meaningful fair use evaluation.[253] Alternatively, MotionDSP's Sean Varah suggests that some, albeit minimal, fair use review could take place: automated audio or visual matches of audiovisual works would not produce an infringing "match" if the corresponding audio or video in the online content did not also match.[254] For instance, a mashup of copyrighted images remixed to a song or sounds in the public domain would pass as fair use.[255] This automated response would inevitably prove both overinclusive and underinclusive because it would overlook infringing derivative and low quality content and would still "match" with some fair use content.

Fundamentally, technologic binary review cannot satisfy the highly complex and delicate process of fair use evaluation. The Electronic Frontier Foundation has responded to the UGC Principles with its own Fair Use Principles, which would similarly adjust the standards for determining and treating "matches" to better accommodate user freedoms.[256] These interests will necessarily be a part of the "*open*, fair, voluntary, *multi-industry*" discussion between service providers and right holders.[257] A cornerstone of Title 17, awareness of fair use, has grown throughout the industry; even the UGC Principles name accommodating fair use as one of their three main objectives.[258] Ultimately, the resulting "standard technical measure" must represent the most viable compromise.

V. CONCLUSION: REALIZING THE BROAD CONSENSUS

Despite their competing interests, right holders and UGCs already employ audio and video fingerprinting technology as the standard measure to police copyright infringement. Given its preexisting universal use, fingerprinting technology should be taken to satisfy the qualifications for "standard technical measures" set out in § 512(i), so that right holders and service providers both may be on notice of their statutory obligations. The "broad consensus" mandated by the statute has already

252. Sawyer, *supra* note 170, at 395.

253. *Id.* at 388.

254. E-mail from Sean Varah, *supra* note 129.

255. Ryan B., *Mashup: A Fair Use Defense*, YALE L. & TECH. (Feb. 4, 2010), http://www.yalelawtech.org/ip-in-the-digital-age/mashup-a-fair-use-defense (contesting the holding in *Bridgeport* and arguing that mashups should not be considered per se infringing); *ContentID and Fair Use*, BROADCASTING OURSELVES (Apr. 22, 2010), http://youtube-global.blogspot.com/ 2010/04/content-id-and-fair-use.html (conceding that ContentID can't identify context "(like 'educational use' or 'parody')," which would be considered fair use). *But see* Bridgeport Music, Inc. v. Dimension Films, 410 F.3d 792 (6th Cir. 2005) (holding that use of even one second of copyrighted song constitutes infringement). *See also* Tim Wu, *Tolerated Use*, 31 COLUM. J.L. & ARTS 617 (2008) (discussing technically infringing but unenforced use of copyrighted works).

256. *Fair Use Principles for User Generated Video Content*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen (last visited Feb. 11, 2010).

257. 17 U.S.C. § 512(i)(2)(A) (2006) (emphasis added).

258. UGC PRINCIPLES, *supra* note 55, ¶ 3(d), (f).

been reached, and the cost and burden requirements have been implicitly satisfied by that consensus.[259] The affected parties must simply realize their unspoken agreement.

True, right holders and UGCs continue to contest the effectiveness of fingerprinting technology to conduct general monitoring and to accommodate fair use.[260] They also refuse to disclose their respective independent applications of that technology. Therefore, the most probable next step will be to garner a broad consensus for a standard protocol to employ this technology. In keeping with Congress's expectation, interested parties should begin to expound this agreement as soon as possible, regardless of individual holdouts or the absence of a standards development body, and ideally without intervention by the FCC. The standards for determining a "match" and how to treat such matches must be agreed upon in light of the crucial interests at stake: protection of copyright, privacy and fair use.

259. 17 U.S.C. § 512(i)(2)(A).

260. *See, e.g.*, Viacom Summary Judgment Motion, *supra* note 33; Balkin, *supra* note 16.