SPORTS & ENTERTAINMENT LAW JOURNAL
ARIZONA STATE UNIVERSITY
VOLUME 7 SPRING 2018 ISSUE 2

#COPYRIGHT INFRINGEMENT VIA SOCIAL MEDIA LIVE STREAMING: SHORTCOMINGS OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

SELENE PRESSELLER*

ABSTRACT

This Note looks at the effectiveness of the Digital Millennium Copyright Act (DMCA) in an age of rampant online copyright infringement resulting from Social Media Live Streaming (SMLS) technology. The Note highlights the problems faced by entertainment artists who attempt to use the DMCA to keep their creative works from appearing on Social Media sites. It also explains the requirements of the DMCA's "safe harbor" exceptions for Internet Service Providers as interpreted by the courts. Finally, the Note presents four alternative solutions to address the problem presented: (1) expanding of the interpretation of the safe harbor "knowledge" requirement to place more responsibility on Social Media sites; (2) establishing measures that prohibit cell phone use at shows; (3) dedicating greater resources to issuing takedown notices and filing lawsuits; and (4) embracing SMLS and develop a way to control and monetize live streams of their shows.

INTRODUCTION

As the lights go down and crowd starts to roar, a subtle glow lights up the stadium. Twenty years ago, this light would be coming from the stage as the artist made their grand entrance. But today, the light emanates from the thousands of smartphones filling the arena as spectators prepare to watch this live show through the tiny window of their smartphones. Obsessed with capturing every moment of the performance to show friends and followers, concertgoers are more and more commonly seeing

* J.D. Candidate 2019, Sandra Day O'Connor College of Law at Arizona State University.

shows through their iPhone camera lens instead of enjoying it in the moment.

Social Media's[1] rise to societal dominance over the last ten years has forced entertainment artists to grapple with the question of how to maintain control of their live performances in the era of Social Media Live Streaming (SMLS). SMLS allows attendees to share every moment of the action with their followers by broadcasting a live feed of the performance from their phone to their Social Media account for others to watch in real-time. Some artists have taken the "if you can't beat them, then join them" approach and have welcomed SMLS. These artists embrace the increased exposure SMLS brings to their shows as fans broadcast their performances. Other artists have decided not to take this rampant copyright infringement lying down. For example, Dave Chappelle has taken matters into his own hands by introducing a new way to take phones out of his audiences' hands. Chappelle has teamed up with Yondr, a company that manufacturers phone restricting cases, which allows him to create a "phone-free zone" at his shows.[2] Both approaches have their pros and cons, but should the responsibility fall solely on the artists to stop copyright infringement of their live shows via Social Media and SMLS?

When you arrive at a Dave Chappelle show, you are given a Yondr case.[3] Once you slip your phone inside, the case is locked and remains locked while you are in the venue.[4] Of course, if you need to use your phone before the show is over, you are welcome to do so, but you must leave the stage area to access your phone.[5] This way, audience members maintain possession of their phones, but are limited to watching the show with their own two eyes. Chappelle says that he does not want people sharing the content of his performances with the world because it increases the likelihood that someone in an upcoming tour city will see the show

---

[1] Social Media broadly speaking refers to any online content, platform, network, or combination of those modalities. The term social media is explained further in Section II (A).

[2] Janet Morrissey, *Your Phone's on Lockdown. Enjoy the Show*, N.Y. TIMES (Oct. 15, 2016), https://www.nytimes.com/2016/10/16/technology/your-phones-on-lockdown-enjoy-the-show.html.

[3] *Id.*

[4] *Id.*

[5] *Id.*

before they actually *see* the show.[6] Chappelle is not the only artist using Yondr cases or other methods to prevent their shows from being broadcast via Social Media.[7] Artists like Taylor Swift have employed a team of attorneys tasked with issuing takedown requests in an effort to scrub the Internet of any infringing content.[8] Under Title II, the Online Copyright Infringement Liability Limitation Act (OCILLA), of the Digital Millennium Copyright Act (DMCA), a copyright holder can submit a takedown request to an Internet Service Provider (ISP) if they believe another individual has illegally posted copyrighted content on the ISP's website.[9] Unfortunately, mega-stars and smaller artists alike are finding little relief through submitting these takedown requests.[10] The DMCA takedown process can be both slow and cumbersome, and online infringement can be so widespread and reoccurring that relief seems impossible for copyright holders.[11] This begs the question: if artists like Chappelle are spending thousands of dollars to purchase special phone cases to protect their copyrighted content from infringers, how effective is the existing legislation that was passed to accomplish this exact purpose?[12]

---

[6] Allison Sylte, *Why Dave Chappelle Won't Let You Have Your Cellphone at His Colorado Shows*, 9 NEWS (July 12, 2017), http://www.9news.com/article/entertainment/why-dave-chappelle-wont-let-you-have-your-cellphone-at-his-colorado-shows/455865355.

[7] Morrissey, *supra* note 2.

[8] James Geddes, *Taylor Swift Employs Dedicated Team to Remove All Periscope Videos from Net*, TECH TIMES (Sept. 28, 2015), http://www.techtimes.com/articles/88791/20150928/taylor-swift-employs-dedicated-team-to-remove-all-periscope-videos-from-net.htm.

[9] Copyright Act of 1976, 17 U.S.C. § 512 (2010).

[10] Mark Schultz, *Digital age changes all the rules on intellectual property*, THE HILL (Nov. 6, 2017, 1:50 PM EST), http://thehill.com/opinion/finance/358963-digital-age-changes-all-the-rules-on-intellectual-property.

[11] Jonathan Bailey, *How Long Should a DMCA Notice Take*, PLAGIARISM TODAY (Dec. 5, 2008), https://www.plagiarismtoday.com/2008/12/05/how-long-should-a-dmca-notice-take/.

[12] In 2016, in response to the changing status of the Internet, the Copyright Office announced that it would be accepting comments and suggestions regarding the DMCA and its effectiveness. Doug Isenberg, *Is the DMCA an Effective Way to Take Down Infringing*

I. SOCIAL MEDIA

A. DEFINED TERMS

The terms Social Network, Social Media, Social Media Network and Social Media Live Streaming are often used interchangeably; but there are important distinctions. Social Network refers to online platforms—and complimentary apps—that allow users to create accounts and connect with other users.[13] Social Networks facilitate creating relationships through engagement.[14] Social Media is the media, *i.e.*, content—blog, video, photo, slideshow, podcast, newsletter, or ebook—that a user uploads to a Social Network site.[15] A Social Media Network, like Facebook, is the whole package.[16] They offer media editing tools and networking capabilities.[17] Colloquially, Social Network, Social Media, and Social Media Network are used interchangeably when referring to whole package that is a Social Media Network. Currently, the most well-known of these platforms include Facebook, Instagram, YouTube, Twitter, and Snapchat.[18] This Note will refer to these types of sites collectively as "Social Media."

Social Media Live Streaming (SMLS) is a feature included on many popular Social Media sites which parties can use to broadcast their life or experiences in real time[19] using a

---

Content?, GIGALAW (Feb. 3, 2016), https://giga.law/blog/2016/02/03/copyright-office-opens-comment-submissions-on-dmca-take-down-notices.

[13] Fauzia Burke, *Social Media vs. Social Networking*, HUFFPOST (Dec. 2, 2013), http://www.huffingtonpost.com/fauzia-burke/social-media-vs-social-ne_b_4017305.html.

[14] *Id*.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Jeff Dunn, *Facebook Totally Dominates the List of Most Popular Social Media Apps*, BUS. INSIDER (July 27, 2017, 3:10 PM), http://www.businessinsider.com/facebook-dominates-most-popular-social-media-apps-chart-2017-7.

[19] Jennifer McDonnow, *What Parents Need to Understand About Live Streaming Apps*, FAM. ONLINE SAFETY INST. (June 20, 2016), https://www.fosi.org/good-digital-parenting/what-parents-need-understand-about-live-streaming/.

phone, tablet, or computer.[20] SMLS is transmitted in real-time to a user's followers. These followers, or perhaps more appropriately viewers, can watch whatever event the user has chosen to broadcast. After the live stream has concluded, a user's followers are able to view a recorded copy of the video for the next twenty-four hours.[21] A user can also choose to archive their video, thus preventing it from expiring after the twenty-four hour window.[22] SMLS presents a unique legal issue because users of this functionality feel entitled to share their experiences with all of their followers; yet, live streaming a concert or other performance is likely copyright infringement of the artist's rights.[23]

---

[20] Mitchell Labiak, *19 FAQs About Live Streaming Your Business on Social Media*, EXPOSURE NINJA (Feb. 4, 2017), https://exposureninja.com/blog/social-media-and-marketing-live-streaming/.

[21] *About*, FACEBOOK LIVE, https://live.fb.com/about/ (last visited Apr. 10, 2018).

[22] *How Long Are Broadcasts Available?*, PERISCOPE (Apr. 26, 2017, 6:04 PM), https://help.pscp.tv/customer/en/portal/articles/2017799-how-long-are-broadcasts-available-; Rich McCormick, *Periscope Users Can Now Save Their Live-Streamed Broadcasts Forever*, THE VERGE (May 5, 2016, 2:04 AM), https://www.theverge.com/2016/5/5/11595244/how-to-save-periscopes-live-streams; *Archive Live Streams*, YOUTUBE HELP, https://support.google.com/youtube/answer/6247592?hl=en (last visited Jan. 7, 2018).

[23] Kerry O'Shea Gorgone, *Live Streaming Video: Is It Legal?*, THE HUFFINGTON POST (Aug. 30, 2017, 11:36 AM), https://www.huffingtonpost.com/entry/live-streaming-video-is-it-legal_us_59a6d4e9e4b08299d89d0b3e; *Legal Ins and Outs of Live Streaming in Public*, SARA F. HAWKINS ATTORNEY AT LAW, https://sarafhawkins.com/legal-live-streaming-in-public/ (last visited Jan. 7, 2018); Charles Bowen, *The Legal Risks of Live Streaming*, THE BOWEN LAW GROUP (June 29, 2016), http://www.thebowenlawgroup.com/blog/the-legal-risks-of-live-streaming; Valeriya Metla, *Periscope & Meerkat: Live Streaming is the Latest Social Media Development*, LAW STREET (Apr. 14, 2015), https://lawstreetmedia.com/issues/technology/periscope-meerkat-live-streaming-latest-social-media-development/.

B. THE EVOLUTION OF SOCIAL MEDIA

Before delving into the legal problem at hand, it is important to look back at the history and evolution of Social Media to understand the breadth of the developments since the passage of the Digital Millennium Copyright Act some 20 years ago.

Six Degrees is considered to be the first Social Networking site.[24] This site was launched in 1997 and included features such as personal profiles, friends lists, and school affiliations.[25] Six Degrees had more than one million registered users, but access to the Internet was scarce at the time which means that the Internet infrastructure had not yet advanced to accommodate a widely used Social Network.[26] In 2002, Friendster launched as a Social Network that allowed people to connect with their current friends and to discover new friends.[27] The site was instantly popular, with three million users registered in the first three months.[28] As the user base on Friendster grew, the technical infrastructure of the site could not accommodate the growth, and the technical difficulties drove users to a rival site: MySpace.[29] MySpace launched in January of 2004 and users exceeded one million in the first month.[30] It was the number one website in 2006 and was valued at $12 billion at its peak in 2007.[31] These three sites served as the foundation upon which today's Social Media platforms were built.

---

[24] *Then and Now: A History of Social Networking Sites*, CBS NEWS, https://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites/2/ (last visited Apr. 10, 2018).

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Jolie O'Dell, *The History of Social Media*, MASHABLE (Jan. 24, 2011), http://mashable.com/2011/01/24/the-history-of-social-media-infographic/#7dlaIjTjnuqD.

[29] *Then and Now: A History of Social Networking Sites*, CBS NEWS, https://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites/2/. MySpace rebranded in 2013 and is now referred to as "Myspace." Monica Riese, *The Definitive History of Social Media*, THE DAILY DOT (Feb. 24, 2017, 5:39 AM), https://www.dailydot.com/debug/history-of-social-media/.

[30] Riese, *supra* note 29.

[31] *Then and Now: A History of Social Networking Sites*, *supra* note 29.

Modern day Social Media giant Facebook[32] launched in 2004 as a Social Network for college students at affiliated universities.[33] Beginning in 2006, Facebook allowed any user with an email to create an account on the site.[34] By July of 2010, Facebook had half a billion users.[35] Instagram, originally just a platform for photo editing and sharing, was launched in 2010.[36] Facebook purchased Instagram in 2012 for nearly one billion dollars.[37] One of the most notable improvements in Facebook's history, "Facebook Live," launched on a limited basis in 2015 and became available to all users in 2016.[38] Facebook Live is a SMLS feature that allows users to share live-streamed content with their Facebook friends.[39] After a user concludes their Facebook Live video, the video is saved to the user's profile.[40] In 2016, Instagram launched "Stories," a feature that allows users to post photos and videos to a twenty-four-hour slideshow that a user's followers can view.[41] The launch of these two features, particularly Facebook Live, has significantly increased the popularity of SMLS with all Social Media users.[42] As of 2017, Facebook had two billion

---

[32] Originally, Facebook was known as "thefacebook.com." Riese, *supra* note 29.

[33] O'Dell, *supra* note 28.

[34] Riese, *supra* note 28.

[35] *Number of Active Users at Facebook over the Years*, THE ASSOCIATED PRESS (May 1, 2013), https://www.yahoo.com/news/number-active-users-facebook-over-230449748.html.

[36] Riese, *supra* note 30.

[37] *Id.*

[38] Joe Lazauskas, *The Untold Story of Facebook Live*, THE CONTENT STRATEGIST (Sept. 27, 2016), https://contently.com/strategist/2016/09/27/facebook-live-resurgence/.

[39] *Id.*

[40] *About*, FACEBOOK LIVE, https://live.fb.com/about/ (last visited Apr. 8, 2018).

[41] Josh Constine, *Instagram Launches "Stories," A Snapchatty Feature For Imperfect Sharing*, TECH CRUNCH (Aug. 2, 2016), https://techcrunch.com/2016/08/02/instagram-stories/.

[42] Nikki Gilliland, *Why Live Video was the Biggest Social Trend of 2016*, ECONSULTANCY (Dec. 20, 2016), https://econsultancy.com/blog/68640-why-live-video-was-the-biggest-social-trend-of-2016.

monthly active users[43] and Instagram had in excesses of seven hundred million monthly active users.[44]

II. EXPLAINING THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

A. THE PURPOSE OF THE DMCA

There are more than one billion websites online,[45] and more than fifty percent of the world's population uses the Internet.[46] When the World Wide Web Project was launched in August of 1991, there was just one website on the Internet.[47] By 1998, barely seven years later, the number of websites on the Internet had exceeded two-million and more than 188 million people were reported to be Internet users.[48] Popular websites like LinkedIn, YouTube, Reddit, Facebook, and Tumblr had not yet been conceived.[49] Yet since the Internet's birth, content industries—Hollywood, music producers, and publishers—have been wary of the massive copyright infringement that could be possible with the Internet.[50] At the time, Title 17 of the United

---

[43] Josh Constine, *Facebook Now Has 2 Billion Monthly Users ... and Responsibility*, TECH CRUNCH (June 27, 2017), https://techcrunch.com/2017/06/27/facebook-2-billion-users/.

[44] Josh Constine, *Instagram's Growth Speeds Up As It Hits 700 Million Users*, TECH CRUNCH (Apr. 26, 2017), https://techcrunch.com/2017/04/26/instagram-700-million-users/.

[45] *Total Number of Websites*, INTERNET LIVE STATS, http://www.internetlivestats.com/total-number-of-websites/ (last visited Jan. 6, 2018).

[46] *Internet World Stats Usage and Population Statistics*, MINIWATTS MARKETING GROUP, http://www.internetworldstats.com/stats.htm (last visited Jan. 6, 2018).

[47] Alyson Shontell, *Flashback: This Is What the First-Ever Website Looked Life*, BUS. INSIDER (June 29, 2011, 4:57 PM), http://www.businessinsider.com/flashback-this-is-what-the-first-website-ever-looked-like-2011-6.

[48] *Total Number of Websites*, INTERNET LIVE STATS, http://www.internetlivestats.com/total-number-of-websites/ (last visited Jan. 6, 2018).

[49] *Id.*

[50] *President Bill Clinton Signs the Digital Millennium Copyright Act into Law*, HISTSORY.COM (2009), http://www.history.com/this-day-in-history/president-bill-clinton-signs-

States Code, as amended by the Copyright Act of 1976, outlined the protections afforded to copyright holders by law.[51] In 1993, Congress acknowledged its own prior deficiency in maintaining copyright laws with emerging technology, and formed a task force to draft updated copyright laws.[52] The Digital Millennium Copyright Act (DMCA), signed into law in October of 1998 by President Bill Clinton, was written to improve upon the existing federal copyright protections in response to the growth of the Internet and the new threats it posed to copyright holders.[53] This Note focuses solely on Title II of the DMCA—Online Copyright Infringement Liability Limitation Act (OCILLA).[54]

---

the-digital-millennium-copyright-act-into-law; *See also* S. REP. No. 105-190 at 9 (1998) [hereinafter *Bill Clinton Signs the DMCA*].

[51] Copyright Act of 1976, 17 U.S.C. § 101 et. seq. (2010).

[52] S. REP. NO. 105-190 at 2 (1998). After five years of collecting testimony from industry experts and other influential personnel, and several revisions to proposed versions of a bill, the Judiciary Committee unanimously ordered the Digital Millennium Copyright Act of 1998 reported favorably. *Id.* at 8 (1998).

[53] *Bill Clinton Signs the DMCA*, *supra* note 50. Congress passed the DMCA to achieve dueling compelling interests of the copyright holder and the Internet Service Provider (ISP). On the one hand, the DMCA assures copyright holders that their content is protected by law and they should continue to feel comfortable making that content readily available to the public. On the other hand, the DMCA assures ISPs that they will receive liability protection for the actions of others on their sites and they should therefore continue to invest in improving the Internet experience. S. REP. NO. 105-190 at 8 (1998).

[54] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998). The DMCA has five primary sections: (1) Title I: WIPO Copyright and Performance and Phonograms Treaties Implementation Act of 1998; (2) Title II: Online Copyright Infringement Liability Limitation Act (OCILLA); (3) Title III: Computer Maintenance Competition Assurance Act; (4) Title IV: Miscellaneous Provisions; and (5) Title V: Vessel Hull Design Protection Act. Title I implements two World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performance and Phonograms Treaty. Title II limits the liability faced by ISPs whose sites may be used by individuals to commit acts of copyright infringement. Title III expands the existing exception relating to copies of computer programs used in conjunction with a computer. Title IV contains six provisions relating to the authority and

B. SECTION 512 [TITLE II] EXPLAINED

Codified by the addition of Section 512 to the Copyright Act,[55] Title II attempts to provide equal protective measures to both copyright owners and Internet Service Providers (ISPs).[56] Congress worried that copyright owners would be deterred from producing and sharing their work if they believed they had no means of protecting their original content.[57] Simultaneously, Congress feared that if ISPs faced a high risk of liability for the content individual users placed on their sites it would stifle the growth of the Internet.[58] Section 512 limits the liability faced by an ISP whose website is used for transmission, storage, or discovery of infringing content.[59] This protection is subject to three mandatory criteria:[60] (1) qualifying as an ISP;[61] (2) implementing a reasonable repeat infringer termination policy;[62] and (3) accommodating standard technical measures.[63] In striking

---

functionality of the Copyright Office. Title V sets out a new system for protecting the designs of vessel hulls. *Id.*

[55] 17 U.S.C. § 512. Title II preserves strong incentives for ISPs and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provided greater certainty to ISPs concerning their legal exposure for infringements that may occur in the course of their activities. S. REP. NO. 105-90 at 20 (1998).

[56] S. REP. NO. 105-190 at 20 (1998).

[57] *Id.* at 8–9.

[58] *Id.* at 8.

[59] *Id.* at 20.

[60] Compliance with all three criteria is necessary for Title II limitation on liability. 17 U.S.C. § 512.

[61] As addressed in subsection (a) of Section 512, the term "service provider" means "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, or material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C. § 512(a). The Social Media sites that will be discussed in this Note are considered to be ISPs.

[62] The second criteria, implementing a termination policy, mandates that an ISP make known to its users that it has a policy of terminating the user accounts of repeat infringers. 17 U.S.C. § 512(i)(1)(A).

[63] The third criterion, "standard technical measures," refers to technical measures employed by the ISP to identify and protect copyrighted works. 17 U.S.C. § 512(i). These technical measures,

a balance between the copyright holder and the ISP, the resulting legislation places the burden of monitoring for copyright infringement on the copyright holder and the responsibility of removing that infringing content expeditiously on the ISP.[64] In other words, an ISP does not have an affirmative duty to monitor its site to claim limited liability;[65] however, if an ISP becomes aware of "red flag" knowledge or receives notice from the copyright holder, then the service provider has an affirmative duty to expeditiously disable access to the content.[66]

Section 512 creates "safe harbors" for four activities commonly conducted by ISPs that allow an ISP to receive the benefit of limited liability.[67] These safe harbors blanket a qualifying ISP in limited liability protection for occurrences on their site that would typically raise a claim of contributory or vicarious liability under existing copyright laws and jurisprudence.[68] An ISP is not liable for monetary damages or other equitable relief if the infringement occurred in the course of one of the following activities: (1) transitory digital network communications;[69] (2) system caching;[70] (3) information residing

---

although required, do not have to be so extensive as to impose substantial costs on the ISP or a great burden on the ISP's network. 17 U.S.C. § 512(i)(2).

[64] S. REP. NO. 105-190 at 44–45 (1998).

[65] "Protecting service providers from the expense of monitoring was an important part of the compromise embodied in the safe harbor." Capitol Records, LLC v. Vimeo, LLC, 826 F.3d 78, 98 (2d Cir. 2016).

[66] S. REP. NO. 105-190 at 44 (1998).

[67] *Id.* at 19.

[68] *Id.*

[69] *Id.* at 41. Subsection (a), "digital network communications," applies to ISPs that act as a conduit for sending the digital communications of others across digital networks. In the course of the ISP transmitting, routing, or providing the connection to complete the sending of digital communications, there is some form of intermediate or transient storage of copies of the content. An ISP is protected from liability for copyright infringement that may occur through the automatic storage of materials transmitted at the direction of another. *Id.*

[70] *Id.* at 42. Subsection (b), "system caching," addresses instances where an ISP serves as an intermediary between the originating site and the intended end user. With system caching, the content in question is stored on the ISP's network for a period of time

on systems or networks at the direction of users;[71] and (4) information location tools.[72] For an ISP to receive limited liability protection under one of the four Section 512 safe harbors, the ISP must comply with the requirements outlined in each subsection.[73] Based on the focus of this Note, the most relevant portion of the DMCA is Section 512(c)—Information Residing on Systems or Networks at Direction of Users.[74]

C. "SAFE HARBOR" REQUIREMENTS

An ISP wishing to benefit from the limitation on liability afforded under Section 512(c) must satisfy four requirements.[75] These four requirements are: (1) an ISP may not have knowledge of the infringing content's presence on their site; (2) an ISP may not receive a financial benefit as a result of the infringing content; (3) an ISP must act expeditiously to remove the infringing content once they have knowledge of its presence; and (4) an ISP must have a designated agent responsible for handling takedown notices.[76] All four of the above standards must be satisfied at all times for an ISP to receive copyright infringement liability protection under the DMCA Section 512(c) safe harbor.[77] An

---

as a means of providing access to the ultimate user. If the stored content is the copyrighted property of another, the ISP has limited liability if the storage was at the direction of a third-party user of the ISP's site. *Id.*

[71] *Id.* at 43. Subsection (c), "information stored on service providers," limits infringement liability for ISPs who store infringing content on their system or network at the direction of a user. This subsection specifically applies to ISPs that provide a forum for users to post content of their choosing, forums such as Facebook, Twitter, or Instagram. Subsection (c) also outlines the procedural requirements for copyright owners to request infringing content be removed from an ISP's network. *Id.*

[72] *Id.* at 47; *see also* 17 U.S.C. § 512(a)-(d), (f) (1998). Subsection (d), "information location tools," applies to ISPs that refer or link users to a secondary online location that hosts infringing material or activity. This reference or linkage to a secondary location is facilitated using information location tools, such as, search engines that recommend sites to users. S. REP. NO. 105-190 at 47 (1998).

[73] 17 U.S.C. § 512 (1998).

[74] *Id.*

[75] *Id.* § 512(c).

[76] *Id.*

[77] *Id.*

understanding of each of the four criteria requires a review of the relevant case law and legislative history.

1. Knowledge

First, the ISP cannot have knowledge of the presence of infringing material on its network.[78] Actual knowledge is not required; if the ISP is aware of facts or circumstances that support even "apparent" knowledge[79] of the infringing material's presence, then that is enough to require the ISP to act expeditiously to remove the infringing content from its site.[80] "Apparent" knowledge is based on facts or circumstances referred to as "red flag" knowledge.[81]

A test for whether an ISP has sufficient knowledge to constitute actual notice came in 2013 from *UMG Recordings v. Shelter Capital Partner*.[82] The court addressed UMG's claim that Veoh, a video-sharing site, had sufficient knowledge or awareness of infringing videos on its site, but did not remove the content.[83] UMG further claimed that Veoh "*must have known* this [UMG's copyrighted music] content was unauthorized, given its general knowledge that its services could be used to post infringing

---

[78] 17 U.S.C. § 512(c)(1)(A)(i).

[79] Also referred to in case law as 'red flags.'

[80] 17 U.S.C. § 512(c)(1)(A)(ii).

[81] S. REP. NO. 105-190, at 44 (1998).

[82] In the case of *UMG Recordings v. Shelter Capital Partner*, Universal Music Group (UMG) filed suit against Veoh Network (Veoh) in 2013 on the grounds that Veoh was liable for direct, vicarious and contributory copyright infringement, and for inducement of infringement based on the infringing content they allowed to be published on their site. Veoh is a publicly accessible website that allows users to share and view video content on the Internet. UMG is one of the largest music producers and publishers. In their complaint, UMG alleges that Veoh's infringement prevention measures, i.e. Veoh's Publisher Terms and Conditions, Terms of Use, and flash filtering software, were not instituted until after infringing content already existed on the Veoh site. Veoh asserted that it was protected by the safe harbor provision in the DMCA. The Ninth Circuit Court of Appeals delivered the ruling on the case. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1011 (9th Cir. 2013).

[83] *Id.* at 1020–21.

material."[84] In its opinion, the court pointed out that Congress required ISPs to have actual knowledge of infringement because "[c]opyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers."[85] The court held that "general knowledge that one's service could be used to share infringing material, is insufficient to meet the actual knowledge requirement under § 512(c)(1)(A)(i)."[86] The burden of identifying infringing material rests on the copyright holder.[87] Ultimately, the court held the safe harbor provision of the DMCA shielded Veoh.[88]

In *Viacom International, Inc. v. YouTube, Inc.*,[89] the court addressed the question of whether the DMCA safe harbor protections required "'actual knowledge' or 'aware[ness]' of facts or circumstances indicating 'specified and identifiable infringements.'"[90] In its opinion, the court stated that:

> The difference between actual knowledge and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and objective standard. In other words, the actual knowledge provision turns on whether the provider actually or 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made

---

[84] *Id.* at 1021 (emphasis added).

[85] *Id.* at 1022.

[86] *Id.*

[87] *Id.* at 1023.

[88] *Id.* at 1006.

[89] Viacom brought a $1 billion lawsuit against Google alleging that YouTube illegally hosted content that infringed on Viacom's copyrighted intellectual property. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012). In its complaint, Viacom alleged that YouTube was liable for direct and secondary copyright infringement resulting from approximately 79,000 videos that appeared on the YouTube website between 2005 and 2008. *Id.* at 26. The court evaluated whether YouTube, as an ISP, was entitled to DMCA safe harbor liability protections. *Id.* at 29.

[90] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012) (quoting *Viacom Int'l, Inc. v. YouTube, Inc.,* 718 F.Supp. 2d 514, 523 (S.D.N.Y. 2010)).

> the specific infringement 'objectively' obvious to a reasonable person.[91]

The court held that, based on the text of § 512(c)(1)(A) and the precedent case law, an ISP will be disqualified from safe harbor protection if they have "actual knowledge or awareness of facts or circumstance that indicate specific and identifiable instances of infringement."[92] The ruling by the court established the red flag knowledge test that has since been used by courts to determine whether an ISP had apparent knowledge.

2. Financial Benefit

Second, the ISP may not receive a direct financial benefit as a result of infringing content that the ISP has the right and the ability to control.[93] In the case of *A&M Records v. Napster, Inc.*,[94] the court sought to interpret the "no direct financial benefit" restriction of the DMCA to determine what would cause an ISP to forfeit their safe harbor liability protections.[95] In addressing the financial benefit an ISP receives from infringing content, the court established that an ISP may not be afforded safe harbor protections if the ISP receives a direct financial benefit from the presence of infringing content on its site.[96] The court stated that "[f]inancial benefit exists where the availability of infringing

---

[91] *Id.*

[92] *Id.* at 32.

[93] 17 U.S.C. § 512(c)(1)(B) (2012).

[94] The case of *A&M Records, Inc. v. Napster, Inc.*, is the first in a line of DMCA cases that interpreted the appropriate application of the DMCA, Section 512. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). Record companies and music producers brought copyright infringement actions against the music sharing website, Napster, on the grounds that Napster, as an ISP, facilitated the transmission and retention of digital audio files by its users. *Id.* at 1011. By accessing the Napster website, users were able to copy MP3 files and upload them to the "library" to be shared with other site users. *Id.* at 1011–12. In response to these claims of contributory and vicarious infringement liability, Napster attempted to establish a defense under the safe harbor protections of the DMCA, Section 512. *Id.* at 1024.

[95] *A&M Records, Inc.*, 239 F.3d 1004.

[96] *Id.* at 1022–25.

material "acts as a 'draw' for customers.'"[97] The court found sufficient evidence showing that Napster's future revenue was linked to the increase in user-base resulting from the infringing content on their site.[98] The court held that the copyrighted material on Napster (music) directly increased the number of site users.[99] As such, Napster was in fact receiving a direct financial benefit from the infringing material because the infringing content drew users to the site.[100] To apply this to Social Media sites, if the presence of infringing content was shown to be a significant draw for users, then this would constitute financial benefit and could render them ineligible for safe harbor protections.

3. Expeditious Removal

Third, once the ISP is notified of the infringing content, pursuant to Section 512(c)(1)(A)(iii), the ISP must either expeditiously remove the infringing materials or disable access to the material.[101] Given that the factual circumstances and technical parameters of each infringement instance will undoubtedly vary, Congress did not establish a uniform time limit for expeditious action.[102] Expeditious removal is not triggered until the ISP has knowledge or awareness of the specific infringing material, as

---

[97] *Id.* at 1023. The *Napster* court cited *Fonovisa, Inc. v. Cherry Auction, Inc.*, in which the court stated that a financial benefit may exist "where infringing performances enhance the attractiveness of the venue." Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263–64 (9th Cir. 1996). Put another way, if the presence of infringing content on a website serves as a draw to users, thereby increasing the user base and thus increasing the financial value of the website, then this is considered to be a direct financial benefit and the ISP is ineligible for Section 512(c) liability protection.

[98] *A&M Records, Inc.*, 239 F.3d at 1023.

[99] *Id.*

[100] *Id.*

[101] 17 U.S.C. § 512(c)(1)(C).

[102] S. REP. NO. 105-190 at 44–45 (1998). Subsection (c)(1)(A)(iii) provides that a service provider must act expeditiously to remove infringing material from their site once they become aware of the material's presence on their site. In contemplating the definition of "expeditiously," the Senate comments, "[b]ecause the factual circumstances and technical parameters may vary from case to case, it is not possible to identify a uniform time limit for expeditious action." *Id.*

defined above, because requiring expeditious removal without specific knowledge or awareness would place too great of a burden on ISPs.[103]

4. Designated Agent

Fourth, the ISP must have a designated agent, whose name and contact information is publicly available through its service in a location that is accessible to the public, including on the ISP's website.[104] The Copyright Office must also have the designated agent's information on file so the Copyright Office can keep an accurate directory of all agents.[105] The designated agent receives all claims of alleged infringement from copyright owners.[106]

D. DMCA TAKEDOWN NOTICE

1. Process for Filing

When Congress passed the DMCA in 1998, some believed that copyright holders
would be best suited to identify infringing content online.[107] By offering protection to ISPs, the Internet could grow and flourish without the constant fear of copyright infringement liability.[108] To strike a balance between the protection of ISPs and the rights of copyright holders, the DMCA includes a takedown notice provision.[109] A copyright owner must file a takedown notice with the ISP's registered agent and must identify the infringing content on the ISP's site.[110] When a copyright owner, or person authorized

---

[103] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 30–31 (2d Cir. 2012). The language of the statute requires expeditious removal of the material at issue. 17 USC § 512(c)(1)(A)(iii). Therefore, to require expeditious removal without specific knowledge of a particular infringement "would be to mandate an amorphous obligation" inconsistent with the statutory intent. *Id.*

[104] 17 U.S.C. § 512(c)(2).

[105] *Id.*

[106] 17 U.S.C. § 512(c)(3)(A)

[107] S. REP. NO. 105-190 at 20 (1998).

[108] *Id.* at 8.

[109] *Id.* at 20.

[110] 17 U.S.C. § 512(c)(3)(A) (2010).

to act on the copyright owner's behalf, submits a takedown notice, the ISP must act expeditiously to remove the infringing content from its site.[111] Upon the filing of a proper takedown notice, the ISP has knowledge of infringing content and is therefore required to take steps to remove the content if the ISP wishes to maintain its safe harbor protections.[112]

A proper takedown notice must include the following information: (1) the complaining party's contact information; (2) identification of the allegedly infringed copyrighted work or works; (3) information detailed enough so the ISP can locate the content; (4) the physical or electronic signature of a person authorized to act on the copyright owner's behalf; (5) a statement affirming that the complaining party has a good faith belief that the infringing content is not authorized by the copyright owner, agent, or law; and (6) a statement that the information in the notice is accurate and that the complaining party is authorized to act on behalf of the copyright owner.[113] A takedown notice that does not substantially comply with these requirements does not trigger an obligation for the ISP to remove the infringing content and is not evidence of the ISP's actual or red flag knowledge of the infringement.[114]

Entertainment artists can submit takedown notices to have infringing content removed from online sites. The notices do not have to be completed by a lawyer, but many artists have lawyers submit the requests on their behalf.[115] Once an individual submits a takedown notice, the party that posted the content may submit a "counter-notice" explaining why they believe they have a good-faith right to use the copyrighted content.[116] The ISP then forwards the counter-notice to the individual that originally submitted the takedown notice.[117] The relevant content remains offline for ten days.[118] During that ten day period, the copyright

---

[111] *Id.*

[112] 17 U.S.C. § 512(c)(1)(Q) (2010).

[113] 17 U.S.C. § 512(c)(3)(A), (d)(3) (2010).

[114] 17 U.S.C. § 512(c)(3)(B)(i) (2010).

[115] Jonathan Bailey, *7 Common Questions about DMCA Counter-Notices Pardon Our Interruption*, PLAGIARISM TODAY (June 3, 2010), https://www.plagiarismtoday.com/2010/06/03/7-common-questions-about-dmca-counter-notices/.

[116] 17 U.S.C. § 512(g) (1998).

[117] Bailey, *supra* note 115.

[118] *Id.*

holder may petition the court for an injunction to prevent the restoration of the content.[119] However, if the original party does not obtain an injunction within ten days, the content is restored to the site.[120] Counter-notices are rare, but when they are filed, a valid copyright holder must then invest a great deal of time and money to protect their content.[121]

2. Effectiveness of Takedown Notices

Artists and ISPs disagree on the effectiveness of DMCA takedown notices.[122] Sites like Google claim that the takedown notices are dealt with in in approximately six hours.[123] Yet most web hosts will likely handle a takedown notice only after 24 to 72 hours.[124] The DMCA requires that an ISP work "expeditiously" to remove infringing content once they have knowledge of its presence on the site, *i.e.* a takedown notice.[125] The lack of clarity surrounding the definition of "expeditiously" has created great discrepancy in what constitutes an adequate ISP takedown notice response time.[126] In its drafting of the DMCA, Congress acknowledged that defining expeditiously would be unwise given the varied nature of the takedown requests.[127] Based on this

---

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] Bailey, *supra* note 11.

[123] *Transparency Report Help Center*, GOOGLE, https://support.google.com/transparencyreport/answer/7347743?hl=en (Google reports that it receives more than six million requests a week and, in total, has received more than one hundred million takedown requests); Stephen Carlisle, *DMCA "Takedown" Notices: Why "Takedown" Should Become "Take Down and Stay Down" and Why It's Good for Everyone*, NOVA SE. U. (July 23, 2014), http://copyright.nova.edu/dmca-takedown-notices/.

[124] Bailey, *supra* note 11. After 72 hours, the probability that the content will be removed decreases and after 96–120 hours the likelihood decreases to almost zero. *Id.*

[125] 17 U.S.C. § 512(c).

[126] Bailey, *supra* note 115.

[127] S. REP. NO. 105–190 at 44 (1998).

legislative history, courts have also avoided defining a uniform time limit that they consider to be expeditiously.[128]

Artists have grown frustrated with the ineffectiveness of the DMCA. In an effort to take action, over 500 artists have signed an open letter to Congress asking that Congress amend the DMCA.[129] The letter called for "sensible reform" of the DMCA.[130] More specifically, the letter called attention to YouTube's safe harbor protection from copyright infringement liability despite the excessive amount of infringing content on the site.[131] Artists claim that YouTube has managed to grow their users and profits on the backs of artists without fairly compensating or protecting those artists.[132] Further, another problem for artists is that after ISPs remove infringing content, there are no sufficient safeguards in place to prevent the same content from being reposted almost immediately.[133] The constant cycle of artists issuing takedown notices, ISPs removing the infringing content, and users reposting the same infringing content can feel like a game of "whack-a-mole."[134] This persistent game of whack-a-mole is cumbersome to smaller artists that lack the resources to constantly monitor and submit takedown notices,[135] and is almost impractical for mega-stars because the amount of

---

[128] *See id.* (explaining that "[b]ecause the factual circumstances and technical parameters may vary from case to case, it is not possible to identify a uniform time limit for expeditious action" under subsection (c)(1)(A)(iii)); *see also* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 521 (S.D.N.Y. 2010).

[129] Emily Blake, *Bruno Mars & Bruce Springsteen Are Latest Artists to Sign DMCA Reform Letter*, MASHABLE (June 22, 2016), http://mashable.com/2016/06/22/dmca-letter-taylor-swift-bruno-mars/#HsalkqiqnOqa.

[130] *Id.*

[131] *Id.*

[132] Jamieson Cox, *The Music Industry Is Begging the US Government to Change Its Copyright Laws*, THE VERGE (Apr. 1, 2016, 9:45 AM), https://www.theverge.com/2016/4/1/11344832/music-industry-copyright-law-change-christina-aguilera-katy-perry.

[133] Devlin Hartline, *Endless Whack-A-Mole: Why Notice-and-Staydown Just Makes Sense*, CPIP (Jan. 14, 2016), https://cpip.gmu.edu/2016/01/14/endless-whack-a-mole-why-notice-and-staydown-just-makes-sense/.

[134] *Id.*

[135] *Id.*

infringing content online is overwhelming.[136] Beyond the DMCA takedown notice, copyright holders have a limited number of remedies to prevent online infringement. The DMCA safe harbor protections afforded to ISPs limit the parties an artist can seek judgment against in a court of law.[137] An artist may choose to file suit directly against the copyright infringer, but this is not likely to stop the incessant infringement that artists are desperate to stop.

One of the more prominent examples of an artist attempting to use the takedown notices to protect their content from online infringers surrounds Taylor Swift's album "1989."[138] In 2014, Universal Music Group (UMG) and Big Machine Records launched a joint effort to remove all online content infringing Swift's "1989."[139] UMG created a group of employees dedicated solely to searching for and issuing takedown notices for any infringing content from the album.[140] Between October of 2014 and March of 2016 the group submitted over 66,000 DMCA takedown notices.[141] Despite this massive effort to remove all infringing content for this one album, there were more than 500,000 links to the album found online and the album was

---

[136] Kevin Madigan, *Despite What You Hear Notice and Takedown is Failing Creators and Copyright Owners*, CPIP (Aug. 24, 2016), https://cpip.gmu.edu/2016/08/24/despite-what-you-hear-notice-and-takedown-is-failing-creators-and-copyright-owners/. "For instance, in 2014, Grammy Award winning composer Maria Schneider testified before Congress that she spends more time sending notices than creating music, and she is hopelessly outmatched by online thieves thanks to the DMCA's feeble protections." Mark Schultz, *Digital Age Changes all the Rules on Intellectual Property*, THE HILL (Nov. 6, 2017, 1:50 PM), http://thehill.com/opinion/finance/358963-digital-age-changes-all-the-rules-on-intellectual-property.

[137] Susan Hong, *Digital Millennium Copyright Act and Protecting Individual Creative Rights: A Proposal for On-Line Copyright Arbitration*, 2 CARDOZO ONLINE J. CONF. RES. 110, 111 (2000).

[138] Kevin Madigan, *Despite What You Hear Notice and Takedown Is Failing Creators and Copyright Owners*, CPIP (Aug. 24, 2016), https://cpip.gmu.edu/2016/08/24/despite-what-you-hear-notice-and-takedown-is-failing-creators-and-copyright-owners/.

[139] *Id.*

[140] *Id.*

[141] *Id.*

illegally downloaded nearly 1.4 million times.[142] Taylor Swift has not stopped trying to remove infringing versions of her album; her team has worked to remove any social media live streams of her concerts as well.[143] Swift's team, appropriately named TAS Rights Management,[144] initially focused primarily on the SMLS app Periscope.[145] The team actively submitted takedown notices for any live-streamed videos from Swift's concerts.[146] This type of infringement is not unique to Taylor Swift, but it is rare that an artist would have the ability to dedicate an entire team to submitting takedown notices.[147] Such a heavy burden seems impractical to place on artists when sites like YouTube and Periscope greatly benefit from the user traffic that infringing content brings to their sites.[148]

III. ALTERNATIVE REMEDIES TO PROTECT ARTISTS FROM SMLS INFRINGEMENT

Operating under the assumption that the DMCA will not be revised in the near future, there are four alternative solutions that would protect artists from SMLS copyright infringement. The first solution presented calls for lawyers to advocate for a change in the interpretation of the DMCA as it is currently written. The last three solutions are directed at the artists. The four suggested solutions to SMLS infringement are as follows: (1) expanding of the interpretation of the safe harbor "knowledge" requirement to place more responsibility on Social Media sites; (2) establishing measures that prohibit cell phone use at shows; (3) dedicating greater resources to issuing takedown notices and filing lawsuits; and (4) embracing SMLS and develop a way to control and monetize live streams of their shows.

A. WORK WITHIN THE EXISTING DMCA TO SHIFT RESPONSIBILITY TO SOCIAL MEDIA SITES

---

[142] *Id.*

[143] *Taylor Swift Cracks Down on Pirating "Periscope" Fans*, TORRENT FREAK (Sep. 25, 2015), https://torrentfreak.com/taylor-swift-cracks-down-on-pirating-periscope-fans-150925/.

[144] TAS stands for Taylor Allison Swift. *Id.*

[145] *Id.*

[146] *Id.*

[147] Madigan, *supra* note 138.

[148] *Id.*

Working within the existing DMCA framework, there may be an alternative view of the knowledge requirement that requires more action on the part of Social Media platforms. To receive safe harbor protections, the DMCA requires that an ISP does not have actual or red flag knowledge of the existence of infringing content on their site.[149] Social Media sites do not actively patrol their sites for infringing content; therefore, they are only required to act once a copyright holder submits a takedown notice.[150] The question artists should be asking is, given how commonly Social Media sites with SMLS capabilities are used for copyright infringement, can Social Media sites continue to hide behind the notion that they have "no actual knowledge" of the infringing content shared on their sites? The court in *UMG* stated that general knowledge of the potential for one's site to be used to share infringing content is not sufficient to satisfy the DMCA knowledge requirement.[151] Yet, given the amount of information that is constantly transmitted from Social Media users back to the host site,[152] if a sudden spike in live streaming occurred in one place at one time, would that trigger the requisite level of knowledge? Taking that one step further, if ISPs could cross reference this type of spike in user activity with concerts and or other major live performance dates, would that establish red flag or possibly even actual knowledge? This type of data analysis to identify patterns that correlate to certain user activity can be compared to the pattern recognition the SEC analytics software uses to identify insider trading.

Since 2014, the SEC has been using two analytics programs to analyze data and identify patterns.[153] The software

---

[149] 17 U.S.C § 512(c).

[150] *Id.*

[151] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1022 (9th Cir. 2013).

[152] David Nield, *You Probably Don't Know All the Ways Facebook Tracks You*, FIELD GUIDE (June 8, 2017, 10:45 AM), https://fieldguide.gizmodo.com/all-the-ways-facebook-tracks-you-that-you-might-not-kno-1795604150.

[153] *SEC—Data Analytics Key to Unlocking Fraud Schemes*, MANATT (Mar. 24, 2017), https://www.manatt.com/Insights/Articles/2017/SEC%E2%80%94Data-Analytics-Key-to-Unlocking-Fraud-Schemes.

"identifies links between individuals and entities by connecting pieces of information from multiple data sources."[154] The SEC has opened nine investigations based on its software's pattern recognition since 2014.[155] This pattern recognition could be instituted in other contexts to achieve a similar goal; for example, within the Facebook framework to detect spikes in user activity. If it is assumed that Facebook and other Social Media sites can no longer claim that they lack knowledge and they cannot claim safe harbor protection, it would be imperative for them to establish a new means of stopping infringers. Instituting a variation of the SEC pattern recognition software would give Social Media sites the ability to identify mass infringement activity and to remove those live streams. This shift of responsibility to Social Media sites is likely only possible if it is determined that they do in fact have actual or red flag knowledge of the infringement on their site, thus stripping them of their DMCA liability protection.

Social Media sites like Facebook are constantly collecting information on their users, so it is hardly practical to allow them to say they have no knowledge of infringing content. The case law is very clear that an ISP cannot exhibit willful blindness and receive safe harbor protection under the DMCA, especially when the ISP increases its own financial gains.[156] Features like Facebook Live attract users to Facebook's site, and the greater the number of users, the higher the ad prices charged by Facebook.[157] If the user infringes on Taylor Swift's copyright protected material by live streaming her concert, then a connection can be shown between Facebook's financial position and the infringement. Combining the financial gain from advertisements garnished from higher user activity with the red flag knowledge based on spikes in user activity, Social Media sites should not be able to claim DMCA safe harbor protections because they do not meet the necessary requirements.

---

[154] *Id.*

[155] *Id.*

[156] *UMG Recordings*, 718 F.3d at 1023.

[157] *See generally How Ad Billing Works on Facebook*, FACEBOOK BUS., https://www.facebook.com/business/help/716180208457684?helpref=page_content (last visited Apr. 10, 2018) (explaining that advertisers are "charged for the number of clicks or the number of impressions your ad received).

B. CREATE PHONE-FREE ZONES AT SHOWS

Artists may choose to take matters into their own hands by prohibiting cellphone use at their shows. In 2014, the California based startup Yondr began offering a way for entertainment artists to create cellphone-free zones.[158] Before attendees enter the venue, they are instructed to put their phone into a Yondr pouch.[159] Attendees keep possession of their phone, but the phone remains locked inside the pouch while they are inside the venue's phone-free zone.[160] If an attendee needs access to their phone, they can step outside the phone-free zone and the pouch can be unlocked.[161] Many singers and comedians, including Alicia Keys, Guns N' Roses, Maxwell, Dave Chappelle, and Donald Glover, have instituted phone-free zones at their shows.[162] These phone-free shows offer artists a greater sense of "creative security."[163] This increased sense of security stems from the alleviation of any fear that a video of the show will be leaked online.[164] Without access to their phones, attendees have no way of live streaming the show. This upfront investment in Yondr pouches would alleviate the need to expend funds to monitor for infringing content shared via Social Media.

C. DEDICATE MORE RESOURCES TO PREVENT INFRINGEMENT

Following Taylor Swift's lead, another option for entertainment artists is to be more aggressive in their monitoring for Internet infringement.[165] For SMLS issues, artists may look to

---

[158] Morrissey, *supra* note 2.

[159] *See How It Works*, YONDR, https://www.overyondr.com/howitworks/ (last visited Apr. 10, 2018).

[160] *Id.*

[161] *Id.*

[162] Morrissey, *supra* note 2.

[163] *Lock Screen: At These Music Shows, Phones Go in a Pouch and Don't Come Out*, NPR (July 5, 2016), http://www.npr.org/sections/alltechconsidered/2016/07/05/483110284/lock-screen-at-these-music-shows-phones-go-in-a-pouch-and-dont-come-out.

[164] *Id.*

[165] Ernesto, *Taylor Swift Cracks Down on Pirating "Periscope" Fans*, TORRENT FREAK (Sept. 25, 2015), https://torrentfreak.com/taylor-swift-cracks-down-on-pirating-periscope-fans-150925/.

allocate financial resources to patrolling Social Media sites during concerts. The DMCA was written to protect artists from online copyright infringement, but with this legislative protection comes the responsibility to monitor the Internet for infringement. Because Facebook, Instagram, and other Social Media sites are complying with the DMCA, it shifts the burden of discovery to artists. If ISPs are fully in compliance with their responsibilities as laid out by the law, then it may be impractical to expect Social Media platforms to patrol their sites more aggressively. Therefore, artists wanting to prevent online infringement of their content should consider allocating a much more significant amount of both time and resources to a continuous monitoring effort. However, this solution assumes that an artist has the financial means to support such a course of action.

D. ADOPT A BUSINESS MODEL THAT CONTROLS SMLS MONETIZATION

As the saying goes, "if you can't beat them, join them." Maybe it is time artists develop a business model that allows them to harness SMLS for their own financial gain instead of trying to fight off infringing streamers. If it is assumed that the DMCA offers the full extent of legal remedies available to artists with online copyright infringements, artists that find this to be an insufficient or ineffective solution must change how they evaluate the problem. An artist could invest excessive amounts of money attempting to stop Social Media users from live streaming a poor-quality version of the concert or they could produce their own live stream and take the power away from infringers. A survey by New York Magazine found that "nearly half of live video audiences would pay for live, exclusive, on-demand video from a favorite team, speaker, or performer."[166] Additionally, the survey revealed that sixty-seven percent of live video viewers reported that they were "more likely to buy a ticket to a concert or event after watching a live video of that event or a similar one."[167] Facebook Live, like other Social Media sites, makes it possible for users

---

[166] Caroline Golum, *Live Video ROI: 4 Strategies for Live Video Monetization*, LIVESTREAM, https://livestream.com/blog/live-video-monetization.

[167] Caroline Golum, *62 Must-Know Live Video Streaming Statistics*, LIVESTREAM, https://livestream.com/blog/62-must-know-stats-live-video-streaming.

hosting a live stream to profit from mid-stream advertisements once a SMLS surpasses a set viewer threshold.[168] Just as artists were forced to pivot when their audience shifted from purchasing CDs of their albums to downloading them from iTunes, it may be time for artists to shift from an exclusively in-person concert model to an in-person/online hybrid model.

CONCLUSION

Today, there are more than three billion active Social Media users globally.[169] This amounts to nearly forty percent of the world's population.[170] In the United States, seven in ten Americans are Social Media users.[171] The numbers are staggering, but the reality is undeniable—Social Media has embedded itself in the fabric of American life. The DMCA and the protections it established were codified before the age of Social Media began. Although ISPs do comply with the takedown requests they receive, given the sheer number of takedown requests, it is unrealistic to believe that the Internet of 2018 could be stripped of all or even most infringing content. Currently the DMCA does not provide artists with adequate protection.

There are several potential solutions to the problem of online infringement via SMLS. Perhaps the most radical of the alternatives presented is to shift some of the burden back onto ISPs, specifically Social Media sites. Safe harbor protections can only be afforded to an ISP that does not have actual or red flag knowledge of the infringement. Given the expansive power of Social Media sites to track user activity, it could be suggested that Social Media sites like Facebook do have some form of red flag knowledge. Even if they do not have "knowledge" within the current court interpreted definition, they may still have the

---

[168] Akshay Chandra, *Earn Monetization Revenue Through Facebook LiveStreaming*, VIDOOLY (Apr. 6, 2017), https://vidooly.com/blog/earn-monetization-revenue-though-facebook-livestreaming.

[169] Brett Williams, *Social Media Reaches 3 Billion Users Globally, Says New Report*, MASHABLE (Aug. 7, 2017), http://mashable.com/2017/08/07/3-billion-global-social-media-users/#eYAb0.fSEaqG.

[170] *Id.*

[171] *Social Media Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/social-media/.