MAVRIX V. LIVEJOURNAL: UNSAFE HARBORS IN THE AGE OF SOCIAL MEDIA

Katherine Burkhart†

I. INTRODUCTION

In recent decades, the reach and influence of social media providers have transformed online communication. With this development, however, the sheer amount of user-submitted content on these platforms has also grown, along with questions about liability for that content. When users break the law by, among other things, infringing copyrights, to what extent should the Internet service providers (ISPs) hosting that content be held liable for that infringement? In the Digital Millennium Copyright Act (DMCA), a statute that largely predates the rise of social media, Congress attempted to insulate ISPs from liability for content hosted "at the direction" of their users via "safe harbor" provisions.[1] Contemporary social media practices, however, often make it difficult to articulate and differentiate the roles of users and hosts.

In *Mavrix v. LiveJournal*, the Ninth Circuit reasoned that the central inquiry for safe harbor analysis was the nature of the relationship between a social media network and the individuals screening that network's content.[2] If moderators work on a social media network's behalf, the Ninth Circuit contended, that network may incur liability for infringing material that is ultimately published.

This Note asserts that the Ninth Circuit's approach in *LiveJournal* presents multiple problems. First and foremost, this approach is not supported by the statutory text. What is more, it provides incentives for social media providers to loosen their moderation practices, in conflict with the doctrine's statutory rationale and at odds with current Congressional conceptions of responsible social media oversight. In the age of online harassment and fake news, an ISP's incentive to take a "hands-off" approach can be a dangerous one.

Part II of this Note provides a foundation for understanding the relevant "safe harbor" provision offered to protect ISPs from liability for copyright infringement. Part III summarizes the district and circuit court's competing

DOI: https://doi.org/10.15779/Z38ZS2KD15

† J.D. Candidate, 2019, University of California, Berkeley, School of Law.

1. 17 U.S.C. § 512 (2012).
2. Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045 (9th Cir. 2017).

approaches to assessing eligibility for these provisions in *Mavrix v. LiveJournal*. Part IV argues that the Ninth Circuit's understanding of ISP eligibility for safe harbor protection is fundamentally at odds with the underlying statutory text and the incentives that text was intended to create.

II. BACKGROUND

A. THE DIGITAL MILLENNIUM COPYRIGHT ACT

In 1998, Congress enacted the DMCA to "update domestic copyright law for the digital age."[3] To ensure "that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand," Title II of the Act reshaped the liability landscape for ISPs whose platforms might publish infringing material.[4] Specifically, the DMCA instituted four "safe harbors" to limit ISP liability for such infringement.[5]

In providing safe harbors, the DMCA sought to balance the interests of ISPs, copyright holders, and platform users.[6] The advent of the Internet, Congress recognized, made copying and disseminating digital content easier than ever before, leaving copyright owners more vulnerable to infringement.[7] Congress sought to protect copyright owners. At the same time, Congress also sought to avoid a chilling effect on ISP innovation. Congress recognized that such entities are necessarily exposed to the danger of copyright infringement liability "in the ordinary course of their operations."[8]

With the balancing it provided, Congress intended for the DMCA to preserve "strong incentives for service providers and copyright owners to cooperate" in identifying and addressing online infringements.[9] Each of the DMCA's safe harbors, for example, is only available to ISPs that implement a protocol for removing users who repeatedly infringe, inform users of this protocol, and accommodate "standard technical measures" copyright holders use to guard their work.[10]

3. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012).
4. S. REP. NO. 105-190, at 2 (1998).
5. 17 U.S.C. § 512 (2012).
6. H. R. REP. NO. 105-551, pt. II, at 21 (1998).
7. S. REP. NO. 105-190, at 8 (1998).
8. *Id.*
9. *Id.* at 20.
10. 17 U.S.C. § 512(i) (2012).

B. "AT THE DIRECTION OF USERS" SAFE HARBOR

While the DMCA provides four safe harbors[11] for ISPs, only the third—the provision for infringing content "residing on systems or networks at the direction of the [ISP's] users"[12]—is relevant here. Section 512(c) provides that an ISP "shall not be liable . . . for infringement of copyright by reason of storage at the direction of a user of material" if the ISP meets three criteria.[13] Specifically, to be eligible for this safe harbor, an ISP must: have no knowledge of the infringing content,[14] gain no direct financial benefit from infringement[15] it had the right and ability to control,[16] and act "expeditiously to remove or disable access to"[17] infringing material upon learning of its presence.[18] The knowledge provision applies to both "actual knowledge," in which an ISP knows of a particular instance of infringement, as well as "red flag knowledge," in which an ISP is aware of conditions "that would have made the specific infringement 'obvious' to a reasonable person."[19] ISPs must additionally adopt "notice and takedown" procedures for removing infringing material after notification by a rights holder.[20]

The threshold question for this safe harbor's applicability is whether infringing material on an ISP ended up there at the direction of the *user*, as opposed to the direction of the ISP *itself*.[21] While the statute does not define

---

11. 17 U.S.C. § 512(a) (2012) ("[t]ransitory digital network communications"); *id.* § 512(b) ("system caching"); *id.* § 512(c) ("information residing on systems or networks at direction of users"); *id.* § 512(d) ("information location tools").

12. *Id.* § 512(c).

13. *Id.*

14. *See id.*

15. *See id.*

16. *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 38 (2d Cir. 2012) (holding that the "right and ability to control" infringing activity "requires something more than the ability to remove or block access to materials posted on [an ISP's] website"). *But see* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001), *as amended* (Apr. 3, 2001), *aff'd sub nom.* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) ("The ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.").

17. S. REP. NO. 105-190, at 44 (1998).

18. *See* 17 U.S.C. § 512(c)(1)(C) (2012).

19. Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013); *see also Viacom*, 676 F.3d at 31 ("The difference between actual and red flag knowledge is [ ] not between specific and generalized knowledge, but instead between a subjective and an objective standard . . . . Both provisions do independent work, and both apply only to specific instances of infringement.").

20. *See* S. REP. NO. 105-190, at 45 (1998) ("This 'notice and takedown' procedure is a formalization and refinement of a cooperative process that has been employed to deal efficiently with network-based copyright infringement.").

21. *See* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1048 (9th Cir.

the concept of storing infringing information "at the direction of the user," legislative history and case law provide some guidance for determining whether information was stored at the direction of a user or the ISP. The DMCA's legislative history suggests that content "resid[ing] on [the ISP's] system or network . . . through [the ISP's] own acts or decisions" falls outside of § 512(c)'s liability protection.[22]

Courts have accordingly held that content is kept at the direction of a user if the ISP was entirely uninvolved with infringing material being made accessible on its platform.[23] But courts have not disqualified ISPs from safe harbor protection on the basis of their involvement in uploading content, so long as the ISP's actions were "narrowly directed" at enhancing a post's accessibility.[24] Accessibility-enhancing actions identified thus far are largely automated processes,[25] but the Ninth Circuit has held that "some manual service provider activities that screen for infringement" may also be within § 512(c)'s purview as "accessibility-enhancing" actions.[26]

ISP screening for copyright infringement is not required, and the DMCA makes clear that an ISP will not be held liable for failing to monitor "its service or affirmatively seek[] facts indicating infringing activity."[27] The question is whether such screening can trigger ISP liability by removing material from the § 512(c) safe harbor on the basis that it is not stored at the direction of the user, but rather by the ISP itself. In *Mavrix v. LiveJournal*, the Ninth Circuit considered the extent of an ISP's ability to screen for infringement within § 512(c) immunity.[28]

III. CASE SUMMARY

A. FACTS

LiveJournal is an online platform "willfully blurring the lines between blogging and social networking."[29] LiveJournal users can operate free online

2017).

22. H. R. REP. NO. 105-551, at 43 (1998).

23. *See* UMG Recordings, Inc. v. Veoh Networks, Inc., 620 F. Supp. 2d 1081, 1092 (C.D. Cal. 2008).

24. *See id.*

25. *See Mavrix*, 873 F.3d at 1056; *see also UMG Recordings*, 718 F.3d at 1020 (describing accessibility-enhancing processes as those in which the ISP "does not actively participate in or supervise uploading, [or] preview or select the files before the upload is completed").

26. *Mavrix*, 873 F.3d at 1056.

27. 17 U.S.C. § 512(m)(1) (2012).

28. *See Mavrix*, 873 F.3d at 1056.

29. *Our Company*, LIVEJOURNAL, https://www.livejournal.com/about [https://perma.cc/5GCU-FK8K].

journals and join "communities" to share themed content with other users.[30] Some LiveJournal communities elect to be moderated groups, in which moderators (users who volunteer for the role) accept or reject content submitted by the community's general membership.[31] When a user submits a post to a moderated group, it is uploaded to LiveJournal's servers and placed in a queue to be inspected by a moderator.[32] Moderators cannot edit a post; they can only reject or accept a user's submission wholesale.[33]

"Oh No They Didn't!" (ONTD) is a moderated LiveJournal community focused on pop culture and celebrity gossip.[34] It is the most popular community on LiveJournal, with nearly 100,000 members in 2017.[35] Due to the community's popularity, LiveJournal hired one of ONTD's volunteer moderators to work as "the community's full time 'primary leader' " in 2010.[36] Other moderators, however, remained active on a volunteer basis.[37]

Mavrix Photographs, LLC (Mavrix) is a "premier entertainment industry image source."[38] Mavrix's business model largely consists of licensing "breaking" photos to celebrity magazines.[39] The dispute in this case concerned seven ONTD posts featuring Mavrix's photos between 2010 and 2014.[40]

Some of these posted photos were watermarked, either with the URL for Mavrix's website or a generic watermark.[41] LiveJournal's technological limits made it impossible to determine which moderator approved any of these posts.[42] Mavrix did not notify LiveJournal of the infringements via the website's notice and takedown procedure.[43] LiveJournal was notified of—and removed—the infringing images when Mavrix filed suit.[44]

30. *See* Mavrix Photographs LLC v. LiveJournal, Inc., No. SACV 13-00517-CJC, 2014 WL 6450094, at *1 (C.D. Cal. Sept. 19, 2014), *rev'd*, 853 F.3d 1020 (9th Cir. 2017), *opinion amended and superseded*, 873 F.3d 1045 (9th Cir. 2017), and *rev'd*, 873 F.3d 1045 (9th Cir. 2017).

31. *See id.*

32. *See id.*

33. *See id.*

34. *See Oh No They Didn't!*, LIVEJOURNAL, http://ohnotheydidnt.livejournal.com [https://perma.cc/EL6C-CNL5].

35. *See* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1050 (9th Cir. 2017).

36. *Id.*

37. *See id.*

38. MAVRIX ONLINE, http://www.mavrixonline.com [https://perma.cc/E6GY-2RFT] (last visited Dec. 21, 2018).

39. *Mavrix*, 873 F.3d at 1050.

40. *See Mavrix*, 2014 WL 6450094, at *2.

41. *See Mavrix*, 873 F.3d at 1050.

42. *See id.*

43. *See id.*

44. *See id.*

B. PROCEDURAL HISTORY

Mavrix brought an infringement action against LiveJournal in the United States District Court for the Central District of California.[45] Mavrix argued that the storage of its photos was not done at the direction of a *user*, but at the direction of LiveJournal itself.[46] Citing *Capitol Records, LLC v. Vimeo*,[47] Mavrix argued that each of ONTD's moderators was an agent of LiveJournal "for purposes of their work on ONTD."[48] That is, when a moderator "approved" the infringing posts for publication on ONTD, he or she did so on LiveJournal's behalf, precluding LiveJournal from § 512(c)'s safe harbor protection.[49] The district court, however, rejected this "agency" argument, reasoning that § 512(c)'s "at the direction of the user" was "clearly meant to cover more than mere electronic storage lockers."[50] The fact that all ONTD posts were subject to moderation before publication did not make those posts less at the direction of users "under the 'broad' statutory language of the DMCA."[51] Moreover, in the absence of DMCA notice, the court noted, LiveJournal would have no actual *or* red flag knowledge that candid "paparazzi"-style photos were infringing without lengthy investigation.[52] The district court granted LiveJournal's motion for summary judgment, and Mavrix appealed the decision.[53]

On appeal, the Ninth Circuit reversed the district court's summary judgment, concluding that agency principles *did* apply to this dispute, and could thus expose LiveJournal to liability. In doing so, the court reasoned that the *posting* of infringing content is the "critical inquiry," not the *submission* of that

45. *See Mavrix,* 2014 WL 6450094, at *1.

46. Plaintiff Mavrix Photographs LLC's Memorandum in Opposition to Defendant LiveJournal Inc.'s Motion for Summary Judgment at 2, Mavrix Photographs LLC v. LiveJournal, Inc., No. SACV 13-00517-CJC, 2014 WL 6450094 (C.D. Cal. Sept. 19, 2014), 2014 WL 10209534, at *2 [hereinafter Mavrix Memorandum].

47. 972 F. Supp. 2d 500, *amended on reconsideration in part*, 972 F. Supp. 2d 537 (S.D.N.Y. 2013) ("To determine whether these employee-uploaded videos may be deemed to have been stored 'at the direction of a user,' the Court must determine whether, under traditional principles of agency law, Vimeo's employees stored their videos as independent users or rather on behalf of the company as Vimeo staff.").

48. Mavrix Memorandum, *supra* note 46, at 8.

49. *Id.* at 7 ("An agency relationship may be informally created. No particular words are necessary, nor need there be consideration. All that is required is conduct by each party manifesting acceptance of the relationship whereby one of them is to perform work for the other under the latter's direction.").

50. *Mavrix*, 2014 WL 6450094, at *5 (quoting UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013)).

51. *Id.*

52. *Id.* at *6.

53. *See id.* at *9.

content.[54]

In order to determine whether LiveJournal (as opposed to its users) facilitated this "posting," the court applied the common law of agency. In doing so, the court reasoned that the DMCA may shield ISPs from liability "for the passive role they play when users submit to them" under § 512(a)[55]—a different safe harbor. Conversely, the DMCA protects service providers that play a role in making users' material publicly accessible on its site under § 512(c).[56] The court reversed the district court's summary judgment and remanded the case for trial, concluding that agency principles *did* apply to this dispute and could expose LiveJournal to liability for posts moderated by its agents.[57] The court additionally instructed that, on remand, the district court must determine "whether the moderators' acts were merely accessibility-enhancing activities or whether instead their extensive, manual, and substantive activities went beyond the automatic and limited manual activities we have approved as accessibility-enhancing."[58]

The court went on to explain that an agency relationship is created "when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf . . . and the agent manifests assent or otherwise consents so to act."[59] This can occur with the delegation of "actual authority" to an agent, in which the principal affirmatively agrees to allow the agent to act on his behalf.[60] This relationship is also created by delegation of "apparent authority," in which the principal never outright *says* that his agent has authority to act on his behalf, but makes some other manifestation that a third party would reasonably understand as authorization

54. Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1053 (9th Cir. 2017) ("[This central inquiry] turns on the role of the moderators in screening and posting users' submissions and whether their acts may be attributed to LiveJournal.").

55. *Id.* Section 512(a) of the DMCA, however, provides no such distinction between submission and posting. Additionally, "[o]n the face of the statute and in the legislative history, it's quite clear that section 512(a) is meant to cover user-initiated, end-to-end routing of information across a provider's network. A residential broadband access provider [for example] is the paradigmatic section 512(a) provider." Annemarie Bridy, *Is Bad News for LiveJournal Bad News for the DMCA Safe Harbors? (Post 1 of 3)*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Apr. 9, 2017), http://cyberlaw.stanford.edu/blog/2017/04/bad-news-livejournal-bad-news-dmca-safe-harbors-post-1-3 [https://perma.cc/5AFW-DDUK].

56. *See* Mavrix Photographs LLC v. LiveJournal, Inc., No. SACV 13-00517-CJC, 2014 WL 6450094, at *5 (C.D. Cal. Sept. 19, 2014).

57. *See Mavrix*, 873 F.3d at 1049.

58. *Id.*

59. *Id.* at 1054 (quoting RESTATEMENT (THIRD) OF AGENCY § 3.01 (AM. LAW INST. 2006)).

60. RESTATEMENT (THIRD) OF AGENCY § 3.01 (AM. LAW INST. 2006).

of the agent.[61]

Regardless of how authority was delegated, however, a principal fundamentally enjoys some level of control over his agent in an agency relationship.[62] For purposes of the *Mavrix* dispute in particular, the Ninth Circuit explained, the record suggested that LiveJournal "maintains significant control over ONTD and its moderators,"[63] providing substantive instruction and even removing moderators through the community's paid "primary leader."[64] On the other hand, the court noted, moderators are "free to leave and go" as they wish, and individual moderators are able to reject user post submissions for a number of reasons not including those in LiveJournal or ONTD's rules, "call[ing] into question the level of control LiveJournal exercised over the moderators."[65] The Ninth Circuit made this very uncertainty the basis of its "agency" approach to safe harbor analysis, instructing an articulation of this relationship on remand.

IV. ANALYSIS

Not only does the Ninth Circuit's application of "agency" law in this manner run afoul of existing case law on the matter, but it is inconsistent with Congressional intent in multiple contexts as well.

A. CASE LAW DOES NOT SUPPORT THE NINTH CIRCUIT'S "AGENCY" APPLICATION

While agency has come into play in federal copyright cases before, the rare instances in which it has been applied to determine whether content was stored "at the direction of the user" bear little resemblance to the facts of *Mavrix v. LiveJournal*.

In asserting its agency argument, Mavrix relied heavily on *Capitol Records, LLC v. Vimeo, LLC*.[66] In that case, the District Court for the Southern District

61. *Id.* at § 3.03; *see also* Hawaiian Paradise Park Corp. v. Friendly Broad. Co., 414 F.2d 750, 756 (9th Cir. 1969) ("The principal's manifestations giving rise to apparent authority may consist of direct statements to the third person, directions to the agent to tell something to the third person, or the granting of permission to the agent to perform acts and conduct negotiations under circumstances which create in him a reputation of authority in the area in which the agent acts and negotiates.").

62. *See* Hollingsworth v. Perry, 133 S. Ct. 2652, 2657 (2013) (discussing a principal's control over an agent as the "basic feature[ ] of an agency relationship"); United States v. Bonds, 608 F.3d 495, 505 (9th Cir. 2010) (describing "the extent of control exercised" by the principal as the "essential ingredient" of an agency relationship).

63. *Mavrix*, 873 F.3d at 1055.

64. *Id.*

65. *Id.*

66. 972 F. Supp. 2d 500 (S.D.N.Y. 2013).

of New York applied agency law to demystify § 512(c)'s "at the direction of a user" language where moderators were involved with the publishing of infringing content.[67] But *Capitol Records* addressed drastically different facts than *Mavrix*. In *Capitol Records*, ten infringing videos were published on Vimeo (an online video-sharing platform) by Vimeo employees[68] who, much like LiveJournal's moderators, had access to "Moderator Tools" to monitor and restrict prohibited content.[69] The infringing material in that case, however, unlike the infringing photos in *Mavrix*, was indisputably uploaded directly by the employee-moderators *themselves*. The only question of "agency" at issue in *Capitol Records* was whether the same set of individuals were acting on behalf of their employer or on their own behalf when uploading the infringing videos.[70] Their moderating authorities were incidental to their act of infringement, while LiveJournal's moderators, if "agents" of the ISP, are liable as conduits for someone else's infringement. While the facts of *Mavrix* and *Capitol Records* are similar at first blush, the application of agency law in each is meaningfully different.

The Ninth Circuit also pointed to *Columbia Pictures Industries, Inc. v. Fung*,[71] a similarly distinguishable case, as precedent for applying common law agency principles to questions of ISP liability for moderators' actions.[72] The defendant in *Fung* operated a "torrent" website, through which users could freely and illegally download copyrighted material.[73] The nature of such "peer-to-peer" sharing sites, however, is such that these files are stored on individual users' computers instead of the site's central servers.[74] In *Fung*, the defendant's website did not store or offer for download any content.[75] Instead, users could only download files that served as "call numbers" of sorts to locate the actual

67. *Id.* at 518.

68. *See id.* ("It is undisputed that ten of the [videos in suit] were uploaded by users who were at the time, or later became, Vimeo employees.").

69. *See id.* at 528.

70. *See id.* at 518 ("[T]he court must determine whether, under traditional principles of agency law, Vimeo's employees stored their videos as independent 'users' or rather on behalf of the company as Vimeo staff.").

71. No. CV 06-5578 SVW(JCX), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009), *aff'd in part as modified*, 710 F.3d 1020 (9th Cir. 2013).

72. *See* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1053 (9th Cir. 2017).

73. *See Fung*, 2009 WL 6355911, at *1.

74. *Id.*

75. *See* Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1025–26 (9th Cir. 2013) ("Although a centralized [peer-to-peer] network has similarities with a client-server network, the key difference is that the indexing server does not store or transfer the content. It just tells users which other peers have the content they seek. In other words, searching is centralized, but file transfers are peer-to-peer.").

content to be exchanged.[76] These files allowed a locally stored application to locate content on other computers in the network, beginning the illegal download.[77] The District Court for the Central District of California held that this technology was categorically ineligible for § 512(c)'s safe harbor, as the infringing content did "not pass through or reside on Defendants' system."[78]

In *Fung*, agency principles were not used to make determinations about DMCA safe harbor eligibility. Rather, agency analysis was solely used to determine if the defendant was liable for contributory infringement by moderators. The torrent site in that case offered forums for users seeking specific files.[79] These forums were managed by moderators who "assisted users seeking to download files or provided links to other websites containing the requested items."[80] Thus, agency principles were applied only to analysis of moderators' roles in actively assisting with forum users' infringement,[81] not to analysis of whether posting was done at the users' direction for purposes of the § 512(c) safe harbor. The court held that the moderators were the defendant's agents and granted summary judgment against the defendant on the issue of inducement liability for copyright infringement.[82]

The Ninth Circuit's *Fung* decision does little to bolster its opinion in *Mavrix*. Unlike the district court, the Ninth Circuit in *Fung* found that "sometimes . . . torrents [were] uploaded by users of [defendant's] sites, while other torrents [were] collected for storage by [defendant's] websites themselves. *The former situation would be at least facially eligible for the* [*§ 512(c)*] *safe harbor, assuming the other criteria are met.*" [83] Accepting the lower court's classification of moderators as the defendant's "agents," the Ninth Circuit signaled that such a relationship did not outright preclude § 512(c) protection for lack of storage "at the direction of the user."[84] The *Fung* defendant was ineligible for the safe harbor not because infringing content was made available at the direction of anyone other than users, but because inducement of others' infringement suggested red flag knowledge that the content was itself

76. *See Fung*, 2009 WL 6355911, at *2.

77. *See id.*

78. *Id.* at *16.

79. *See id.* at *13.

80. *Id.* ("All of these statements demonstrate that there was an active role played by the [moderators] of the websites within the forum, encouraging and providing technical assistance for users seeking to engage in infringing activities.").

81. This was alleged to be inducement of infringement outside of any statutory safe harbor. *See id.*

82. *See id.* at *19.

83. Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1042–43 (9th Cir. 2013) (emphasis added).

84. *Id.* at 1043.

infringing.[85] Moreover, even if this were not the case, the DMCA's legislative history expressly excluded ISPs like the torrent sites in *Fung* from § 512(c) protection.[86] To characterize *Fung* as analogous to *Mavrix* is to misapply both the facts of *Fung* and Congress' intent behind the DMCA.

As Mavrix conceded in its opening brief, only one case in the Ninth Circuit, *UMG Recordings, Inc. v. Shelter Capital Partners LLC*,[87] has assessed the meaning of § 512(c)'s "at the direction of users" language.[88] In *UMG*, the Ninth Circuit held that *automatic* access-facilitating activities—in which ISPs do not "actively participate in or supervise file uploading"—allow infringement to remain at users' direction.[89] However, the court's reasoning did not preclude manual processes like moderation from this categorization.[90] Elsewhere in the court's *UMG* opinion, it opted for a broad interpretation of § 512(c) that would impose "no limitation on [an ISP's] ability to modify user-submitted material to facilitate storage and access."[91] "If Congress had intended a narrower scope," the court noted, "it would have said so expressly and unambiguously, as it did in the narrower definition of 'service provider.' "[92]

Moreover, § 512(c) details an extensive notice and takedown procedure for copyright owners to inform ISPs of infringement on their platforms, through which ISPs are prompted to remove access to infringing content.[93] Against a

---

85. *See id.*

> [T]he record is replete with instances of Fung actively encouraging infringement, by urging his users to both upload and download particular copyrighted works, providing assistance to those seeking to watch copyrighted films, and helping his users burn copyrighted materials onto DVDs. The material in question was sufficiently current and well-known that it would have been objectively obvious to a reasonable person that the material solicited and assisted was both copyrighted and not licensed to random members of the public.

86. *See* S. REP. NO. 105-190, at 48–49 (1998) (explaining that "pirate directories" are outside scope of safe harbor "because the infringing nature of such sites would be apparent from even a brief and casual viewing [and such sites] do not follow the routine business practices of legitimate service providers").

87. 718 F.3d 1006 (9th Cir. 2013).

88. Appellant's Opening Brief at 31, Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1053 (9th Cir. 2017), 2015 WL 13236719, at *31 [hereinafter Appellant's Opening Brief].

89. *UMG Recordings*, 718 F.3d at 1020.

90. *See id.* at 119 (holding defendant ISP's encoding process within the §512(c) safe harbor when such processes "are used to facilitate access to content submitted to [the ISP's] website").

91. *Id.*; *see also* Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1147 (N.D. Cal. 2008) (holding defendant ISP's encoding process within the § 512(c) safe harbor when such processes "are used to facilitate access to content submitted to [the ISP's] website").

92. *UMG Recordings*, 718 F.3d at 1020.

93. *Id.* at 1018.

narrow interpretation of § 512(c), the court in *UMG* reasoned that this "carefully considered . . . protocol, and [§ 512(c)'s] attendant references to 'disabl[ing] access' to infringing materials would be superfluous[94] if we accepted [a] constrained reading of the statute."[95] That is, these provisions are predicated on the understanding that ISPs will provide (and sometimes disable) access to users' (potentially infringing) material. It cannot, then, be the case that control over access alone precludes safe harbor protection.[96]

The only Ninth Circuit case evaluating § 512(c)'s threshold language points to a scope broad enough to contain an agency relationship because an ISP's power to disable access would include the power to moderate content on its own platform. Indeed, compliance with notice and take-down procedures would require that ISPs exercise this power. Most tellingly, at no point in *UMG* is "agency" mentioned as a mechanism for determining if content was stored at the direction of users. Thus, there is no precedent for applying agency law as the Ninth Circuit did in *Mavrix*.

B. THE NINTH CIRCUIT'S APPROACH IS AT ODDS WITH CONGRESSIONAL INTENT IN ENACTING THE DMCA

With the DMCA's construction and policy goals in mind, agency law maps poorly onto ISP liability analysis and directs courts to the wrong inquiry. First, the Ninth Circuit's focus immediately diverged from the statutory language: while § 512(c) focuses specifically on actions of ISP *users*,[97] the Ninth Circuit opted instead to prioritize the *ISP*'s role in infringing content.[98] Second, the DMCA's legislative history explicitly anticipates ISP use of "human editors and reviewers" to monitor content on their platforms,[99] indicating that such monitoring does not disqualify ISPs from the § 512(c) safe harbor.

The Ninth Circuit's application of agency principles would incentivize ISPs to cut back on—or even eliminate—content moderation. This conflicts not only with the DMCA's stated goal of promoting cooperation between

94. *See* Greenwood v. CompuCredit Corp., 615 F.3d 1204, 1209 (9th Cir. 2010), *rev'd and remanded*, 565 U.S. 95 (2012) ("We must, if possible, interpret a statute such that all its language is given effect, and none of it is rendered superfluous.").

95. *UMG Recordings*, 718 F.3d at 1018 (emphasis added).

96. *See id.* ("Indeed, it is not clear how copyright holders could even discover infringing materials on service providers' sites to notify them as the protocol dictates if § 512(c) did not contemplate that there would be access to the materials.").

97. *See* 17 U.S.C. § 512(c)(1) (2012) (providing that ISPs are not liable "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the ISP.").

98. *See* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1053 (9th Cir. 2017) ("[The critical inquiry] turns on the role of the moderators in screening and posting users' submissions and whether their acts may be attributed to LiveJournal.").

99. S. REP. NO. 105-190, at 48–49 (1998).

copyright owners and ISPs,[100] but also with the DMCA's knowledge standard. This standard, the legislative history explains, "should not be applied in a manner which would create a disincentive to the development of directories which involve human intervention."[101]

In the absence of actual knowledge of infringement, Congress envisioned that an ISP should be assumed aware of infringement "only with respect to pirate sites or in similarly obvious and conspicuous circumstances, and not simply because the [ISP] viewed an infringing site during the course of assembling the directory."[102] To proceed otherwise is to undermine the statute's structure as applying to content published at the direction of users. Discouraging ISPs from moderating content on their platforms serves the interest of neither ISPs nor copyright holders. If agency law is applied to ISP moderators as the Ninth Circuit suggests, courts risk undermining the DMCA's fundamental framework and undercutting the very "certainty" the DMCA's safe harbors were adopted to establish for ISPs in the first place.

Though the technology available to ISPs has improved drastically since 1998, the need for ISPs to be able to monitor their platforms remains. Copyright holders like Mavrix could certainly argue that Congress could not have fully appreciated the technological capabilities today's ISPs would have for purposes of filtering content. Passage of the DMCA in the first place was largely predicated on the assumption that ISPs could not realistically screen *everything* with absolute precision;[103] this assumption remains true today. Regardless of whether this is due to a lack of automated monitoring technology (as was the case in 1998) or the resources and time required to make complete human monitoring sustainable (which many ISPs lack today), some semblance of immunity is required to avoid chilling ISP operation and innovation.

If Congress indeed deemed mere moderation enough to preclude safe harbor protection, other statutory provisions in the DMCA would be rendered irrelevant. Copyright holders could argue further that an ISP in LiveJournal's position would *have* to have some knowledge of infringement, given that every user submission was manually approved or rejected by a moderator.[104] However, the presence of § 512(c)'s notice and takedown provisions indicate that Congress did not envision mere moderation triggering infringement

100. *See id.* at 20 ("Title II [of the DMCA] preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment.").

101. *Id.* at 49.

102. *Id.*

103. *See id.*

104. *See* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1058 (9th Cir. 2017).

liability for ISPs. An ISP might still lack the information necessary to discern[105] if an image was in the public domain or still under copyright protection, or whether the image's use was licensed or permitted under fair use.[106] Conversely, copyright owners "know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers."[107] Moreover, the DMCA's legislative history, coupled with other court decisions in this realm, seems to attempt to avoid imposing liability on ISPs where such platforms are merely trying their best to curate content in keeping with their usual practices, even where those attempts may extend beyond the most fundamental accessibility-enhancing acts.[108]

C. THE NINTH CIRCUIT'S APPROACH IS AT ODDS WITH CONGRESSIONAL INTENT IN SIMILAR POLICY REALMS

ISPs have interests in monitoring the user-submitted content on their platforms for purposes beyond identifying instances of copyright infringement. Indeed, many ISPs "generally can't determine whether [user-submitted] content violates its policies" without at least looking at that content,[109] and that interaction with user-submitted content is often part and

105. *See* Brief of Online Service Providers Etsy, Kickstarter, Pinterest, and Tumblr in Support of Appellee at 13, Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1053 (9th Cir. 2017), 2015 WL 3970267, at *13 [hereinafter Brief of Online Service Providers].

106. *See* S. REP. NO. 105-190, at 48 (1998).

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

108. *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 41 (2d Cir. 2012) ("Refusing to accommodate or implement a 'standard technical measure' exposes a service provider to liability; refusing to provide access to mechanisms by which a service provider affirmatively monitors its own network has no such result. In this case, the class plaintiffs make no argument that the content identification tools implemented by YouTube constitute 'standard technical measures,' such that YouTube would be exposed to liability under § 512(i). For that reason, YouTube cannot be excluded from the safe harbor by dint of a decision to restrict access to its proprietary search mechanisms."); *see also* CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 556 (4th Cir. 2004) ("To the extent that LoopNet's intervention in screening photographs goes further than the simple gatekeeping function described above, it is because of CoStar's complaints about copyright violations . . . CoStar can hardly request LoopNet to prevent its users from infringing upon particular unmarked photographs and then subsequently seek to hold LoopNet liable as a direct infringer when Loop–Net complies with CoStar's request. In short, we do not conclude that LoopNet's perfunctory gatekeeping process, which furthers the goals of the Copyright Act, can be taken to create liability for LoopNet as a direct infringer when its conduct otherwise does not amount to direct infringement.").

109. Brief of Online Service Providers, *supra* note 105, at 25.

parcel with being a successful ISP. As ISP *amici* Etsy,[110] Kickstarter,[111] Pinterest,[112] and Tumblr[113] argued in their brief supporting LiveJournal, ISPs' efforts to "facilitate [user] access . . . to a massive amount of content, with new material pouring in constantly" often requires "engagement with users' material."[114] In some cases, as Congress mentioned in the DMCA's legislative history, "[i]t is precisely the human judgment and editorial discretion" that makes ISP tools valuable to users.[115] The value of engaging with users' content is not limited to modern social media practices, however. Rather, it has existed since the days of the early World Wide Web.

Shortly before enacting the DMCA in 1998, Congress enacted the Communications Decency Act (CDA) as part of the Telecommunications Act of 1996.[116] Section 230 of the CDA[117] generally protects[118] ISPs from liability for third-party actions on their platforms,[119] as well as liability for electing to screen or remove certain content.[120] Unlike the DMCA's focus on copyright infringement, however, § 230 was aimed at addressing "offensive material," such as pornography, submitted by ISP users.[121] In doing so, the statute provides that an ISP shall not assume the role of "publisher or speaker of any information" provided by another party.[122]

---

110. An e-commerce platform for user-to-user sale of handmade or vintage items. *See* ETSY, https://www.etsy.com/about [https://perma.cc/UH7M-DZXY] (last visited Dec. 21, 2018).

111. A crowdfunding platform that allows users to create and donate to projects and initiatives. *See* KICKSTARTER, https://www.kickstarter.com/about [https://perma.cc/5CLE-XW3Q] (last visited Dec. 21, 2018).

112. A social networking platform centering collection of image-based material online. *See* PINTEREST, https://about.pinterest.com/en [https://perma.cc/75PK-5FTT] (last visited Dec. 21, 2018).

113. A microblogging platform; similar to LiveJournal in functionality, but users are only able to create and interact with individual accounts. *See* TUMBLR, https://www.tumblr.com/about [https://perma.cc/Q7P7-PU6G] (last visited Dec. 21, 2018).

114. Brief of Online Service Providers, *supra* note 105, at 24–26.

115. S. REP. NO. 105-190, at 49 (1998).

116. The Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. Section 230 was codified as § 509 of the Telecommunications Act of 1996.

117. 47 U.S.C. § 230 (2012).

118. Section 230 contains exclusions for violations of federal criminal statutes, intellectual property claims, and enforcement of the Electronic Communications Privacy Act of 1996 or similar state laws. *See* § 230(e).

119. *See* § 230(c)(1).

120. *See* § 230(c)(2).

121. § 230(c)(2)(A) (providing that ISPs removing what they believe to be "obscene, lewd, lascivious, filthy, excessively, violent, harassing, or otherwise objectionable" in good faith shall not be held liable on account of interaction with that material).

122. § 230(c)(1).

While § 230 has no bearing—and, in fact, explicitly should not "be construed to limit or expand any law pertaining to intellectual property,"[123] the provision's implementation nonetheless sheds light on the Congressional intent behind the DMCA. Both schemes establish partial protection for online providers, balancing ISP interests with the public's interest in keeping offensive or otherwise harmful material offline. Additionally, though the § 230 rules are not entirely analogous to § 512, defendant ISPs must meet similar requirements to take advantage of this "safe harbor" of sorts.[124] Most telling, however, is the CDA's principal goal, which it shares with the DMCA: to "promote the continued development of the Internet and other interactive computer services and other interactive media."[125]

Ironically, the CDA was initially enacted to remedy the same uncertainty among ISPs that the Ninth Circuit's *Mavrix* decision has created. In the days of the early Internet, ISPs faced unpredictable liability risks for offensive material others posted to their platforms. In *Cubby, Inc. v. CompuServe, Inc.*,[126] for example, the defendant ISP offered a subscription-based news archive.[127] A news aggregator claimed that a competitor published defamatory remarks about their service and the individuals involved via the defendant ISP's service.[128] The District Court for the Southern District of New York found no liability on the ISP's part, likening its relationship with the defamatory content to a brick-and-mortar library's relationship with the content of the books it carries.[129] Other courts, like the New York Supreme Court in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[130] however, put ISPs in a more difficult position. In that case, the defendant ISP was an online bulletin board community for

123. § 230(e)(2).

124. *See* Stoner v. eBay, Inc., No. 305666, 2000 WL 1705637, at *1 (Cal. Super. Ct. Nov. 1, 2000) ("Immunity under the CDA requires proof of three elements. Defendant [ISP] must establish (1) that [it] is an interactive computer services provider; (2) that [it] is not an information content provider with respect to the disputed activity; and (3) that plaintiff seeks to hold [defendant] liable for information originating with a third-party user of its service."); *See* § 230(c)(1)–(2).

125. § 230(b)(1); *see also Stoner*, 2000 WL 1705637, at *3 ("A principal objective of the immunity provision is to encourage commerce over the Internet by ensuring that interactive computer service providers are not held responsible for how third parties use their services."); Paul Ehrlich, *Communications Decency Act 230*, 17 BERKELEY TECH. L.J. 401, 404 (2002).

126. 776 F. Supp. 135 (S.D.N.Y. 1991).

127. *See id.* at 137.

128. *See id.*

129. *See id.* at 140 ("[The defendant ISP] has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for [the ISP] to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so.").

130. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

finance discussions.[131] Leaders of this community could use an "emergency delete" functionality for removal of user notes that were insulting, off-topic, bad advice, or in poor taste.[132] Despite the board's receipt of more than 60,000 messages daily—making manual review of each message infeasible—the court held that by electing to moderate *some* user posts, the ISP became liable for *all* unlawful posts on the platform.[133] This decisional inconsistency incentivized ISPs to take a "hands-off" approach to maintaining their platforms, lest they incur greater liability for trying to keep them clear of obscene or harmful material.[134]

With the enactment of § 230, ISPs gained the certainty necessary to operate their platforms in an informed way. In this sense, Congress's rationale for implementing § 230 appears similar to its motivation for enacting the DMCA: when ISPs are free to interact with material on their platforms without fear of incurring liability for their users' activity, they are then also free to innovate and improve their services.[135] If Congress meant—as the Ninth Circuit's approach would dictate—to withhold protection for ISPs voluntarily moderating material within their services, it could have explicitly articulated this to distinguish the DMCA from the CDA. However, it did not, and Congress, in fact, *endorsed* such acts[136] with its explicit contemplation of "human editors and reviewers" within its DMCA framework.[137]

Of course, while similar, CDA § 230 and the DMCA address categorically different kinds of online material. Admittedly, offensive material and infringing material are harmful in different ways. And, while their goals are indeed similar, Congress enacted the CDA with the more specific twin goals of removing "disincentives for the development and utilization of blocking and filtering technologies,"[138] and preserving "the vibrant and competitive free

131. *See id.* at *1.

132. *Id.* at *3.

133. *See id.* at *5 ("[The ISP's] conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability . . . to the extent computer networks provide such services, they must also accept the concomitant legal consequences.").

134. *See* Ehrlich, *supra* note 125, at 404.

135. *See* Sophia Cope, *Stop SESTA: Section 230 Is Not Broken*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Sept. 6, 2017), https://www.eff.org/deeplinks/2017/09/stop-sesta-section-230-not-broken [https://perma.cc/Q4GA-RRZN] ("Section 230 reflects a purposeful balance that permits Internet intermediaries to be on the hook for their users' content in certain carefully considered circumstances, and the courts have expanded upon these rules.").

136. *See* Brief of Online Service Providers, *supra* note 105, at 9 ("It would make no sense to interpret the DMCA to withhold protection from services engaging in the very kind of voluntary moderation that Congress expressly endorsed.").

137. S. REP. NO. 105-190, at 48–49 (1998).

138. 47 U.S.C. § 230(b) (2012).

market that presently exists for the Internet."[139] Thus, § 230 was partially predicated on the idea that the Internet as a marketplace would help weed out offensive material as ISP users sought out providers with better-filtered content.[140] Market forces, however, would do little to curb online copyright infringement, since everyday ISP users are unlikely to even recognize infringing material as such (and, even if they do, they may be attracted to it). Second, the harm incurred by offensive material online arguably affects the broader community of Internet users, while copyright infringement results in individual harm to the copyright holder. Moreover, for copyright holders like Mavrix, the harm sustained—for example, lost licensing deals once their photos have been scooped—can be complete and irrevocable the moment infringing content is published by an ISP.[141] Conversely, early removal of obscene content may mitigate harm to the public by minimizing its exposure.

Despite these differences, however, the underlying goals for ISP development are meaningfully the same between the DMCA and § 230. Both were enacted with the understanding that ISPs are discouraged from innovating and exploring new services for their users when they are vulnerable to liability for content those users publish. Further, such widespread liability would, as previously discussed, create a disincentive[142] for ISPs to interact with user-created content altogether,[143] and undermine the business models of ISPs

---

139. *Id.*

140. *See* Ehrlich, *supra* note 125, at 412 ("[T]he market will still encourage internet service providers to filter where appropriate. There are several reasons to believe this to be true. First, the bright-line rule of immunity will remove uncertainty and thereby stimulate innovation. Second, the unique characteristics of Internet speech and mobility will quickly guide the market toward equilibrium. The net result will be a general level of filtering consistent with Internet community norms.").

141. *See* Appellant's Opening Brief, *supra* note 88, at 6 ("When Mavrix secures valuable exclusive photos of celebrities, often before it can even monetize the photos, those photos are stolen and leaked to the internet, which in turn eliminates the full value Mavrix can secure by license deals with its clients.").

142. *See* Corynne McSherry, *Ninth Circuit Sends a Message to Platforms: Use a Moderator, Go to Trial*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 8, 2017), https://www.eff.org/deeplinks/2017/04/ninth-circuit-sends-message-platforms-use-moderator-go-trial [https://perma.cc/E5NX-UCZY] ("The irony here is that copyright owners are constantly pressuring service providers to monitor and moderate the content on their services more actively. [The *Mavrix v. LiveJournal*] decision just gave them a powerful incentive to refuse.").

143. *See* Guinevere Jobson, Armen N. Nercessian, *"Oh No They Didn't!"—Ninth Circuit Throws DMCA Safe Harbors for Moderated Content into Disarray*, LEXOLOGY (Apr. 12, 2017), https://www.lexology.com/library/detail.aspx?g=845462af-ee94-46de-86ba-8342c6a303a3 [https://perma.cc/2U9T-2E7V]

> Even where a website, like LiveJournal [in *Mavrix v. LiveJournal*], has procedures for expeditiously removing allegedly infringing user-generated materials identified on takedown notices, *Mavrix* teaches that a service

previously operating without the constant threat of liability for the actions of their users.[144] The Ninth Circuit's characterization of the relationship between an ISP and its moderating staff as the threshold inquiry for § 512(c) protection raises the same troubles Congress faced in 1996 with the CDA, and again in 1998 with the DMCA. Specifically, its decision revives the same uncertainty and risk these doctrines were enacted to combat in the first place.[145]

D. THE NINTH CIRCUIT'S APPROACH IS AT ODDS WITH PRESSURE CONGRESS IS *CURRENTLY* PLACING ON ISPS

The Ninth Circuit's implicit message that an ISP's engagement with user-submitted content imperils its safe harbor protection[146] is not only at odds with Congressional intent in enacting the DMCA and statutes in similar policy realms, but it is at odds with *current* Congressional conceptions of proper ISP oversight as well. As ISPs—particularly social media ISPs—have increasingly become intertwined with day to day life in the years since the DMCA was enacted, the new threat of "fake news" has highlighted the perils of ISPs taking a "hands-off" approach to monitoring what their users publish to their

> provider may still lose safe harbor protection based on its efforts to curate materials available on its platform. This ruling incentivizes platforms seeking to avail themselves of the safe harbor to exercise less oversight of materials that users submit for posting. That is particularly true in light of the impracticability of having a platform, which lacks both information about the ownership of posted materials and competence to make judgments about their legal status, to screen materials based on infringement.

144. Jeremy Goldman & Andrew Ungberg, *Federal Appeals Court Weakens DMCA Safe Harbor Protection for Moderated Online Content*, FRANKFURT KURNIT KLEIN & SELZ PC (May 3, 2017), https://www.focusonthedata.com/2017/05/federal-appeals-court-weakens-dmca-safe-harbor-protection-moderated-online-content [https://perma.cc/R62H-D58E] ("Although *Mavrix* suggests that the surest way to qualify for DMCA safe harbor status is to refrain from moderating, many ISPs cannot risk leaving their brands exposed in a moderator-free Wild West bonanza."); *see also* Cope, *supra* note 135 ("[I]f Internet intermediaries are not largely shielded from liability for content their users create or post—particularly given their huge numbers of users—existing companies risk being prosecuted or sued out of existence, and potential new companies may not even enter the marketplace for fear of being prosecuted for sued out of existence (or because venture capitalists fear this).").

145. *See* Brianna Dahlberg, *Ninth Circuit Ruling Raises New Legal Risks for Websites That Use Moderators to Screen User-Submitted Content (*Mavrix v. LiveJournal*)*, COWAN DEBAETS ABRAHAMS & SHEPPARD LLP (Apr. 17, 2017), http://cdas.com/nnew-legal-risks-websites-use-moderators [https://perma.cc/9TZR-37L4] ("While copyright owners will be pleased with the [*Mavrix v. LiveJournal*] decision because it makes it easier to enforce against online infringement, the decision creates new uncertainty and risk for social media websites, digital publishers, and other internet platforms which allow user-submitted content.").

146. *See* Goldman & Ungberg, *supra* note 144 ("The takeaway from *Mavrix* is clear—an ISP can no longer take its DMCA safe harbor status for granted if it engages with user-submitted content beyond merely performing 'accessibility-enhancing activities.' ").

platforms. Indeed, "[s]ome of the biggest companies in the world—Google, Apple, Facebook, Amazon and Alibaba among them—are finding they need to play by an entirely new set of rules on the once-anarchic internet."[147]

Nearly twenty years after the DMCA was enacted, the rise of fake news has proven to be the latest manifestation of the perennial problem facing ISPs: for better or worse, user-submitted content on their platforms is becoming increasingly impactful in shaping other users' views, beliefs, and behaviors on and offline. False news stories tied to Russian originators, for example, reached 126 million people via Facebook during the United States' 2016 presidential election, and similar instances of false propaganda successfully using popular ISPs as conduits have cropped up globally.[148] In the United States, individual members of Congress have already begun demanding increased ISP accountability for the consequences of such events,[149] signaling a growing desire for *more* ISP supervision of user-generated content on their platforms.[150]

If the Ninth Circuit's de facto narrowing of safe harbor eligibility for ISPs is to become the status quo, ISPs will be forced into a catch-22. On the one

147. Mike Isaac, Paul Mozur & Mark Scott, *Facebook Faces a New World as Officials Rein in a Wild Web*, N.Y. TIMES (Sept. 17, 2017), https://www.nytimes.com/2017/09/17/technology/facebook-government-regulations.html [https://perma.cc/Y2VY-57HM].

148. *See* James Temperton, *As Congress Circles, Facebook and Google Scramble for Transparency*, WIRED UK (Oct. 31, 2017), http://www.wired.co.uk/article/facebook-russia-election-adverts-congress-twitter-google [https://perma.cc/5ZBB-A642]

> In the UK, investigations are underway into suspected links between Russian-backed social media propaganda campaigns and the Brexit vote. In Germany, the far-right AfD had great success with divisive advertising on Facebook and Twitter in the run-up to the recent elections. And from India to Tanzania, political WhatsApp [a messenger service owned by Facebook] groups with thousands of members have become powerful propaganda tools.

149. *See* Mathew Ingram, *For Facebook, the Political Reckoning Has Begun*, COLUM. JOURNALISM REV. (Oct. 30, 2017), https://www.cjr.org/covering_trump/facebook-congress-russia.php [https://perma.cc/595N-KHX7] ("Among the questions Congress will have to confront: How much of this is Facebook's fault? Did it knowingly permit Russian agents to influence American voters, or was it just an unfortunate outcome of how the network functions?").

150. *See id.* ("If [Congress' proposed plan] becomes a reality, Facebook . . . could be required to be a lot more hands on in monitoring what it runs and where."); *see also* Mike Isaac, *At Facebook, Hand-Wringing over a Fix for Fake Content*, N.Y. TIMES (Oct. 27, 2017), https://www.nytimes.com/2017/10/27/technology/facebook-fake-content-employees.html [https://perma.cc/RN7Z-NQL4] ("On one side are employees who idealize Facebook's lofty goals of unfettered speech and do not think the company should be in the business of censoring what its users have to say. On the other side are workers who worry that the company's hands-off approach has already caused problems—ones that will grow worse if nothing is done.").

hand, the looming danger of liability for user infringement incentivizes ISPs to cut back on (if not abolish entirely) moderation practices, while pressure from angry lawmakers provides motivation to implement more editorial safeguards than ever before. This harkens back to the DMCA's balancing of interests and again calls into question the degree to which ISPs should be held responsible for the content their users generate.[151]

Interestingly, the manual screening activities the Ninth Circuit found so problematic within LiveJournal and ONTD's internal procedures in *Mavrix* are the same protocols lawmakers are currently pressuring similar ISPs to adopt to mitigate fake news.[152] In fact, fully automated processes, which the Ninth Circuit contended should be the only basis for ISP protection under § 512(c), [153] have exacerbated ISP-based propaganda and harassment problems.[154] Despite automated systems' and engines' status as an essential component of the service itself for many ISPs, technology giants like Google and Facebook have nonetheless promised to "add more human oversight" to avoid future instances of offensive or bogus content. [155] In this sense, Facebook's tricky position is very much like LiveJournal's: both ISPs strive to serve as neutral platforms through which users can "freely post, read and view

151. *See* Kevin Roose, *Forget Washington. Facebook's Problems Abroad Are Far More Disturbing*, N.Y. TIMES (Oct. 29, 2017), https://www.nytimes.com/2017/10/29/business/facebook-misinformation-abroad.html [https://perma.cc/EG2J-MT8X]

> Facebook is not directly responsible for violent conflict, of course, and viral misinformation is hardly unique to its services. Before social media, there were email hoaxes and urban legends passed from person to person. But the speed of Facebook's growth in the developing world has made it an especially potent force among first-time internet users, who may not be appropriately skeptical of what they see online . . . . Correcting misinformation is a thorny philosophical problem for Facebook, which imagines itself as a neutral platform that avoids making editorial decisions.

152. *See* Jennifer Golbeck & Andrea Matwyshyn, *Fake News, Hate Speech and Social Media Abuse: What's the Solution?*, KNOWLEDGE@WHARTON (Nov. 21, 2016), http://knowledge.wharton.upenn.edu/article/whats-the-solution-to-fake-news [https://perma.cc/AR5M-4Y8D] ("Addressing fake news and other forms of gaming social media platforms will be a multi-faceted process . . . Doing more will likely require a combination of human oversight, algorithms designed to weed out falsehood or abuse, and tools to further empower users.").

153. *See* There is, however, a narrow exception for manual activities specifically directed at improving accessibility. *Id.*

154. *See* Ingram, *supra* note 149 ("Without automation there would be no way for [ISPs like Facebook] to achieve the kind of scale necessary to reach more than two billion people per day. The downside of this kind of automation extends beyond just potential Russian involvement—in several cases, Facebook has accepted advertising that was directed at offensive categories such as 'Jew haters.' ").

155. *See id.*

content."[156] Practically speaking, however, as social media's "reach and influence have grown," these ISPs must face growing questions of responsibility for what exists on their networks.[157] To curb fake news, for example, Facebook has begun implementing technological measures to make flagging improper content easier for users within moderated groups, ultimately sending disputed content further down users' news feeds within the platform.[158] Such initiatives, however, under the Ninth Circuit's misguided "agency" approach to liability shields for ISPs, would bar companies like Facebook from taking such actions and remain protected from liability for their users' bad behavior. This, too, is at odds with the DMCA's central tenet of balancing the interests of the ISPs with the interests of their users and backs ISPs into a corner. Despite the quandary the Ninth Circuit would place them in, "social media networks do not have the option of doing nothing in preventing fake news."[159]

V. CONCLUSION

In an increasingly complex environment for ISPs, the Ninth Circuit's unprecedented insistence that agency is an appropriate approach for discerning ISP safe harbor protection ignores Congressional goals in enacting the DMCA as well as current Congressional concerns centering ISPs and the information they transport. Given this practical break with the legislative history and goals of the DMCA doctrine, as well as the present era of rampant fake news and online harassment, it seems particularly imprudent for the Ninth Circuit to interpret the DMCA's safe harbors in a way that might discourage human interaction with user-submitted content. Such an approach threatens to undercut the very purpose of the DMCA, and should be reconsidered in future safe harbor analysis.

156. Mike Isaac, *Facebook Mounts Effort to Limit Tide of Fake News*, N.Y. TIMES (Dec. 15, 2016), https://www.nytimes.com/2016/12/15/technology/facebook-fake-news.html [https://perma.cc/M4VF-EM82].

157. *Id.*

158. *See* Isaac, *supra* note 156; *see also* Saqib Shah, *Facebook Reports Success in Removing Fake News for Germany's Election*, DIGITAL TRENDS (Sept. 28, 2016), https://www.digitaltrends.com/social-media/facebook-fake-news-germany [https://perma.cc/5WUT-H523] ("While Facebook admitted that [its] efforts did not ultimately eliminate all fake news, initiatives did make the proliferation of faulty information less rampant.").

159. Golbeck & Matwyshyn, *supra* note 152.