VOLUME 61 | 2016/17

MICHAEL S. ISSELIN

#StopImmunizing: Why Social Networking Platform Liability Is Necessary to Provide Adequate Redress for Victims of Cyberbullying

61 N.Y.L. Sch. L. Rev. 369 (2016–2017)

ABOUT THE AUTHOR: Michael S. Isselin was a Notes and Comments Editor of the 2014–2015 *New York Law School Law Review*. He received his J.D. from New York Law School in 2015. This note was awarded the Otto L. Walter Distinguished Writing Award from New York Law School in 2015.

I. INTRODUCTION

On September 22, 2010, college freshman Tyler Clementi committed suicide after his roommate streamed a video of Tyler kissing another man.[1] His story brought the issue of cyberbullying[2] to the world stage, garnering intense news media coverage. Public figures, including President Barack Obama, Ellen DeGeneres, and Anderson Cooper spoke out against cyberbullying soon thereafter.[3]

Two years later, in September 2012, after being harassed by a stranger online, fifteen-year-old Amanda Todd posted a video describing her experience of being threatened and bullied.[4] Amanda hanged herself a few weeks later.[5] The following

1. Lisa W. Foderaro, *Private Moment Made Public, Then a Fatal Jump*, N.Y. Times (Sept. 29, 2010), http://www.nytimes.com/2010/09/30/nyregion/30suicide.html.

2. A number of definitions of "cyberbullying" exist. Social science definitions often start with three concepts: "intent to harm, imbalance of power and usually a repeated action." Bobbie Mixon, *Defining a Cyberbully*, Nat'l Sci. Found. (Nov. 8, 2011), http://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=121847. Dictionary definitions include "the act of harassing someone online by sending or posting mean messages, usually anonymously." *Cyberbullying*, Dictionary.com, http://www.dictionary.com/browse/cyberbullying (last visited Apr. 6, 2017). For the purpose of this note, cyberbullying is defined as the use of electronic communication to intentionally cause extreme harassment or embarrassment, beyond what a reasonable person in the victim's position would expect. This narrow definition provides social networking platforms with a workable definition to help readily distinguish cyberbullying from harmless activity. *See, e.g.*, Carrie Goldman, *How Do I Know What's Bullying and What's Normal Conflict?*, N.Y. Times: Motherlode (Oct. 10, 2014, 8:06 AM), http://parenting.blogs.nytimes.com/2014/10/10/how-do-i-know-whats-bullying-and-whats-normal-conflict (stating that bullying is distinguished from normal social conflict when three factors are present: repetition, unwanted aggression, and a power imbalance).

3. *See Anderson Cooper's Anti-Bullying Series: Too Many Kids Have Died Already*, Huffington Post (Dec. 7, 2011), http://www.huffingtonpost.com/2011/10/07/anderson-cooper-bullying_n_1000024.html; Mike Isaac, *Obama on Twitter, Cyberbullying, the Internet: Play Nice*, Forbes (Oct. 14, 2010, 8:16 PM), http://www.forbes.com/sites/velocity/2010/10/14/obama-on-twitter-cyberbullying-the-internet-play-nice; Aliyah Shahid, *Tyler Clementi: Video by Ellen DeGeneres, Speaks Out Against Teen Bullying, Alongside Abdul, Ciara*, N.Y. Daily News (Oct. 1, 2010, 3:08 PM), http://www.nydailynews.com/new-york/tyler-clementi-video-ellen-degeneres-speaks-teeny-bullying-abdul-ciara-article-1.191179. Following Tyler Clementi's suicide, gay rights activist Dan Savage's "It Gets Better" project grew in support and recognition. James Montgomery, *Dan Savage Explains Why He Started 'It Gets Better' Project*, MTV News (Sept. 30, 2010), http://www.mtv.com/news/1649114/dan-savage-explains-why-he-started-it-gets-better-project. Private citizens and public figures alike have created videos for the campaign to communicate to LGBT youth that "it gets better." *What Is the It Gets Better Project?*, It Gets Better Project, http://www.itgetsbetter.org/pages/about-it-gets-better-project (last visited Apr. 6, 2017). Among thousands of others, former Secretary of State Hillary Clinton, actress Anne Hathaway, and the staffs of Facebook and Gap Inc. have contributed videos for the project. *Id.*

4. *See* Ryan Grenoble, *Amanda Todd: Bullied Canadian Teen Commits Suicide After Prolonged Battle Online and in School*, Huffington Post (Oct. 12, 2012), http://www.huffingtonpost.com/2012/10/11/amanda-todd-suicide-bullying_n_1959909.html. The video reports that a man on Facebook threatened Amanda Todd by demanding that she "put on a show" or he would disseminate an image of her showing her breasts on camera. *Id.* Todd's video, titled "My Story: Struggling, Bullying, Suicide, Self Harm," was viewed more than seventeen million times at the time of her suicide. *The Top Six Unforgettable CyberBullying Cases Ever*, NOBullying.com (Oct. 19, 2016), http://nobullying.com/six-unforgettable-cyber-bullying-cases.

5. *See* Rachael E. Ferrante, *The Relationship Between Digital Assets and Their Transference at Death: "It's Complicated*," 15 Loy. J. Pub. Int. L. 37, 60 (2013).

year, twelve-year-old Rebecca Sedwick jumped to her death after two teenage girls sent her harassing messages online.[6] Tyler's, Amanda's, and Rebecca's tragedies reveal the horrific consequences of inadequately protecting online users against cyberbullying.

Victims of cyberbullying currently have limited options for legal redress.[7] They may bring criminal charges if the relevant jurisdiction has laws in place,[8] or file a civil action against an individual aggressor, but *only* if they can identify the aggressor.[9] Redress options exclude filing suits against the online platform where the cyberbullying occurred. Significantly, social networking platforms,[10] where arguably the most cyberbullying occurs,[11] are immune from liability.[12] As a result, the current legal landscape severely limits the parties a victim can hold accountable.

The shortcomings of redress highlight two parts of the problem. First, victims of anonymous[13] cyberbullying face the unmasking process, which can be challenging and expensive and may deter victims from seeking redress.[14] Second, the current judicial interpretation of § 230 of the Communications Decency Act (CDA)[15] grants

---

6. Stephanie Allen & Matthew Pleasant, *Lakeland Girl Commits Suicide After 1½ Years of Being Bullied*, Ledger (Sept. 10, 2013, 10:37 AM), http://www.theledger.com/article/20130910/news/130919963. Following Rebecca Sedwick's death, one harasser posted on Facebook, "I bullied Rebecca nd [sic] she killed herself." Josh Sanburn, *A Florida Tragedy Illustrates Rising Concern About Cyber-Bullying Suicides*, Time (Oct. 16, 2013) (alteration in original), http://nation.time.com/2013/10/16/a-florida-tragedy-illustrates-rising-concern-about-cyber-bullying-suicides.

7. *See* Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 Yale. L.J. Pocket Part 41, 41 (2007) ("Given its immediacy, anonymity, and accessibility, the Internet offers an unprecedented forum for defamation and harassment. The salient problem with such 'cyberbullying' is that victims are typically left without adequate recourse.").

8. For more on state cyberbullying laws, see generally Sameer Hinduja & Justin W. Patchin, Cyberbullying Res. Ctr., State Cyberbullying Laws (2016), http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf.

9. *See infra* Part II.A.

10. A "social network" is defined as "a network of friends, colleagues, and other personal contacts" and "an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc[etera]." *Social Network*, Dictionary.com, http://www.dictionary.com/browse/social--network (last visited Apr. 6, 2017). For the purpose of this note, "social networking platforms" refers to such networks operated via the Internet.

11. According to a 2012 McAfee survey,

> 93% of teens who have witnessed cruel behavior online say that [the] majority of cruel online behavior took place on Facebook. Furthermore half of teens have had a negative experience as a result of a social network site. Email was reported as one of the safest online activit[ies] with only 6.37% of teens reporting cruel behavior . . . .

70% of Teens Hide Their Online Behavior from Their Parents, McAfee Reveals What U.S. Teens Are Really Doing Online, and How Little Their Parents Actually Know, Intel Security (June 25, 2012), http://www.mcafee.com/us/about/news/2012/q2/20120625-01.aspx.

12. *See infra* Part II.B.

13. For the purpose of this note, "anonymous" includes pseudonymous and unidentifiable individuals.

14. *See infra* Part II.A.

15. 47 U.S.C. § 230 (2012).

social networking platforms immunity against a victim's claims.[16] The resulting landscape cries for a workable solution.

Scholars have recently identified several ways to provide victims better redress options.[17] However, each option fails to specifically address social networking platforms, where the risk of cyberbullying is greatest.[18] One proposal creates a single standard for courts to apply when deciding whether to compel an Internet company to disclose an anonymous user's identity.[19] Another proposal calls for Congress to amend the CDA by creating an exception to the blanket immunity that exists for Internet Service Providers (ISPs).[20] Yet another proposal suggests implementing qualified notice-based liability for ISPs.[21] This note proposes a process similar to notice-based liability but expands the focus to social networking platforms,[22] recognizing that as technology advances and new social networking platforms emerge, a clear shift in the legal landscape must occur.

This note argues that an intertwining web of laws and precedent has eliminated virtually all avenues of redress available to victims of cyberbullying. The unmasking and immunity problems—eliminating adequate redress options—affect legal traditions, public policy, and society. First, by immunizing social networking platforms, the current legal landscape departs from established principles of third-party liability.[23] Second, platforms owe a self-made duty to protect users from offensive content, and by limiting victim redress to the individual aggressor the landscape disincentivizes platforms from upholding this duty.[24] Finally, by eliminating accountability the legal landscape perpetuates the cyberbullying problem.[25]

To mitigate these impacts and provide victims with sufficient redress, this note proposes a takedown process mirroring that of the Digital Millennium Copyright Act (DMCA)[26] that will work alongside the CDA to provide victims the opportunity to hold social networking platforms liable for failing to remove cyberbullying

16. *See infra* Part II.B.

17. *See infra* Part IV.

18. *See supra* note 11 and accompanying text; *see also infra* note 123 and accompanying text.

19. Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 Yale L.J. 320, 363–64 (2008).

20. Cara J. Ottenweller, Note, *Cyberbullying: The Interactive Playground Cries for a Clarification of the Communications Decency Act*, 41 Val. U. L. Rev. 1285, 1288, 1326–30 (2007); *see also infra* Part III.

21. Areheart, *supra* note 7, at 43–44.

22. It is imperative to independently address social networking platforms because of the amount of cyberbullying that occurs on such platforms. *See supra* note 11. Additionally, the unique nature of these platforms requires a specific approach to accountability. *See infra* Part II.B.

23. *See infra* Part III.

24. *See infra* Part III.

25. *See infra* Part III.

26. 17 U.S.C. § 512(c) (2012).

content.[27] This process carefully balances the need for victim redress with a user's First Amendment right to speak freely, avoids overturning case law, works alongside the CDA, and embodies the fundamental values of § 230.

A thorough review of why the problem exists as well as its challenges demonstrates why this proposal is the best solution. Following this Introduction, Part II explains how the redress problem came about. Specifically, Part II.A reviews the history of the unmasking problem and its burdens on victims seeking redress, while Part II.B focuses on the problematic legal landscape created by granting social networking platforms immunity. Part III addresses how the redress problem expands beyond victims to affect legal traditions, public policy, and society. Part IV describes current proposals to solve the problem and their shortcomings, and instead proposes a DMCA-like process that will better address a victim's redress options. Part V concludes this note. Appendix A sets forth the language of the proposal in Part IV alongside corresponding provisions from the DMCA.

II. THE PROBLEM: INADEQUATE REDRESS IN THE CURRENT LEGAL LANDSCAPE

A. The Unmasking Problem

The unmasking problem typically arises when the cyberbullying results from an anonymous aggressor. Since many social networking platforms allow users to remain unidentifiable, victims face a significant challenge to hold an aggressor liable.[28] An overview of the unmasking process demonstrates this hurdle.

The U.S. Supreme Court recognizes that the First Amendment protects online speech,[29] including an individual's right to speak anonymously.[30] However, this right is not unlimited.[31] Plaintiffs may seek redress for harmful online speech made by anonymous users, but they must first learn the aggressor's identity.[32] This process,

27. *See infra* Part IV and Appendix A.

28. Anonymity on social networking platforms provides individuals with the opportunity to speak without believing any consequence will result, thereby increasing the potential for cyberbullying. *See* Sameer Hinduja & Justin W. Patchin, Bullying Beyond the Schoolyard 20 (2009) ("Malicious words and statements that an individual might be ashamed or embarrassed to use in a face-to-face setting are no longer off-limits or even tempered when that person is physically distant from the target."). However, as discussed herein, anonymity does not eliminate accountability because "individuals are not completely anonymous when interacting in cyberspace." *Id.* at 21.

29. Reno v. ACLU, 521 U.S. 844, 870 (1997).

30. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment."); Talley v. California, 362 U.S. 60, 64 (1960) (finding that requiring an author's identity on handbills "would tend to restrict freedom to distribute information and thereby freedom of expression").

31. Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 Notre Dame L. Rev. 1537, 1600 (2007) ("[T]he right is not absolute but must be balanced against plaintiffs' interests in order to foster uninhibited public discourse."); *see also McIntyre*, 514 U.S. at 357 ("The right to remain anonymous may be abused when it shields fraudulent conduct.").

32. *See McIntyre*, 514 U.S. at 341, 353; Doe I v. Individuals, 561 F. Supp. 2d 249, 254 (D. Conn. 2008).

known as unmasking, can be a lengthy back-and-forth task for plaintiffs.[33] First, the plaintiff must subpoena[34] the online entity to obtain the aggressor's registration information or Internet Protocol (IP) address.[35] If the online service provider provides the IP address, the plaintiff must then contact the appropriate ISP, usually by subpoena, seeking information linked to the IP address.[36] Before responding to the subpoena, the ISP will attempt to notify the aggressor,[37] who may then move to prevent disclosure of her identity.[38] If the aggressor moves to prevent disclosure, or the ISP does not respond to the subpoena, the plaintiff must then file an order requesting a court to compel the ISP to respond to the subpoena.[39]

Faced with a motion to compel disclosure of an anonymous aggressor's identity, courts will balance the defendant's First Amendment right to speak anonymously against the plaintiff's right to seek legal redress.[40] To strike this balance, courts commonly reference two judicially created tests: the *Dendrite* and *Cahill* tests. In *Dendrite International, Inc. v. Doe, No. 3*, the New Jersey Superior Court set forth a

33. The period between filing the subpoena and a court deciding a victim's motion to compel discovery can take several months. *See, e.g.*, Directory Assistants, Inc. v. Does 1–10, No. MC 11-00096-PHX-FJM, 2011 WL 5335562, at *1 (D. Ariz. Nov. 4, 2011) (deciding the plaintiff's motion to compel a website to comply with a subpoena sent to the website in May 2011, five months earlier).

34. A "subpoena" is "a writ commanding a person designated in it to appear in court under a penalty for failure." *Subpoena*, Merriam-Webster, https://www.merriam-webster.com/dictionary/subpoena (last visited Apr. 6, 2017). The verb form is defined as "to order someone to appear in court to give evidence." *Id.* Subpoenas that seek a defendant's identity are often referred to as "John Doe subpoenas."

35. Gleicher, *supra* note 19, at 328.

36. *Id.* This process is necessary because an IP address only provides the string of numbers identified with an individual computer, subject to change each time a user accesses the Internet, but the ISP still has access to the computer user's contact information. *Id.* Because of the changing nature of information connected to an individual IP address, this may require the plaintiff to serve additional subpoenas on an ISP. *Id.*; Ashley I. Kissinger & Katharine Larsen, *Untangling the Legal Labyrinth: Protections for Anonymous Online Speech*, 13 J. Internet L. 1, 23 (2010) ("With the increased use of open networks and anonymizers, IP disguisers, MAC spoofing, and similar technological tools, the IP address sought by a plaintiff may not conclusively identify the anonymous speaker.").

37. 47 U.S.C. § 551(a) (2012) (requiring notice to ISP subscribers before the ISP may disclose the subscriber's identity to a third party). There are policy and business reasons why an ISP would notify an alleged cyberbully before disclosing her identity. For instance, notifying the alleged cyberbully gives the individual the opportunity to file a motion to quash the subpoena so the ISP is not forced to disclose the information sought. *See Frequently Asked Questions for Subpoena Targets*, Electronic Frontier Found., https://www.eff.org/pages/frequently-asked-questions-subpoena-targets#prevent_disclosure (last visited Apr. 6, 2017). Another reason is to protect the alleged cyberbully from fraudulent claims by putting her on notice. A third reason is that notice also gives the alleged cyberbully the opportunity to take matters into her own hands and settle the matter outside the judicial system.

38. *See, e.g.*, Doe v. Cahill, 884 A.2d 451, 455 (Del. 2005) ("Doe filed an 'Emergency Motion for a Protective Order' seeking to prevent the [plaintiffs] from obtaining his identity from [the ISP].").

39. *See, e.g.*, Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001) (providing guidelines to trial courts "when faced with an application by a plaintiff for expedited discovery seeking an order compelling an ISP to honor a subpoena and disclose the identity of anonymous Internet posters").

40. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342, 353 (1995); Doe I v. Individuals, 561 F. Supp. 2d 249, 254 (D. Conn. 2008); *Dendrite*, 775 A.2d at 760–61.

four-pronged test, requiring the plaintiff to support her claim with sufficient facts to withstand a motion to dismiss and a balancing of the parties' interests.[41] In *Doe v. Cahill*, the Delaware Supreme Court altered the *Dendrite* test by dismissing it in part as unnecessary and adopting its first and third prongs: "the plaintiff must make reasonable efforts to notify the defendant and must satisfy the summary judgment standard."[42] Although the *Dendrite* and *Cahill* tests appear straightforward, courts have modified them haphazardly, which has unfairly burdened plaintiffs.[43]

Since redress for cyberbullying is limited to the individual aggressor, and aggressors can remain anonymous on many social networking platforms,[44] the unmasking process is often a part of a victim's legal challenge.[45] The haphazard nature of the courts' standards creates uncertainty about what is sufficient evidence for an unmasking order. This uncertainty results in such a burden that a victim may be less likely to bring a case and, if so, makes it harder for a victim to win. To demonstrate this burden, the table below reflects how courts indiscriminately apply factors when deciding whether to compel disclosure[46]:

41. 775 A.2d at 760–61. In *Dendrite*, the plaintiff sought the identity of a user who pseudonymously posted comments on Yahoo!'s Dendrite bulletin board. *Id.* at 763. The plaintiff alleged, inter alia, that certain statements were false, defamatory, and misappropriated trade secrets. *Id.* The court articulated the following test: (1) the plaintiff must attempt to notify the anonymous user that they are subject to a subpoena and withhold action allowing the user to oppose the request; (2) the plaintiff must set forth the user's exact statements; (3) the plaintiff must establish a prima facie cause of action against the user to withstand a motion to dismiss for failure to state a claim; and (4) assuming the plaintiff has established a prima facie cause of action, courts must balance the user's First Amendment right against the strength of the plaintiff's case and the need for disclosure. *Id.* at 760–61.

42. 884 A.2d at 461. The *Cahill* court found that the remaining *Dendrite* test requirements were unnecessary because they are subsumed into the summary judgment inquiry. *Id.*

43. For detailed analyses of the haphazard standards applied by courts, and arguments for, or against, a uniform standard, see Gleicher, *supra* note 19, at 338–45; Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. Rev. 833, 847–59 (2010); Sophia Qasir, Note, *Anonymity in Cyberspace: Judicial and Legislative Regulations*, 81 Fordham L. Rev. 3651, 3672–84 (2013).

44. For example, Instagram and Twitter users must create usernames, which may contain any number of letters, numbers, and certain symbols, leaving the user unidentifiable. *Creating an Account & Username*, Instagram Help Ctr., https://help.instagram.com/182492381886913 (last visited Apr. 6, 2017); Twitter, https://twitter.com/signup (last visited Apr. 6, 2017); *see also* Heather Kelly, *Anonymous Social Apps Provide Forum for Gripes, Gossip*, CNN (Feb. 28, 2014, 5:17 PM), http://www.cnn.com/2014/02/28/tech/social-media/secret-social-apps (discussing new social networking platforms that allow users to register and post content anonymously and the associated harms).

45. *See* Kissinger & Larsen, *supra* note 36, at 16 ("[A] party seeking redress for injuries caused by [an anonymous user's] post generally has no cause of action against the computer service itself, but only against the poster. As such, the discovery of the poster's identity is essential to pursuing a claim.").

46. This table is adopted from Gleicher, *supra* note 19, at 343. It identifies five factors courts consider and specifies those considered in leading cases: (1) whether there was notice to the defendant and an opportunity for her to respond anonymously, *id.* at 345; (2) the strength of the plaintiff's claim, that is, whether the claim meets standards of good faith, ability to survive a motion to dismiss, ability to withstand a motion for summary judgment, and ability to establish a prima facie case, *id.* at 350; (3) whether information a plaintiff seeks has "some degree of relevance to the plaintiff's case," *id.* at 357; (4) the plaintiff's level of specificity in making a claim, *id.* at 359; (5) a balancing of the interests of the

	Notice	Strength of Argument	Relevance	Specificity	Balancing Test	Exhaustion
Seescandy.com (1999)[47]		X	X			X
In re AOL (2000)[48]		X	X	X		
Dendrite (2001)[49]	X	X	X	X	X	
2TheMart.com (2001)[50]		X	X			X
Cahill (2005)[51]	X	X				
Mobilisa (2007)[52]	X	X			X	
Krinsky (2008)[53]	X	X				

Of the examples above, the *Dendrite* test, created by the New Jersey Superior Court, includes the most factors—notice, strength of the plaintiff's argument, relevance, specificity, and a balancing test—rendering it the most challenging for a victim to overcome.[54] Alternatively, in every example, the court's standard includes a review of the strength of the plaintiff's argument. The later cases—*Cahill*, *Mobilisa*, and *Krinsky*—show how this factor is one of only two or three considered.[55]

Although it may seem that the fewer factors a victim must prove the lesser the burden, the opposite is true in unmasking cases. Absent a number of other factors bearing on a court's analysis, courts following the framework of recent unmasking decisions are effectively forced to severely scrutinize the strength of a victim's argument.[56] The likelihood of success then heavily, if not entirely, rests on proving the

plaintiff and the defendant, *id.* at 360; and (6) whether the plaintiff can "demonstrate that he has exhausted all other means to identify the defendant," *id.* at 362.

47. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999).

48. *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26, 37 (Cir. Ct. 2000), *rev'd sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

49. Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

50. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

51. Doe v. Cahill, 884 A.2d 451, 461 (Del. 2005).

52. Mobilisa, Inc. v. Doe, 170 P.3d 712, 721 (Ariz. Ct. App. 2007).

53. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 244–45 (Ct. App. 2008).

54. *See* Roger M. Rosen & Charles B. Rosenberg, *Suing Anonymous Defendants for Internet Defamation*, L.A. Law., Oct. 2001, at 19, 21 (calling *Dendrite* "[t]he strictest test to date" for Internet defamation claims).

55. *See* Gleicher, *supra* note 19, at 343.

56. *See* Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001) ("The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. In addition to establishing that its action can withstand a motion to dismiss . . . , the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.").

claim will survive a motion to dismiss, thereby heightening the demand on a victim to plead her case with sufficient evidence.[57] This increased demand is further complicated by the uncertainty of what evidence a court will find sufficient to satisfy this factor,[58] burdening the victim to prove any and all arguments, and provide any and all evidence, that could tip the balance in her favor. If insufficient, Part II.B explains how the current interpretation of § 230 of the CDA then leaves victims without redress.

B. The Immunity Problem

Whether or not a victim of cyberbullying knows an aggressor's identity, the current legal landscape diminishes a victim's ability to hold any party other than the individual aggressor accountable. First, § 230 of the CDA immunized online platforms from liability for unlawful user-generated content.[59] Then, courts expanded this blanket immunity to cover social networking platforms. However, upon closer examination, this interpretation is over-inclusive and improper. As a result, courts have erroneously immunized social networking platforms, limiting available redress for cyberbullying victims.

In *Stratton Oakmont, Inc. v. Prodigy Services Corp.*, a supreme court in New York held Prodigy, an ISP, liable for defamatory statements posted by third parties on its online bulletin board.[60] Congress passed § 230 of the CDA one year later in large part as a response to the *Stratton Oakmont* decision,[61] "to remove the disincentives to selfregulation" that it imposed.[62] According to Congress, § 230 was intended to

57. *See* Gleicher, *supra* note 19, at 341–43 (stating how the standards set forth in *Cahill*, *Mobilisa*, and *Krinsky* "demand stronger showings of plaintiffs," *id.* at 343, than those set forth in *Seescandy.com*, *In re AOL*, *Dendrite*, and *2TheMart.com*).

58. While the court may adopt the summary judgment standard from *Dendrite*, 775 A.2d at 760, it may modify this standard because the standard can be "confusing and varie[s] between jurisdictions." Gleicher, *supra* note 19, at 343; *see also Krinsky*, 72 Cal. Rptr. 3d at 244 ("We find it unnecessary and potentially confusing to attach a procedural label, whether summary judgment or motion to dismiss, to the showing required of a plaintiff seeking the identity of an anonymous speaker on the Internet."). Therefore, absent existing case law in the relevant jurisdiction, a victim should set forth information to satisfy *Dendrite*'s rigorous standard, even though the court may choose to adopt a lesser standard.

59. *See infra* notes 61–66 and accompanying text.

60. 1995 WL 323710, at *7 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 133, 138–39 (codified at 47 U.S.C. § 230 (2012)).

61. H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) ("One of the specific purposes of [§ 230] is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

62. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) ("Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230's broad immunity 'to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.'" (quoting 47 U.S.C. § 230(b)(4))).

promote the freedom of the Internet,[63] and included significant "Good Samaritan" protections.[64] These protections state that "interactive computer service[s]"[65] are not treated as publishers or speakers of content, and cannot be liable for taking good faith actions to remove or restrict access to objectionable content by third-party users.[66]

One year after Congress adopted § 230, the U.S. Court of Appeals for the Fourth Circuit in *Zeran v. America Online, Inc.* interpreted its provisions to grant immunity to "a service provider for the exercise of its editorial and self-regulatory functions."[67] Zeran's claims stemmed from messages an anonymous user posted on an America Online (AOL) bulletin board.[68] The messages advertised t-shirts bearing offensive slogans related to the 1995 Oklahoma City bombing, and directed anyone interested in buying a shirt to call "Ken" at Zeran's home phone number.[69] As a result, Zeran received death threats and angry phone calls, which increased after a radio station reported the story and urged listeners to call.[70] Zeran sued AOL, an ISP, in part for its delayed removal of the defamatory messages.[71] The *Zeran* court, interpreting § 230 of the CDA, granted AOL immunity for the defamatory postings by the anonymous third-party user.[72]

---

63. 47 U.S.C. § 230(b)(2) ("It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation[.]").

64. *Id.* § 230(c).

65. The statute defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id.* § 230(f)(2).

66. *Id.* § 230(c). The section reads in full:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material.
>
> (1) Treatment of publisher or speaker: No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability: No provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [subparagraph (A)].

Id.

67. 129 F.3d 327, 331 (4th Cir. 1997).

68. *Id.* at 329.

69. *Id.*

70. *Id.*

71. *Id.* at 328.

72. *Id.*

Courts have applied *Zeran* to extend CDA immunity to social networking platforms. For example, in *Doe v. Myspace, Inc.*, the U.S. Court of Appeals for the Fifth Circuit held that § 230 immunized Myspace, a social networking platform, from liability for a Myspace user's sexual assault of a plaintiff's thirteen-year-old daughter.[73] Though the court acknowledged the challenge *Zeran*'s interpretation of § 230 places on a victim seeking redress, it reiterated the *Zeran* court's finding that victims have other recourses against the content creator.[74]

Subsequently, courts have followed *Myspace* and extended § 230 immunity to social networking platforms. For example, in *Gaston v. Facebook, Inc.*, the U.S. District Court of Oregon applied § 230 to immunize Facebook from the plaintiff's defamation claim.[75] Without much analysis, the court stated that the defendants—Facebook, Google, and Lexis Nexis—"clearly fall within [the] definition" of "interactive computer service" for § 230 immunity.[76] Similarly, in *Klayman v. Zuckerberg*, the U.S. District Court for the District of Columbia granted Facebook immunity against the plaintiff's assault and negligence claims.[77] The court found that "[r]estricting a defendant's liability as an information content provider to information actually created or developed by the defendant . . . is in keeping with the stated policy of the CDA."[78]

The *Myspace*, *Gaston*, and *Klayman* decisions help demonstrate the problem created by the *Zeran* court: "[B]y setting a precedent that the [CDA] bars all defamation claims for content posted by third parties," social networking platforms receive absolute

73. 528 F.3d 413, 418 (5th Cir. 2008). Additionally, the court refused to accept the plaintiffs' later argument that Myspace's activity placed them outside § 230 immunity because Myspace "was partially responsible for creating information exchanged between" the victim and the user. *Id.* at 422. The court did not consider this argument because the claim was not presented to the district court, thereby barring the plaintiffs from raising the argument on appeal. *Id.*

74. *Id.* at 419 ("[T]hey may sue the third-party user who generated the content, but not the . . . service that enabled them to publish the content online."); *see also Zeran*, 129 F.3d at 330 ("None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability.").

75. No. 3:12-cv-0063-ST, 2012 WL 629868, at *7 (D. Or. Feb. 2, 2012). Specifically, the plaintiff claimed that the defamatory statements posted online forced him into bankruptcy, to quit law school, to live out of his car, and resulted in the denial of "relationships and anything he applie[d] for." *Id.* at *3 (citation omitted). These claims mirror those often asserted by victims of cyberbullying. Dictionary definitions of "defamation" include "the act of defaming; false or unjustified injury of the good reputation of another, as by slander or libel; calumny." *Defamation*, Dictionary.com, http://www.dictionary.com/browse/defamation (last visited Apr. 6, 2017). For defamatory statements described in the cyberbullying context, see *infra* note 90.

76. *Gaston*, 2012 WL 629868, at *7.

77. 910 F. Supp. 2d 314, 321 (D.D.C. 2012).

78. *Id.* Although the court relied on *Blumenthal v. Drudge* to support its reading of the CDA, *id.* at 320–21, the *Blumenthal* court heavily relied on *Zeran*'s interpretation of the CDA's immunity provisions. *See* Blumenthal v. Drudge, 992 F. Supp. 44, 50–52 (D.D.C. 1998).

immunity.[79] While cases exist where a platform was *not* immune under the CDA, such cases are often distinguishable from those brought by victims of cyberbullying.[80]

Judges are not blind to the perverse implications of *Zeran*. In *Grace v. eBay, Inc.*, the California Second Division Court of Appeal recognized that if ISPs are immune from distributor liability *and* publisher liability, as suggested by *Zeran*, ISPs need not fear liability and have no incentive to develop filtering and blocking technologies or to monitor for malicious content.[81] Despite judicial awareness of the pitfalls of *Zeran*, the decision has continued to singlehandedly eliminate all avenues of redress for victims beyond the individual aggressor, whether or not the aggressor can be identified.

The *Zeran* decision itself exemplifies how victim redress is nearly impossible. First, Zeran faced the burdens of the unmasking process described in Part II.A. Specifically, he claimed that he could not bring any action against the individual aggressor because "AOL made it impossible to identify the original party by failing to maintain adequate records of its users."[82] Faced with the inability to hold his aggressor accountable, Zeran brought a separate defamation action in the U.S. District Court for the Western District of Oklahoma against the radio station that further publicized the information.[83] The radio station moved for summary judgment and the court granted the motion. The Tenth Circuit subsequently affirmed the decision to grant summary judgment on several grounds, including that the talk show host's failure to verify the authenticity of the Internet posting did not meet the standard of recklessness.[84] Like many victims, Zeran lost any chance of redress—his aggressor was unidentifiable and the judiciary denied his claims against the remaining parties.

An additional problem with *Zeran* is the over-inclusive and improper interpretation of § 230. First, the Fourth Circuit found that § 230 grants immunity to "publishers" of information *and* "distributors" of information.[85] However, the CDA removes

79. Ottenweller, *supra* note 20, at 1320.

80. *See, e.g.*, Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 803 (N.D. Cal. 2011) (holding that the CDA did not grant Facebook immunity). In *Fraley*, the plaintiffs sued Facebook for misappropriation of their names, photographs, and identities in paid advertisements in Facebook "Sponsored Stories." *Id.* at 790. The court agreed with the plaintiffs' argument that "Facebook contributes, at least in part, to the creation or development of the Sponsored Stor[ies]," and denied Facebook's motion to dismiss under § 230 immunity. *Id.* at 801–03. Under this framework, a victim must show that the social networking platform assisted in the creation of the cyberbullying material.

81. 16 Cal. Rptr. 3d 192, 201 (Ct. App. 2004) ("[T]he total elimination of distributor liability under *Zeran* would eliminate a potential incentive to the development of [filtering] technologies, that incentive being the threat of distributor liability.").

82. Zeran v. Am. Online, Inc., 129 F.3d 327, 329 n.1 (4th Cir. 1997).

83. Zeran v. Diamond Broad. Inc., 19 F. Supp. 2d 1249, 1251–52 (W.D. Okla. 1997) (claiming that after the radio station broadcast regarding the AOL post, Zeran received an increased number of calls, including death threats, resulting in sleep deprivation and anxiety), *aff'd*, 203 F.3d 714 (10th Cir. 2000).

84. *Zeran*, 203 F.3d at 720. Additionally, the court remanded the case to consider whether the station should receive its costs. *Id.* at 722–23.

85. *Zeran*, 129 F.3d at 332.

liability from a "publisher or speaker,"[86] and explicitly omits the term "distributor."[87] In addressing this omission, the court disagreed with Zeran's argument that AOL is a distributor, not a publisher.[88] The court concluded that the CDA forecloses distributor liability, asserting that distributor liability is a subset of publisher liability for the purpose of defamation law.[89]

This interpretation is inconsistent with well-established common law principles of defamation liability. Like Zeran, victims of cyberbullying share similar defamation claims.[90] In defamation actions, courts identify three levels of liability by the corresponding degrees of an entity's control over content.[91] Specifically, publishers (of newspapers and books, for example) may be held strictly liable for disseminating defamatory content; distributors (such as booksellers and libraries) are subject to notice-based liability; and common carriers (such as telephone and cable companies) are not liable for defamatory content.[92] Such degrees of liability are deeply embedded in U.S. jurisprudence,[93] and case law dating back to the nineteenth century.[94] However, by grouping distributors with publishers for § 230 immunity, the *Zeran* court ignored this framework and made it nearly impossible for *any* entity—publisher, distributor, or common carrier—to face liability for defamatory or offensive content.

86. The relevant provision reads, in part, "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1) (2012).

87. "[T]he placement of 'speaker' alongside 'publisher' suggests that Congress meant for the [CDA] to eliminate *only* primary publisher liability for ISPs, but to keep distributor liability intact." Ottenweller, *supra* note 20, at 1316 (emphasis added).

88. *Zeran*, 129 F.3d at 331–32 (rejecting the plaintiff's argument that ISPs are normally considered to be distributors).

89. *Id.* at 332.

90. *See* Ottenweller, *supra* note 20, at 1296–97. Defamatory statements include "false statements [that] are posted and published for the sole purpose of harming the reputation of a fellow classmate or peer." *Id.* at 1297.

91. Paul Ehrlich, Note, *Communications Decency Act § 230*, 17 Berkeley Tech. L.J. 401, 403 (2002).

92. *Id.* The entity's control over content indicates the level of liability it may face. *Id.* Publishers face the greatest liability because of their ability to control the final content; distributors face liability only if there is evidence that they knew or should have known of the content and failed to remove it because they only control content through delivery or transmission; finally, common carriers do not face liability because they merely "transmit information mechanically with no opportunity to review its content." *Id.*; *see also* Ottenweller, *supra* note 20, at 1297–98.

93. *See* Hoover v. Peerless Publ'ns, Inc., 461 F. Supp. 1206, 1209 (E.D. Pa. 1978) ("[T]he black-letter rule [states] that one who republishes a libel is subject to liability just as if he had published it originally, even though he attributes the libelous statement to the original publisher, and even though he expressly disavows the truth of the statement.").

94. *See, e.g.*, Metcalf v. Times Publ'g Co., 40 A. 864, 865 (1898) ("As a publisher of news and items of public importance the press should have the freest scope, but as a scandal monger it should be held to the most rigid limitation. If a man has not the right to go around to tell of charges made by one against another, much less should a newspaper have the right to spread it broadcast and in enduring form.").

This over-inclusive reading of § 230 becomes even more problematic in the context of social networking platforms and their unique operations. Unlike publishers, distributors do not affirmatively exercise control over content and thus receive the lesser notice-based liability.[95] Generally, social networking platforms reserve the right to remove any content that does not meet their terms of use or to delete a user's account for violations.[96] Platforms do not control the substance of user-generated content, but typically employ individuals to *retroactively* review content and user-generated notifications of offensive content,[97] operating like distributors. By abolishing distributor liability, *Zeran* leaves the original content creator as the only person who can be liable.[98] As a result, platforms receive immunity, even when one operates as a distributor *and* receives notice of the defamatory or cyberbullying material, which diverts from the long-established legal approach.[99]

Additionally, grouping social networking platforms as publishers is fundamentally improper. Unlike traditional publishers, some platforms *create* content, thereby making § 230 immunity inapplicable.[100] For instance, Facebook and Myspace provide new users with pre-made answers to questions.[101] Accordingly, grouping such platforms as publishers under *Zeran*'s view of § 230 ignores these functions.

95. *See* Ehrlich, *supra* note 91, at 403.

96. *See, e.g.*, *The Twitter Rules*, Twitter Help Ctr., https://support.twitter.com/articles/18311 (last visited Apr. 6, 2017).

97. For examples of violation reporting and social networking platform review procedures, see *Abuse & Spam*, Instagram Help Ctr., https://help.instagram.com/165828726894770 (last visited Apr. 6, 2017); *Community Guidelines*, Tumblr, https://www.tumblr.com/policy/en/community (last modified June 23, 2016); *Report Something*, Facebook Help Ctr., https://www.facebook.com/help/263149623790594 (last visited Apr. 6, 2017); *The Twitter Rules*, *supra* note 96. Platforms such as Facebook and Twitter grant users nearly complete control over content they post and only remove content—exercising editorial control—after receiving reports from other users of content violations. *See* Nina Bahadur, *Why Instagram Removed This Woman's Picture*, Huffington Post (May 20, 2014), http://www.huffingtonpost.com/2014/05/20/meghan-tonjes-instagram_n_5353804.html (reporting on Instagram's removal of a video blogger's image, which displayed her backside covered only by underwear, after Instagram received notice that the image violated the platform's anti-pornography guidelines); Miguel Helft, *Art School Runs Afoul of Facebook's Nudity Police*, N.Y. Times: Bits (Feb. 18, 2011, 8:50 PM), http://bits.blogs.nytimes.com/2011/02/18/art-school-runs-afoul-of-facebooks-nudity-police (describing an instance when Facebook removed an image of an artistic drawing posted by the New York Academy of Art after receiving notice that the image violated the platform's nudity guidelines, only to later claim that the removal was a "mistake" and re-post the image).

98. *See* Amanda Groover Hyland, *The Taming of the Internet: A New Approach to Third-Party Internet Defamation*, 31 Hastings Comm. & Ent. L.J. 79, 82 (2008) ("The results of the *Zeran* interpretation have been problematic. By abolishing distributor liability, usually the only defendant that can be held accountable is the original content creator. *This outcome is particularly frustrating when the . . . operator had an active role in posting the content or was otherwise acutely aware of the defamatory statement's existence on its web space*." (emphasis added)).

99. Ottenweller, *supra* note 20, at 1319–20.

100. *See* Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 801–03 (N.D. Cal. 2011).

101. On both Facebook and Myspace, users can choose from options when answering questions regarding their sex, relationship status, and other personal information. *See, e.g.*, Doe v. Myspace, Inc., 528 F.3d 413, 420 (5th Cir. 2008) (discussing the claim that Myspace partially created the content at issue by facilitating a user's profile creation and choosing the information users share publically via a questionnaire).

Contributing to user content distinguishes social networking platforms from ISPs, which receive immunity under the *Zeran* court's interpretation of § 230.[102] The grant of immunity to social networking platforms where the platform *contributes* to user content—although not necessarily in the cyberbullying context—conflates social networking platform cases with ISP cases. As a result, subsequent courts improperly grant blanket immunity to platforms and erroneously limit a victim's redress to the individual aggressor.

III. THE IMPACT: PROBLEMS AND SCOPE OF REDRESS LIMITATIONS

While the challenges of unmasking a cyberbullying aggressor burdens a victim seeking redress from the aggressor, the application of CDA immunity eliminates the prospect of seeking relief from the platform on which the cyberbullying occurred. These two redress problems affect not only the victims of cyberbullying, but also legal traditions, public policy, and society. First, immunizing social networking platforms departs from established legal principles of third-party liability. Second, platforms owe a duty to protect users from offensive content, and by limiting victim redress to the individual aggressor the landscape creates a disincentive to upholding this duty. Finally, granting platforms immunity removes incentives for platforms to effectively combat cyberbullying, thereby facilitating the problem.

Under the current approach, CDA immunity impedes a victim's ability to hold a third party liable for the unlawful acts of another, departing from a principle recognized in other areas of law. For example, intellectual property law recognizes secondary liability for copyright and trademark infringement.[103] Generally, secondary liability requires showing that the third party knew or should have known of the direct infringer's activity,[104] and willful blindness rarely excuses liability.[105] Vicarious liability in this context stems from the agency doctrine of respondeat superior,[106]

102. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (interpreting § 230 to grant immunity for the exercise of the "editorial and self-regulatory functions" of a service provider).

103. *See* MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) ("Although '[t]he Copyright Act does not expressly render anyone liable for infringement committed by another,' these doctrines of secondary liability emerged from common law principles and are well established in the law." (alteration in original) (citation omitted) (quoting Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 434 (1984))).

104. *See* Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 860 (1982) ("[A] finding of contributory [trademark] infringement requires proof of either an intent to induce illegal substitution or continued sales to particular customers whom the manufacturer knows or should know are engaged in improper palming off." (citing William R. Warner & Co. v. Eli Lilly & Co., 265 U.S. 526 (1924))); Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (articulating the vicarious liability test for copyright infringement as "even in the absence of an employer-employee relationship one may be vicariously liable if he has the *right and ability to supervise* the infringing activity and also has a *direct financial interest* in such activities" (emphasis added)).

105. *See* Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1149 (7th Cir. 1992) ("To be willfully blind, a person must suspect wrongdoing and deliberately fail to investigate." (citing Louis Vuitton S.A. v. Lee, 875 F.2d 584, 590 (7th Cir. 1989))).

106. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 260–62 (9th Cir. 1996) (applying vicarious liability to copyright infringement by third-party venders). For "respondeat superior" defined, see *infra* note 108.

applied in both tort and criminal law[107] to determine employer liability for acts by an employee.[108] This doctrine dates back to the sixteenth century,[109] and vicarious liability for copyright infringement traces its roots back to the early twentieth century.[110] In contrast to intellectual property, tort, and criminal law, the landscape of CDA immunity departs from the lengthy history of third-party liability.

Law professors Doug Lichtman and Eric Posner identify two factors that traditionally warrant third-party liability: control and activity-level.[111] Liability is warranted when one party is able to "control" another party's bad acts, and when liability may serve to motivate a party to account for her "activities" in light of the negative effects they may have.[112] At a minimum, social networking platforms satisfy the control factor because of their ability to instantly remove cyberbullying content or delete a user's account for violations.[113] Accordingly, it is logical to hold platforms accountable when their operations satisfy at least one of these two factors. Wrongfully granting them immunity under § 230 then obstructs a victim's redress options and departs from well-settled legal traditions.

Eliminating platform accountability also creates bad public policy. Platforms are aware that users post unauthorized content, and many platforms therefore establish community standards for what kind of content users can and cannot post. For instance, Facebook and Instagram forbid discriminatory and hateful speech.[114] Violations are so widespread that many platforms even review certain content *before* it is posted.[115] As a result, platforms have established a self-made duty to protect

107. Commonwealth v. Koczwara, 155 A.2d 825, 827 n.1 (Pa. 1959) (discussing the application of respondeat superior in the criminal context for the charges at issue, as compared to its application in tort law).

108. *See* Jeffrey S. Nowak, Note, *Employer Liability for Employee Online Criminal Acts*, 51 Fed. Comm. L.J. 467, 471 (1999) ("The traditional basis for an employer's liability for its employees' acts is the doctrine of respondeat superior, under which the employer is liable for employee acts that are within the scope of employment or in furtherance of the employer's interest.").

109. *See* Rhett B. Franklin, Comment, *Pouring New Wine into an Old Bottle: A Recommendation for Determining Liability of an Employer Under Respondeat Superior*, 39 S.D. L. Rev. 570, 573–74 (1994).

110. *See* Kalem Co. v. Harper Bros., 222 U.S. 55 (1911) (holding that a film production company was liable for copyright infringement when it distributed a film based on the content of a book to free lancers who executed the work); Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304 (2d Cir. 1963) (holding that a department store was vicariously liable when a record concession within the department store infringed on phonograph record copyrights).

111. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 Sup. Ct. Econ. Rev. 221, 230–33 (2006).

112. *Id.* at 230–31.

113. *See supra* notes 96–97 and accompanying text.

114. *Community Standards*, Facebook, https://www.facebook.com/communitystandards (last visited Apr. 6, 2017); *Terms of Use*, Instagram Help Ctr., http://instagram.com/legal/terms (last visited Apr. 6, 2017).

115. For example, Grindr, a social dating platform for gay men, reviews a user's profile photograph for nudity before it is made public. *See Grindr Profile Guidelines*, Grindr, http://grindr.com/profile-guidelines (last visited Apr. 6, 2017). Additionally, Instagram removes users' ability to search hashtags it deems inappropriate; for example, hashtags that promote self-harm such as "probulimia" and "proanorexia."

users from offensive content, and some have even created anti-cyberbullying campaigns.[116] Therefore, eliminating accountability is illogical and would serve as a disincentive for platforms to protect users from cyberbullying content.

Platform immunity is also unjust because of the vast resources available to many social platforms that could address cyberbullying content. Facebook, for example, is estimated to be worth $350 billion.[117] Social networking platforms employ large numbers of individuals: Recent statistics show that Facebook employs over 17,000 people[118] and Twitter employs over 3,800 people.[119] Moreover, these platforms pay large amounts in damages to plaintiffs in successful suits.[120] Thus, social networking platforms could easily relocate a fraction of their resources to input monitoring mechanisms that combat cyberbullying, ultimately placing them in the best position to make a victim whole.

Finally, immunizing social networking platforms affects all of us by perpetuating the cyberbullying problem. Immunity allows platforms to ignore removal requests for cyberbullying content, forcing victims to "endure the embarrassment or avoid using the Internet altogether in an effort to remain psychologically healthy."[121] The dangers are widespread and the harm is real. In December 2016, Facebook reported an average of 1.23 billion daily users,[122] while a 2016 survey of over 5,000 middle school and high school students in the United States found that nearly thirty-four per cent of students between the ages of twelve and seventeen claimed to have experienced cyberbullying.[123] In the aftermath of Tyler Clementi's, Amanda Todd's, and Rebecca Sedwick's suicides,[124] the problem remains so vast that scholars Sameer Hinduja and Justin W.

Instagram's New Guidelines Against Self-Harm Images & Accounts, Instagram: Blog (Apr. 20, 2012), http://blog.instagram.com/post/21454597658/instagrams-new-guidelines-against-self-harm-images. However, this should not affect the argument *supra* Part II.B that platforms qualify as distributors because in the Grindr and Instagram examples, the platforms do not control the substance of the final post (as a newspaper would). They merely ensure that content meets certain guidelines.

116. *E.g.*, *Put a Stop to Bullying*, Facebook, https://www.facebook.com/safety/bullying (last visited Apr. 6, 2017).

117. Paul R. La Monica, *Facebook Worth $1 Trillion? Not So Crazy*, Cnn Money (July 21, 2016, 2:13 PM), http://money.cnn.com/2016/07/21/investing/facebook-stock-trillion-dollar-market-value.

118. *Company Info*, Facebook Newsroom, http://newsroom.fb.com/company-info (last visited Apr. 6, 2017).

119. *About*, Twitter, https://about.twitter.com/company (last visited Apr. 6, 2017).

120. For example, in *Fraley*, the court required Facebook to pay the class $20 million. Fraley v. Facebook, Inc., 966 F. Supp. 2d 939, 943–44 (N.D. Cal. 2013), *aff'd sub nom.* Fraley v. Batman, 638 Fed. App'x 594 (9th Cir. 2016).

121. Ottenweller, *supra* note 20, at 1326; *see also* Bryan H. Choi, *The Anonymous Internet*, 72 Md. L. Rev. 501, 539 (2013) ("When anonymity allows perpetrators to escape detection, harms go unredressed and the aggregate incidence of harmful behavior increases." (footnote omitted)).

122. *Company Info*, *supra* note 118.

123. Justin W. Patchin, *2016 Cyberbullying Data*, Cyberbullying Res. Ctr. (Nov. 26, 2016), http://cyberbullying.org/2016-cyberbullying-data.

124. *See supra* notes 1–6 and accompanying text.

Patchin created the term "cyberbullicide" to describe suicide that occurs as a result of online victimization.[125] Furthermore, Facebook recently formalized its suicide prevention efforts with a new feature that allows users to report potential instances of self-harm directly from another user's post.[126]

Upon notice of alleged cyberbullying, platforms are able to decide whether to remove the objectionable content. The longer the post exists, the broader its dissemination and the greater the harm to the victim.[127] Accordingly, Part IV proposes a solution that incentivizes platforms to expeditiously respond to cyberbullying or risk liability.

IV. THE SOLUTION: A DMCA-LIKE PROCESS FOR REDRESS

Scholars have recognized a victim's challenge to gain redress as well as the problematic application of CDA immunity. This note reviews three scholarly proposals and how each fails to solve a victim's redress problem. The redress problem requires a novel approach to limit CDA immunity. This proposal, set forth in Appendix A, presents the best method to provide victims with redress, while keeping certain protections in place for social networking platforms and their users.

The first proposal addresses the unmasking problem. Nathaniel Gleicher presents a uniform standard for courts to consider when addressing an unmasking request that balances the First Amendment interests of both plaintiffs and defendants.[128] Gleicher's standard involves four elements,[129] which add to the central factors of unmasking standards—notice and a prima facie showing by the plaintiff—third-party notice requirements and the explicit evaluation of factors courts previously considered

125. Hinduja & Patchin, *supra* note 28, at 66–71, 185.

126. Alexis Kleinman, *Facebook Adds New Feature for Suicide Prevention*, Huffington Post (Mar. 2, 2015), http://www.huffingtonpost.com/2015/02/25/facebook-suicide-prevention_n_6754106.html. With this feature, a user suspected of considering self-harm is prompted with a notice and can choose to reach out to friends or suicide hotlines or receive tips on how to deal with suicidal thoughts. *Id.*

127. *See* Shira Auerbach, Note, *Screening Out Cyberbullies: Remedies for Victims on the Internet Playground*, 30 Cardozo L. Rev. 1641, 1643 (2009) ("Because of its accessibility, . . . Internet content is often disseminated to a wide audience, thereby strengthening its impact.").

128. Gleicher, *supra* note 19, at 362–63.

129. The four elements are as follows:

> First, both the recipient of the subpoena and the plaintiff should make reasonable efforts to notify the defendant, including notice via the same medium used by the defendant to send or post the contested message. . . .
>
> Second, the court should evaluate the strength of the plaintiff's argument. . . .
>
> Third, the plaintiff shall demonstrate that each specific element of information sought by subpoena is necessary for the identification of the defendant, and that the defendant's identity is central to the continuation of the plaintiff's case. . . .
>
> Fourth, if the first three factors do not yield a clear outcome, the court should balance the parties' interests, giving preference to the party whose hardships and First Amendment interests are greater.

Id. at 363.

implicitly.[130] However, despite lessening the challenge victims would face with a uniform unmasking standard,[131] the proposal fails to solve the need for *additional* redress beyond the individual aggressor to properly make a victim whole.[132]

Another proposal by Cara J. Ottenweller returns judicial focus to the traditional common law tort of defamation by interpreting § 230 to provide ISPs only *qualified* immunity.[133] Under this proposal, an exception to immunity would treat a provider as a distributor, holding it liable for failure to remove defamatory content if it knows or has reason to know of the defamatory material.[134] This exception returns to *Stratton Oakmont*'s landscape, which holds ISPs liable as distributors, and recognizes that Congress never intended the CDA to grant *blanket* liability to ISPs.[135] However, Ottenweller's proposal falls short by providing a broad definition of "distributor,"[136] creating a grey area for courts to find that social networking platforms do not qualify and thus leave them immune to a victim's claims.[137]

Finally, Bradley A. Areheart proposes a practical solution to combat cyberbullying with a notice-based liability scheme.[138] His proposal adopts the DMCA process,[139] in which upon receiving particularized notice,[140] an ISP must disable or remove offensive content (or have the user remove it) or risk liability.[141] Areheart claims the proposal creates economic incentives for ISPs to be sensitive to user complaints and to ensure that they have mechanisms in place to respond to takedown requests.[142] However, this fails to solve the redress problem many victims face because it only addresses ISPs, not social networking platforms and the growth of cyberbullying

130. *Id.* Additionally, Gleicher claims this proposal is bifurcated to provide stronger protection for speech targeting public figures and to protect speech on matters of public concern. *Id.* at 363–64.

131. *See supra* Part II.A (discussing the haphazard application of unmasking standards and the resulting uncertainty).

132. *See, e.g.*, *supra* Part II.B (discussing that whether or not a uniform unmasking standard existed at the time of *Zeran*, AOL's inability to identify Zeran's individual aggressor would still leave Zeran without available redress).

133. Ottenweller, *supra* note 20, at 1326.

134. *Id.* at 1327, 1330.

135. *Id.* at 1329.

136. A distributor would be defined as "any person or entity that delivers or transmits information . . . through the Internet . . . without exercising editorial control over the information." *Id.* at 1328.

137. According to Ottenweller, if an ISP takes editorial control and screens for harmful content, the CDA would preclude ISP liability. *Id.* at 1332. This leaves open judicial findings that social networking platforms, by screening for offensive content either before or after notice, could remain immune.

138. Areheart, *supra* note 7. Areheart recognizes that "victims currently lack meaningful redress, but modestly reforming ISP immunity could give them effective options." *Id.* at 42.

139. 17 U.S.C. § 512(c)(1) (2012).

140. Areheart, *supra* note 7, at 46. If notice is not sufficient, the ISP may remain immune. *Id.* Areheart argues that this caveat limits incentives for ISPs to over-comply with takedown requests. *Id.*

141. *Id.*

142. *Id.* at 47.

thereon.[143] This note adopts a modified version of Areheart's proposal, extending it to such social platforms and providing recommended language for such a process.

Congress passed the DMCA in 1998 just two years after adopting § 230, establishing a takedown procedure[144] that requires ISPs to perform the very activities the *Zeran* court feared.[145] Specifically, the DMCA grants immunity to service providers[146] from copyright infringement claims if the provider falls under its safe harbor provisions.[147] The provisions grant providers immunity for not knowing that copyright material stored on its network is infringing, or for removing or disabling access to the material quickly upon learning of its infringement.[148] Apparently, Congress felt confident in a provider's ability to review and respond to such notices.

Although both the CDA and the DMCA divert from established levels of liability for offensive content,[149] the CDA's safe harbor *grants immunity* for nearly *all* providers, while the DMCA's safe harbor *limits liability* for *qualified* providers.[150] Congress narrowly limited immunity under the DMCA, reasoning that case law on secondary liability for copyright infringement is evolving and cannot fit within traditional vicarious liability standards.[151] Similarly, cyberbullying on social networking platforms is evolving and does not fit within the traditional legal framework.[152] Therefore, the DMCA properly addresses an uncertain area of law without granting blanket immunity, instead drawing clear procedures for *limiting* liability.

The proposal requires amending the CDA to include a new section or passing a standalone statute specific to cyberbullying on social networks. Unlike Ottenweller's approach, this proposed process is nearly identical to the DMCA's process: A platform shall not be liable for cyberbullying without actual knowledge or awareness of the activity.[153] If a platform receives notice of cyberbullying, or obtains knowledge or awareness on its own, it must either *immediately* remove the content or disable the creator's account. Similar to the DMCA, if notice of cyberbullying is not sufficiently particularized, the platform may not be liable for failing to remove the content.

---

143. *See supra* note 11 and accompanying text, and text accompanying note 123; *see also* Patchin, *supra* note 123.

144. 17 U.S.C. § 512(c)(1).

145. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

146. Under the DMCA, a "service provider" is defined as "an entity offering the transmission, routing, or providing of connections of digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received," 17 U.S.C. § 512(k)(1)(A), and "a provider of online services or network access, or the operator of facilities therefor," *Id.* § 512(k)(1)(B).

147. *Id.* § 512(c)(1).

148. *Id.*

149. *See supra* notes 90–93 and accompanying text.

150. *See* S. Rep. No. 105-190, at 18–19, 36–37 (1998).

151. *See* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 Colum. J.L. & Arts 233, 249–50 (2009).

152. *See supra* text accompanying notes 85–99.

153. For the full proposal, see *infra* Appendix A.

Designated agents review notices to determine particularity, but if identifying cyberbullying requires further investigation,[154] the content is temporarily removed. Upon further investigation, if an agent determines no cyberbullying occurred, the content is re-posted and the platform receives immunity (as it would under § 230).

The benefits of this process far outweigh any drawbacks. First and foremost, victims obtain the ability to hold accountable an additional, easily identifiable entity. Specifically, the victim has the ability to seek redress from the social media platform instead of trying to unmask hers or the anonymous aggressor's identity through the lengthy and complex unmasking process.[155] To address congressional concerns regarding liability for third-party generated content,[156] this process properly immunizes platforms from claims when specific remedial steps are taken. For example, like the DMCA's safe harbor provisions,[157] the proposal immunizes a platform if it "responds expeditiously to remove the claimed cyberbullying material or to disable the account of the user posting the claimed cyberbullying material."[158] Additionally, the notice process does not unduly burden platforms,[159] considering that many currently have employees reviewing user requests for content removal.[160] In fact, contrary to the concern expressed by the Fourth Circuit in *Zeran* that notice-based liability "would deter service providers from regulating the dissemination of offensive material,"[161] platforms are incentivized to take notices seriously and to act expeditiously to mitigate harm.[162]

The proposed solution also considers First Amendment concerns regarding the right to speak freely online.[163] Under the CDA, a provider can remove or block speech protected under the First Amendment whether or not it receives a request for

154. *See* Goldman, *supra* note 2 (discussing the differences between bullying and normal conflict).

155. The proposal attempts to circumvent the need to unmask an anonymous cyberbully entirely. The proposal seeks to provide what the current legal landscape does not—redress for the victim and an identified entity to hold liable. If the social networking platform fails to adhere to the DMCA-like notice, the victim can hold it liable. Of course, the platform may invoke indemnification found in its terms of use and require that the anonymous cyberbully defend it against the victim's claims. Even in such an event the victim, in the weaker position, is not faced with the burden of unmasking the bully—it is in the hands of the platform that already knows identifiable information about the anonymous individual.

156. *See supra* note 61 and accompanying text.

157. 17 U.S.C. § 512(c)(1) (2012).

158. *Infra* Appendix A.

159. Further, the process *fairly* burdens victims and platforms by requiring particularized notice and prompt review.

160. *See supra* notes 96–97 and accompanying text.

161. Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) ("Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at self-regulation.").

162. According to Areheart, a DMCA-like scheme is the "first step in requiring [platforms] to take a more involved role in addressing torts in cyberspace." Areheart, *supra* note 7, at 47.

163. *See supra* notes 30–32 and accompanying text. Areheart also addressed First Amendment objections in his proposal:

removal.[164] Alternatively, free speech receives *stronger* protection under the proposal by requiring platforms to make a determination as to whether the speech is harmful, based on the review of a detailed notice *before* removal.[165] Under the proposal, a designated Reviewing Agent reviews a detailed Notification of Claimed Cyberbullying intended to adequately provide the Agent with sufficient knowledge of whether the content is cyberbullying or potentially protectable free speech.[166]

Another aspect of this DMCA-like solution highlights the unique functions of social networking platforms to combat First Amendment objections. Scholars note that restoring liability for user-generated content involves a trade-off,[167] one that would eliminate user comments on online platforms to avoid any possible liability.[168] However, such a hypothetical cannot logically extend to social networking platforms. In their most basic form, they essentially *require* user-generated content to operate; there would be no Facebook without profiles and no Twitter without tweets.[169] While such objections may bear on other online community forums, the proposed notice-based liability scheme would not stifle user-generated content on social networking platforms beyond proscribing harmful speech.

> [I]mposing liability only for actual knowledge would limit collateral damage to protected forms of speech by not providing any incentive or requirement for ISPs to police the Internet. . . .
>
> . . . ISPs, like newspapers, obtain economic benefits by providing a forum for highly controversial material that will make it worth the risks to continue to do so in the future. Accordingly, First Amendment concerns may well be over-stated.

Areheart, *supra* note 7, at 45.

164. *See* Ottenweller, *supra* note 20, at 1323 ("The very wording of the statute suggests that Congress gave ISPs the green light to remove or block offensive material, including instances of cyberbullying, even if such material would traditionally be protected by the Constitution. Therefore, the words used in the statute coupled with the actual purpose of the CDA suggests that the *Zeran* court placed too much weight on the policy of free speech on the Internet.").

165. Additionally, free speech on social networking platforms can be distinguished from speech historically protected under the First Amendment. *See* Renee L. Servance, Comment, *Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment*, 2003 Wis. L. Rev. 1213, 1235 ("Not only is Internet speech ever-present but one can also quickly and easily disseminate its content to an infinite number of people. This situation stands in stark contrast to flyers, posters, newspapers, speeches, and other traditional forms of expression that reach a far more limited audience and exist in a particular time and place.").

166. *See infra* Appendix A.

167. *See* Choi, *supra* note 121, at 536.

168. *See id.* ("Reforming section 230 to restore intermediary liability for user-generated defamation would pressure websites to adopt corresponding restrictions that limit their exposure to risky user behavior."); *id.* at 536 n.138 (quoting Jack M. Balkin, *Free Speech and Press in the Digital Age: The Future of Free Expression in a Digital Age*, 36 Pepp. L. Rev. 427, 436 (2009) ("If I were liable for comments posted in response to my blog posts, I simply would not allow any comments. The same is true for online versions of newspapers and magazines . . . . Without section 230, many website operators would simply disable these features.")).

169. *See* Jonathan Strickland, *How Facebook Works*, HowStuffWorks (Dec. 10, 2007), http://computer.howstuffworks.com/internet/ social-networking/networks/facebook.htm; Jonathan Strickland & Nathan Chandler, *How Twitter Works*, HowStuffWorks (Dec. 17, 2007), http://computer.howstuffworks.com/internet/social-networking/networks/twitter.htm.

A final benefit of the proposal is its practical approach that avoids conflict with the CDA and avoids overturning settled case law. Specifically, the proposal runs alongside the CDA, acting as an exception to § 230 immunity, and leaves case law intact. This approach requires platforms—those in the best position to stop the harm—to promptly remove the content, a function many already perform.[170]

Adopting a DMCA-like solution to address cyberbullying is appropriate because the values embodied in the DMCA reflect those in the CDA. In both statutes, Congress sought to protect the freedom and operation of the Internet.[171] Additionally, the DMCA's takedown process—and similarly, the process proposed in this note—mirrors the policy underlying § 230 that online platforms hosting user-generated content do not have the burden to police content violations.[172] The proposed solution effectively furthers the freedom of the Internet without requiring any additional action from social networking platforms beyond the procedures Congress expressly provided for in the DMCA.[173] Therefore, it is both practical and logical to apply the framework of the DMCA to provide adequate redress to victims of cyberbullying.

V. CONCLUSION

The unmasking and immunity problems contribute to the intertwining web of laws and precedent that unfairly eliminates a victim's ability to hold social networking platforms accountable. This landscape forces victims to face aggressors head-on, decreasing the adequacy of available redress and unfairly burdening victims. The redress problem not only affects victims, it also affects legal traditions, public policy, and society. Under the proposed DMCA-like process, platforms risk appropriate liability for failing to mitigate the cyberbullying problem, providing the best solution that balances the interests of victims, users, and platforms. This process may not singlehandedly end cyberbullying, but it addresses the situation better than does the current legal landscape.

---

170. *See supra* notes 96–97 and accompanying text.

171. 47 U.S.C. § 230(b)(2) (2012) (stating that one of several policy considerations listed under subsection (b) is "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation"); S. Rep. No. 105-190, at 49 (1998) ("Information location tools are essential to the operation of the Internet; without them, users would not be able to find the information they need.").

172. *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1022 (9th Cir. 2013) ("Congress made a considered policy determination that the 'DMCA notification procedures [would] place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.'" (alteration in original) (quoting Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007))); *see also* H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) (discussing how § 230 was meant to overrule the burden set forth in *Stratton-Oakmont* that Internet content providers may be liable for failing to remove content created by third-party users).

173. 17 U.S.C. § 512(c)(1)(A)(iii) (2012) (requiring service providers, upon gaining knowledge of allegedly infringing content, to "expeditiously" remove the content in order to receive the statute's Good Samaritan protections).

APPENDIX A

DMCA Provisions[174]	Proposed Cyberbullying Provisions
"A service provider shall not be liable for monetary relief, injunctive or other equitable relief, . . . for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider— (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity . . . ; and (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[175]	(1) Platform Liability. A social networking platform[176] shall not be liable for monetary relief, injunctive relief, or other equitable relief, for cyberbullying activity[177] submitted and posted on the platform's system or network or on an application controlled or operated by the platform, if the platform— (A)(i) does not have actual knowledge of the cyberbullying activity on the platform's system or network; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which cyberbullying activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material. (B) upon Notification of Claimed Cyberbullying, set forth below, the platform responds expeditiously to remove the claimed cyberbullying material or to disable the account of the user posting the claimed cyberbullying material. (2) Platform Review. All social networking platforms shall have at least one designated Reviewing Agent who is a direct employee of the platform, responsible for the review of all Notifications of Claimed Cyberbullying. Platforms without a Reviewing Agent waive any immunity granted herein.
"(3) Elements of notification.— (A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following: (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.	(3) Elements of Notification. Social networking platforms must have in place and available to all users a standard Notification of Claimed Cyberbullying submission form that is immediately submitted to the platform's Reviewing Agent(s) and includes substantially the following— (A) An electronic signature of the individual reporting the cyberbullying activity, where the reporting individual need not be a user of the platform or the victim or intended target of the claimed cyberbullying material;

174. *Id.* § 512.

175. *Id.* § 512(c)(1).

176. "A social platform is a Web-based technology that enables the development, deployment and management of social media solutions and services. It provides the ability to create social media websites and services with complete social media network functionality." *Social Platform*, Techopedia, https://www.techopedia.com/definition/23759/social-platform (last visited Apr. 6, 2017).

177. For the definition of cyberbullying for this note and proposal, see *supra* note 2.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. (iv) Information reasonably sufficient to permit the service provider to contact the complaining party . . . . (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law. (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed."[178]	(B) A URL link, screen shot, or otherwise identifiable evidence of the claimed cyberbullying activity that allows a Reviewing Agent to readily find the cyberbullying activity and the username of the content creator; (C) Information reasonably sufficient to permit the platform or its Reviewing Agent to contact the complaining party; (D) A statement that specifies with sufficient particularity the complaining party's good faith belief that the cyberbullying activity is a violation of the platform's terms of use and is not intended for light-hearted humor; (E) A statement that the information provided in the Notification is accurate and, if determined to be false, acknowledges the platform's ability to disable the complaining party's access to the platform.
"(1) No liability for taking down generally.—Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing. (2) Exception.—Paragraph (1) shall not apply . . . unless the service provider— (A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material; (B) upon receipt of a counter notification . . . , promptly provides the person who provided the notification . . . with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and (C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice . . . ."[179]	A social networking platform shall not be liable to any person for any claim based on the platform's good faith removal of cyberbullying activity, or the disabling of a party's account, based on the Notification of Claimed Cyberbullying, regardless of whether the content is ultimately determined to be cyberbullying activity. If a Reviewing Agent cannot reasonably determine whether the reported material is cyberbullying activity, the Reviewing Agent or the platform must remove the claimed cyberbullying activity and immediately conduct an investigation. If the material is determined not to be cyberbullying activity, the platform must immediately re-post the material but is not liable for the initial removal.
"(m) Protection of privacy.—Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on— (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity . . . ."[180]	(m) Protection of privacy. A social networking platform shall not be required to monitor its system or network or affirmatively seek facts indicating cyberbullying activity unless the platform or its Reviewing Agent(s) have actual knowledge of, or have received a Notification of, specific cyberbullying activity.

178. 17 U.S.C. § 512(c)(3).

179. *Id.* § 512(g)(1)–(2).

180. *Id.* § 512(m).

NEW YORK LAW SCHOOL LAW REVIEW

www.nylslawreview.com