UC Irvine Law Review

Volume 10 | Issue 4 Article 7

6-2020

Civil Liability for Cyberbullying

Ronen Perry

Follow this and additional works at: https://scholarship.law.uci.edu/ucilr

 Part of the Internet Law Commons, and the Law and Economics Commons

Recommended Citation
Ronen Perry, *Civil Liability for Cyberbullying*, 10 U.C. IRVINE L. REV. 1219 (2020).
Available at: https://scholarship.law.uci.edu/ucilr/vol10/iss4/7

This Article is brought to you for free and open access by UCI Law Scholarly Commons. It has been accepted for inclusion in UC Irvine Law Review by an authorized editor of UCI Law Scholarly Commons.

Civil Liability for Cyberbullying

Ronen Perry*

---

* Professor of Law and Director, Aptowitzer Center for the Study of Risk, Liability, and Insurance, University of Haifa. I am grateful to the editors of the *UC Irvine Law Review* for their meticulous editorial work.

INTRODUCTION

In 2006, the world was shocked when thirteen-year-old Megan Meier committed suicide after being told that the world would be better off without her by a fake user on the social networking platform Myspace.[1] This was neither the first nor the last suicide attributed to cyberbullying,[2] and although suicide remains an infrequent outcome, its salience has called attention to the pervasiveness and gravity of technology-facilitated bullying among adolescents. Unfortunately, the law has failed to provide a satisfactory response. This Article aims to fill the gap, providing a law and economics analysis of the different models of civil liability for cyberbullying. It acknowledges three categories of potential defendants (see *Figure 1*): (1) the juvenile wrongdoers, (2) real-life supervisors (parents, school personnel), and (3) virtual supervisors (such as social networking platforms). It systematically analyzes the legal rules delineating each party's liability and evaluates the alternatives from an economic perspective. The Article demonstrates that technological innovation not only generates new risks or exacerbates old ones, but also simplifies the construction of efficient liability models to control them. In the context of juvenile bullying, imposing liability on real-life supervisors may be an inevitable solution to the fundamental inefficiencies of primary wrongdoers' liability.[3] Alas, supervisors' liability in the digital age entails considerable information costs. Technology, which has transformed an old schoolyard problem into a cyberspace pandemic, now provides the tools to substantially reduce these costs. It facilitates the collection, analysis, and flow of information, thereby reducing the cost of preventive action. Liability rules can and should endorse these developments in an effort to secure efficient conduct of all parties involved.

---

1. Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES (Nov. 28, 2007), https://www.nytimes.com/2007/11/28/us/28hoax.html [https://perma.cc/P7TL-BSAK].

2. *See, e.g.*, Lizette Alvarez, *Felony Counts for 2 in Suicide of Bullied 12-Year-Old*, N.Y. TIMES (Oct. 15, 2013), https://www.nytimes.com/2013/10/16/us/felony-charges-for-2-girls-in-suicide-of-bullied-12-year-old-rebecca-sedwick.html [https://perma.cc/G9LU-L8P6] (discussing Rebecca Sedwick's suicide); *see also* Nicole P. Grant, *Mean Girls and Boys: The Intersection of Cyberbullying and Privacy Law and Its Social-Political Implications*, 56 HOW. L.J. 169, 185–88 (2012) (discussing suicide cases); Shira Auerbach, Note, *Screening Out Cyberbullies: Remedies for Victims on the Internet Playground*, 30 CARDOZO L. REV. 1641, 1641–42 (2009) (same); Emily Poole, Note, *Hey Girls, Did You Know? Slut-Shaming on the Internet Needs to Stop*, 48 U.S.F. L. REV. 221, 236–39 (2013) (same); Tiffany Sumrall, Comment, *Lethal Words: Harmful Impact of Cyberbullying and the Need for Federal Criminalization*, 53 HOUS. L. REV. 1475, 1480–81 (2016) (same).

3. *E.g.*, Benjamin Walther, Comment, *Cyberbullying: Holding Grownups Liable for Negligent Entrustment*, 49 HOUS. L. REV. 531, 534 (2012) (presenting the negligent-entrustment theory of liability for cyberbullying cases).

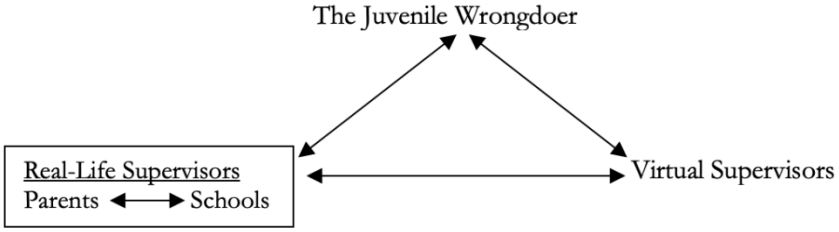

Figure 1. Interaction and Information Flow

Almost all adolescents in the United States currently have Internet access,[4] most have smartphones,[5] and a majority of teenagers with web-access also have personal profiles on social networking platforms, such as Facebook, Instagram, Tumblr, Twitter, WhatsApp, and YouTube.[6] Regrettably, electronic devices and applications are increasingly used to transmit and disseminate harmful content, especially among teens. This harmful conduct can take various forms, from sending personal insults and threats, through the publication or sharing of embarrassing or humiliating texts, photographs, and videos, to organizing social boycotts and inciting real-life harassment.[7] It may be carried out through text messaging, instant messaging, electronic mail, social networks, blog and forum posts, online comments and reviews, and the like.[8] When such conduct is intentional, repeated, and involves a real or perceived power imbalance, it is generally referred to as "cyberbullying,"[9] although the term is rarely used in the context of adult cyber-harassment or cyber-stalking.[10] Studies on both sides of the Atlantic show that one-third to fifty

4. *See* Grant, *supra* note 2, at 178 (reporting 87% access rate in 2010); Mary-Rose Papandrea, *Student Speech Rights in the Digital Age*, 60 FLA. L. REV. 1027, 1032 (2008) (reporting 87% internet access rate in 2004); Poole, *supra* note 2, at 226 (reporting 95% general access rate and 75% mobile access rate in 2013).

5. *See* Poole, *supra* note 2, at 226.

6. Grant, *supra* note 2, at 178–79.

7. *Cf.* U.S. Dep't of Health & Human Servs., *What Is Cyberbullying*, STOPBULLYING.GOV, http://www.stopbullying.gov/cyberbullying/what-is-it/index.html [https://perma.cc/5YG3-HDW5] (last visited Feb. 15, 2020) ("Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.").

8. *Id.*

9. *Id.* (defining "cyberbullying" as "bullying that takes place over digital devices"); U.S. Dep't of Health & Human Servs., *What Is Bullying*, STOPBULLYING.GOV, https://www.stopbullying.gov/what-is-bullying/index.html [https://perma.cc/T84D-7UDD] (last visited Feb. 15, 2020) (defining "bullying" as "unwanted, aggressive behavior among school aged children that involves a real or perceived power imbalance" and is "repeated, or has the potential to be repeated, over time"); *see also* Clay Calvert, *Fighting Words in the Era of Texts, IMS and E-Mails: Can a Disparaged Doctrine Be Resuscitated to Punish Cyber-Bullies?*, 21 DEPAUL J. ART TECH. & INTELL. PROP. L. 1, 16–19 (2010) (defining cyberbullying); Kathleen Conn, *Best Practices in Bullying Prevention: One Size Does Not Fit All*, 22 TEMP. POL. & C.R.L. REV. 393, 393, 402 (2013) (same); Grant, *supra* note 2, at 183 (same); Peter K. Smith et al., *Cyberbullying: Its Nature and Impact in Secondary School Pupils*, 49 J. CHILD PSYCHOL. & PSYCHIATRY 376, 376 (2008) (same); Auerbach, *supra* note 2, at 1643 (same).

10. Calvert, *supra* note 9, at 18–19.

percent of teens suffer from cyberbullying, many of them regularly.[11] Not only are these practices more common among minors, but they are also more harmful to minors who are in greater need of social acceptance.[12]

Cyberbullying may cause annoyance, anxiety, fright, embarrassment, humiliation, lowered self-esteem, and distress, and may even lead to social disorders, psychological disorders, and occasionally suicide attempts.[13] A recent medical review article concluded that juvenile victims of cyberbullying are twice as likely as non-victims to cause self-harm and exhibit suicidal ideation and behavior.[14] Cyberbullying may be more severe than traditional bullying, because (1) it can be carried out effortlessly and instantly;[15] (2) it has a much wider potential reach, increasing expected impact;[16] (3) it can transcend the temporal and spatial boundaries of school activity;[17] (4) the harmful speech may be harsher, because perpetrators behind a screen are not restrained by victims' facial and bodily expressions of harm and bystanders' expressions of indignation;[18] (5) technology facilitates anonymity, which encourages unconstrained speech by shielding perpetrators from embarrassment, reprimand, and retaliation;[19] (6) offensive speech cannot be easily removed, particularly when disseminated through various media;[20] and (7) juvenile online speech cannot be easily overseen by adults.[21] Apart from its effects on victims, juvenile cyberbullying has negative effects on perpetrators, who

---

11. *E.g.*, A THIN LINE, 2009 AP-MTV DIGITAL ABUSE STUDY 1–2 (n.d.), http://www.athinline.org/MTV-AP_Digital_Abuse_Study_Executive_Summary.pdf [https://perma.cc/7SFN-V7ZU] (last visited Feb. 15, 2020) (reporting 50% victimization rate in the US); DITCH THE LABEL, THE ANNUAL BULLYING SURVEY 2017, at 15 (5th ed. 2017), https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf [https://perma.cc/7Q9S-WVM3] (last visited Feb. 15, 2019) (reporting that 33% of UK teens experience cyberbullying often to constantly); Grant, *supra* note 2, at 178, 184 (reporting near 42%); Auerbach, *supra* note 2, at 1643 (reporting 75%); Amanda Lenhart, *Cyberbullying*, PEW RES. CTR. (June 27, 2007), http://www.pewinternet.org/2007/06/27/cyberbullying [https://perma.cc/5DCA-YTSD] (reporting 32%).

12. Alison Virginia King, Note, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 851–52 (2010).

13. *See* Conn, *supra* note 9, at 396–97; Duffy B. Trager, *New Tricks for Old Dogs: The Tinker Standard Applied to Cyber-Bullying*, 38 J.L. & EDUC. 553, 556 (2009); King, *supra* note 12, at 850–51.

14. Ann John et al., *Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review*, 20 J. MED. INTERNET RES. 129 *passim* (2018); *see also* Sameer Hinduja & Justin W. Patchin, *Bullying, Cyberbullying, and Suicide*, 14 ARCHIVES SUICIDE RES. 206, 206 (2010) (finding a link between suicidal ideation and cyberbullying).

15. Auerbach, *supra* note 2, at 1643; Poole, *supra* note 2, at 243–44.

16. Auerbach, *supra* note 2, at 1643; Poole, *supra* note 2, at 243–44.

17. Calvert, *supra* note 9, at 14–16, 20; Poole, *supra* note 2, at 244–45; Sumrall, *supra* note 2, at 1479; Walther, *supra* note 3, at 534.

18. Calvert, *supra* note 9, at 20; Auerbach, *supra* note 2, at 1644; Sumrall, *supra* note 2, at 1479.

19. Calvert, *supra* note 9, at 20; Grant, *supra* note 2, at 173–74, 198–99; Auerbach, *supra* note 2, at 1643–45; King, *supra* note 12, at 852; Poole, *supra* note 2, at 243, 259; Sumrall, *supra* note 2, at 1479–80.

20. Poole, *supra* note 2, at 244.

21. *Id.*

are more prone to criminal activity and antisocial behavior,[22] and on bystanders, who are exposed to greater mental risks.[23]

The most common legal response to cyberbullying is delegating the responsibility to school boards.[24] All state legislatures in the United States require school districts to prescribe and enforce anti-bullying policies,[25] and many explicitly apply these rules to cyberbullying.[26] While similar in principle, state statutes differ in various respects, including the definition of bullying and the degree of

---

22. Conn, *supra* note 9, at 397–99; Susan M. Swearer & Shelley Hymel, *Understanding the Psychology of Bullying: Moving Toward a Social-Ecological Diathesis–Stress Model*, 70 AM. PSYCHOLOGIST 344, 347 (2015) (presenting impact on perpetrators).

23. Conn, *supra* note 9, at 399–402.

24. Naomi Harlin Goodno, *How Public Schools Can Constitutionally Halt Cyberbullying: A Model Cyberbullying Policy That Considers First Amendment, Due Process, and Fourth Amendment Challenges*, 46 WAKE FOREST L. REV. 641 (2011); Walther, *supra* note 3, at 539.

25. *See* ALA. CODE §§ 16-28B-1 to 16-28B-9 (2018); ALASKA STAT. § 14.33.200 (2006); ARIZ. REV. STAT. ANN. § 15-341(36) (2019); ARK. CODE ANN. § 6-18-514(d)–(f) (2019); CAL. EDUC. CODE § 48900.4 (2003); COLO. REV. STAT. § 22-32-109.1 (2019); CONN. GEN. STAT. § 10-222d(b)–(c) (2018); DEL. CODE ANN. tit. 14, § 4164(a)–(b) (2017); FLA. STAT. § 1006.147(2), (4) (2019); GA. CODE. ANN. § 20-2-751.4(b) (2016); HAW. CODE R. § 8-19-6 (LexisNexis 2009); IDAHO CODE § 33-1631 (2019); 105 ILL. COMP. STAT. 5 / 27-23.7 (2017); IND. CODE § 20-33-8-13.5(a) (2018); IOWA CODE § 280.28(3) (2007); KAN. STAT. ANN. § 72-6147(b)–(c) (2013); KY. REV. STAT. ANN. § 158.148(5) (West 2016); LA. STAT. ANN. § 17:416.13(A)–(B) (2017); ME. REV. STAT. ANN. tit. 20-A, § 1001(15) (2019); MD. CODE ANN., EDUC. § 7-424.1(b)(1)–(2) (West 2018); MASS. GEN. LAWS ch. 71, § 37O(b), (d)(1)–(2) (2014); MICH. COMP. LAWS § 380.1310b(1) (2017); MINN. STAT. § 121A.031 (2015); MISS. CODE ANN. § 37-11-67(2) (2017); MO. REV. STAT. § 160.775(1) (2016); MONT. CODE ANN. § 20-5-209 (2015); NEB. REV. STAT. § 79-2,137(3) (2008); NEV. REV. STAT. § 388.133 (2019); N.H. REV. STAT. ANN. § 193-F:4(II) (2010); N.J. STAT. ANN. § 18A:37-15(a), (b) (West 2012); N.M. CODE R. § 6.12.7.6 (2019); N.Y. EDUC. LAW § 13 (McKinney 2013); N.C. GEN. STAT. § 115C-407.15(b), (d) (2009); N.D. CENT. CODE § 15.1-19-18 (2019); OHIO REV. CODE ANN. § 3313.666(B) (West 2012); OKLA. STAT. tit. 70, § 24-100.4(A) (2016); OR. REV. STAT. § 339.356(1) (2012); 24 PA. CONS. STAT. § 13-1303.1-A(a) (2008); 16 R.I. GEN. LAWS § 16-21-34 (2011) (imposing the duty on the state department of education); S.C. CODE ANN. § 59-63-140(A), (B) (2006); S.D. CODIFIED LAWS § 13-32-14 (2012); TENN. CODE ANN. § 49-6-4503(a) (2019); TEX. EDUC. CODE ANN. § 37.001(a)(7) (West 2019); UTAH CODE ANN. § 53G-9-605(1)–(3) (LexisNexis 2019); VT. STAT. ANN. tit. 16, § 165(a)(8) (2019); VA. CODE ANN. §§ 22.1-279.6(D), 22.1-291.4(A) (2019); WASH. REV. CODE § 28A.600.477(1)(a) (2018); W. VA. CODE § 18-2C-3(a)–(b) (2011); WIS. STAT. § 118.46 (2019); WYO. STAT. ANN. § 21-4-314(a) (2009).

26. *See* ARK. CODE ANN. § 6-18-514(b)(2) (2019); CONN. GEN. STAT. § 10-222d(a)(2) (2018); FLA. STAT. § 1006.147(3)(a) (2019); GA. CODE. ANN. § 20-2-751.4(a) (2016); 105 ILL. COMP. STAT. 5 / 27-23.7(b) (2017); IOWA CODE § 280.28(2)(b) (2007); KAN. STAT. ANN. § 72-6147(a)(2) (2013); LA. STAT. ANN. § 17:416.13(C)(1)(b) (2017); MASS. GEN. LAWS ch. 71, § 37O(a) (2014); MICH. COMP. LAWS § 380.1310b(10)(b)–(c) (2017); MINN. STAT. § 121A.031(a)(2)–(3) (2015); MISS. CODE ANN. § 37-11-67(1) (2017); MO. REV. STAT. § 160.775(2) (2016); MONT. CODE ANN. § 20-5-208(1) (2015); NEB. REV. STAT. § 79-2,137(2) (2008); NEV. REV. STAT. § 388.133(1) (2019); N.H. REV. STAT. ANN.§ 193-F:4(II) (2010); N.J. STAT. ANN. § 18A:37-15.1(b) (West 2012); N.M. CODE R. § 6.12.7.7(a)–(b) (2019); N.Y. EDUC. LAW § 11(7)–(8) (McKinney 2013); N.C. GEN. STAT. § 115C-407.15(a) (2009); OHIO REV. CODE ANN. § 3313.666(A)(2)(a) (West 2012); OKLA. STAT. tit. 70, § 24-100.4(A)(1) (2016); OR. REV. STAT. § 339.356(2)(a) (2012); 24 PA. CONS. STAT. § 13-1303.1-A(e) (2008); 16 R.I. GEN. LAWS § 16-21-33(a)(1) (2011); TENN. CODE ANN. § 49-6-4503(a) (2019); UTAH CODE ANN.§ 53G-9-605(3)(a)–(b) (LexisNexis 2019); VT. STAT. ANN. tit. 16, § 11(a)(32) (2019); VA. CODE ANN. § 22.1-279.6(A) (2019); WASH. REV. CODE § 28A.600.477(5)(b)(ii) (2018).

particularity.[27] A less frequent legal response, which raises serious freedom of speech concerns,[28] is criminalization of the harmful conduct. Legislators and scholars advocated federal criminalization of cyberbullying following Megan Meier's suicide, but these attempts ultimately failed.[29] A few state legislatures have already criminalized cyberbullying,[30] but these criminal statutes typically apply to extreme subsets of this phenomenon, such as cyberstalking.[31] Cases involving threats of violence may also be covered by specific federal legislation.[32] In theory, cyberbullying resulting in suicide may be considered homicide,[33] although causation may be difficult to establish.[34]

A third possible response—namely civil liability—is rarely considered, hence undertheorized. There have been few civil lawsuits for real-life bullying,[35] and even less reported attempts to sue for cyberbullying.[36] In *Finkel v. Dauber*,[37] members of

27. Conn, *supra* note 9, at 419–24 (discussing state anti-bullying legislation); Mathew Fenn, Note, *A Web of Liability: Does New Cyberbullying Legislation Put Public Schools in Sticky Situation?*, 81 FORDHAM L. REV. 2729, 2754–55 (2013) (same).

28. *See, e.g.*, State v. Bishop, 787 S.E.2d 814, 822 (N.C. 2016) (finding the criminalization of online publication of "private, personal, or sexual information pertaining to a minor" unconstitutional); People v. Dietze, 549 N.E.2d 1166, 1168 (N.Y. 1989) (holding a criminal proscription of abusive speech with intent to harass unconstitutional hence invalid).

29. Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. § 3 (2009), https://www.gpo.gov/fdsys/pkg/BILLS-111hr1966ih/pdf/BILLS-111hr1966ih.pdf [https://perma.cc/K85N-QWLH] (imposing criminal penalties on "whoever transmits in interstate or foreign commerce any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior"). For more information about this bill, see Grant, *supra* note 2, at 201; Sumrall, *supra* note 2, at 1477, 1499–1500; and Walther, *supra* note 3, at 534, 536–37.

30. *See, e.g.*, ALA. CODE § 13A-11-8(b) (2019); FLA. STAT. § 1006.147(4)(h)(i) (2019); IDAHO CODE § 18-917A(2) (2015); LA. STAT. ANN. § 14:40.7 (2019); N.Y. PENAL LAW § 240.30 (McKinney 2019); N.C. GEN. STAT. § 14-458.1 (2012), *invalidated in part by* State v. Bishop, 787 S.E.2d 814, 822 (N.C. 2016).

31. Walther, *supra* note 3, at 537.

32. Federal law penalizes threats to injure transmitted over interstate lines, 18 U.S.C. § 875(c) (2018), and electronic stalking which places the victim in a fear of serious injury or death or causes substantial emotional distress, 18 U.S.C. § 2261A(2) (2018).

33. *See* Commonwealth v. Carter, 115 N.E.3d 559, 570 (Mass. 2019) ("[A] person might be charged with involuntary manslaughter for reckless or wanton conduct, including verbal conduct, causing a victim to commit suicide."); Audrey Rogers, *Death by Bullying: A Comparative Culpability Proposal*, 35 PACE L. REV. 343, 365 (2014) ("For egregious bullying cases, prosecutors can and should consider possible homicide charges.").

34. *See* Nicholas LaPalme, Note, *Michelle Carter and the Curious Case of Causation: How to Respond to a Newly Emerging Class of Suicide-Related Proceedings*, 98 B.U. L. REV. 1443, 1446–53 (2018) (discussing the causation hurdle in prosecuting encouragement of suicide).

35. Tracy Tefertiller, *Out of the Principal's Office and Into the Courtroom: How Should California Approach Criminal Remedies for School Bullying?*, 16 BERKELEY J. CRIM. L. 168, 189 (2011); *see, e.g.*, Doe v. Bristol Bd. of Educ., No. CV065002257, 2007 Conn. Super. LEXIS 3508 (Mar. 23, 2007); Jasperson v. Anoka-Hennepin Indep. Sch. Dist. No. 11, No. A06-1904, 2007 Minn. App. Unpub. LEXIS 1071 (Oct. 30, 2007).

36. *See* D.C. v. R.R., 106 Cal. Rptr. 3d 399, *rev. denied*, No. S181558, 2010 Cal. LEXIS 6052 (June 17, 2010); Finkel v. Dauber, 906 N.Y.S.2d 697 (Sup. Ct. 2010); Draker v. Schreiber, 271 S.W.3d 318 (Tex. App. 2008).

37. *Finkel*, 906 N.Y.S.2d. 697.

a Facebook group run by New York adolescents posted defamatory statements about their school peer, claiming that she contracted HIV by having sex with an animal or a male prostitute, or by sharing a needle with a heroin addict, and consequently "morfed [sic] into the devil."[38] The claim was dismissed.[39] In *D.C. v. R.R.*,[40] a Los Angeles high school student was the subject of posts by fellow students on his own website "making derogatory comments about his perceived sexual orientation and threatening him with bodily harm."[41] The student sued, but the only legal issue decided by the court was whether the California anti-SLAPP statute applied (a question answered in the negative).[42] The scarcity of case law may explain why no serious attempt has been made to analyze and evaluate competing liability theories in the legal literature.[43] This reality is perplexing in light of the general jurisprudential assumption that criminal liability, which is frequently considered as a response to juvenile cyber-wrongdoing, is a residual system, reserved for cases in which less stringent legal and extra-legal systems fail.[44]

Part I systematically discusses the law pertaining to civil liability of the three categories of potential defendants. Section A begins with an overview of the various causes of action that can be employed in lawsuits against cyberbullies. It identifies the possible obstacles to primary wrongdoers' liability on the legal, technological, and financial levels. Section B focuses on real-life supervisors. It first examines relevant theories of parental liability and their limits. Next, it analyzes common law and statutory bases of school district and school personnel liability and explains the constitutional constraints on school regulation of student conduct. Section C discusses virtual supervisors' liability. It shows that bringing lawsuits against virtual supervisors for wrongful user-contributions is almost impossible under American law and presents alternative models.

Part II evaluates the different liability regimes from an economic perspective and constructs an efficient technologically-assisted model. Section A explains that primary wrongdoers' liability cannot achieve efficient deterrence because of minors' (1) inability to compensate their victims, (2) limited cognitive, emotional, and social capacity, and (3) frequent use of anonymity. Section B evaluates real-life supervisors' liability, focusing on the gap between the ability to affect juvenile conduct and the high cost of information about misconduct. Section C shows that virtual

38. *Id.* at 700.

39. *Id.* at 702. In *Draker*, 271 S.W.3d at 318, a claim for cyberbullying was similarly denied, but the victim was not a minor, so the case does not squarely fall within the ambit of this article.

40. *D.C.*, 106 Cal. Rptr. 3d at 404–05.

41. *Id.* at 1199.

42. *Id.* The acronym SLAPP stands for strategic lawsuit against public participation.

43. Noteworthy exceptions are Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41 (2007), and Walther, *supra* note 3, but each focuses on a different defendant and neither provides comprehensive legal and economic analyses.

44. *See, e.g.*, Douglas Husak, *The Criminal Law as Last Resort*, 24 OXFORD J. LEGAL STUD. 207 *passim* (2004) (discussing the principle of criminalization as a last resort); Nils Jareborg, *Criminalization as Last Resort*, 2 OHIO ST. J. CRIM. L. 521, 525 (2005) (same).

supervisors' liability may be inefficient due to the high cost of monitoring, non-internalization of the vast economic benefits of Web 2.0 services by service providers, and an asymmetry between false negative and false positive determinations of wrongfulness. More importantly, it argues that virtual supervisors may have some access to relevant information but lack the power to affect juvenile conduct. Finally, Section D constructs an efficient liability model based on parental supervision and technologically-facilitated reduction in information costs.

I. LEGAL FOUNDATIONS

A. The Wrongdoer

1. Causes of Action

The obvious candidate for liability in a case of cyber-wrongdoing is the primary wrongdoer. The first analytical step, therefore, is to identify possible causes of action for such wrongdoing. When cyber-wrongdoing leads to actual violence, or consists of threats thereof, an action for battery or assault may ensue.[45] This, however, is uncommon; cyberbullying is mostly a speech-based phenomenon and should be addressed accordingly.[46] No jurisdiction in the United States has hitherto recognized a specific cause of action for cyberbullying.[47] In *Finkel v. Dauber*, for example, the court made clear that New York law does not "recognize cyberbullying or Internet bullying as a cognizable tort action."[48] Of course, this does not preclude future development of such a tort. Indeed, the legislature of the Canadian province of Nova Scotia explicitly recognized a specific tort of cyberbullying,[49] and some scholars advocated a similar development in the United States.[50] However, until this happens, victims must rely on other causes of action.[51]

---

45. If a person "acts intending to cause a harmful or offensive contact with the person of the other or a third person, or an imminent apprehension of such a contact" then he is liable for battery if a harmful contact results, RESTATEMENT (SECOND) OF TORTS § 13 (AM. LAW INST. 1965), and for assault if the other is only "put in such imminent apprehension." *Id.* § 21.

46. *See* Walther, *supra* note 3, at 542 ("Unlike the traditional bully who could be sued for assault and battery, the cyberbully only engages in hurtful speech over the Internet.").

47. Finkel v. Dauber, 906 N.Y.S.2d 697, 703 (Sup. Ct. 2010); Walther, *supra* note 3, at 542.

48. *Finkel*, 906 N.Y.S.2d at 703.

49. The first legislative recognition of a specific tort was in the Cyber-Safety Act, S.N.S. 2013, c 2, § 21 (Can.). This Act was struck down for infringing the constitutional freedom of expression and right to liberty. Crouch v. Snell, 2015 NSSC 340, paras. 106, 116, 137, 158, 166, 175, 184, 187, 191, 203, 207, 221 (Can. N.S.). In 2017, the Nova Scotia legislature enacted a more limited liability rule. Intimate Images and Cyber-Protection Act, S.N.S. 2017, c 7, § 6(3) (Can.).

50. *See, e.g.*, Jonathan Heller, Note, *The Chat Room Moderator: Creating a Duty for Parents to Control Their Cyberbully*, 53 FAM. CT. REV. 165, 172 (2015) (addressing criticism of the Nova Scotia statute).

51. This Section discusses common law causes of action. There may be state-specific statutory causes of action. For example, in California, any person has the right to be free from "intimidation by threat of violence" motivated by the victim's actual or perceived disability, gender, race, religion or sexual orientation. CAL. CIV. CODE § 51.7(a) (West 2019).

If a child or an adolescent publishes disparaging statements about another through electronic devices and applications, an action for defamation may be appropriate. Defamation is defined as a communication that tends to "harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[52] To successfully bring a defamation claim, the plaintiff must prove that (1) the defendant's statement about the plaintiff was both false and defamatory, (2) the statement was published without privilege to a third party, (3) the defendant's conduct involved fault (at least negligence), and (4) the statement is actionable per se or its publication caused special harm.[53]

The main obstacle here is that an action for defamation is based on a statement of fact, not an opinion.[54] Generally, opinions enjoy First Amendment protection.[55] The Supreme Court highlighted this distinction in *Milkovich v. Lorain Journal Co.*,[56] holding that a statement is one of fact, rather than mere opinion, if it is "provable as false" and can be "reasonably interpreted as stating actual facts."[57] Thus, imaginative expressions, rhetorical hyperboles, and conjectures, which a reasonable audience cannot perceive as statements of fact, are not actionable.[58] In *Finkel v. Dauber*,[59] mentioned in the Introduction, members of a teenage Facebook group posted defamatory statements about their peer, claiming that she contracted HIV through contemptible conduct and "morfed [sic] into the devil."[60] The court held that group members could not be liable for defamation, because the posts could only be read as puerile attempts by adolescents to outdo each other, not as statements of fact.[61] Similarly, in *Draker v. Schreiber*,[62] teenage students created a Myspace profile under their vice-principal's name, which contained her personal information and explicit and graphic sexual references. The vice-principal sued, and the trial court granted the students' motion for summary judgment dismissing the cause of action for defamation.[63] It agreed that the "exaggerated and derogatory statements" included in the fake profile were not assertions of fact that could be objectively verified and therefore could not be defamatory.[64]

---

52. RESTATEMENT (SECOND) OF TORTS § 559 (AM. LAW INST. 1977).
53. *Id.* § 558.
54. Sumrall, *supra* note 2, at 1496; Walther, *supra* note 3, at 544.
55. Auerbach, *supra* note 2, at 1667.
56. Milkovich v. Lorain Journal Co., 497 U.S. 1 (1990).
57. *Id.* at 19–20.
58. *Id.*; *see also* Hustler Magazine v. Falwell, 485 U.S. 46, 50 (1988); Greenbelt Coop. Publ'g Ass'n v. Bresler, 398 U.S. 6, 13–14 (1970); Catherine J. Ross, *Incredible Lies*, 89 U. COLO. L. REV. 377, 400–17 (2018) (discussing incredible lies in defamation law).
59. Finkel v. Dauber, 906 N.Y.S.2d 697 (Sup. Ct. 2010).
60. *Id.* at 700.
61. *Id.* at 702.
62. Draker v. Schreiber, 271 S.W.3d 318 (Tex. App. 2008).
63. *Id.* at 321.
64. *Id.*

Another obstacle is that even defamatory statements of fact cannot be actionable unless they are false. Truth has always been an absolute defense against a lawsuit for defamation.[65] Statements made by adolescents to harass their peers are sometimes true, as in the unfortunate yet common event of bullying based on sexual orientation.[66] Additionally, when the harassment takes the form of private communication between the wrongdoer and the victim, such as a personal text message or an e-mail, the requirement of publication is not satisfied.[67] Finally, teenage victims may be unable to establish special harm.[68]

In many cases, cyberbullying involves public disclosure of private matters, which is one of the recognized categories of the tort of invasion of privacy. Liability can arise if the defendant (1) gave publicity to a matter concerning the private life of the plaintiff, (2) the matter publicized would be highly offensive to a reasonable person, and (3) the matter is not of legitimate concern to the public.[69] This tort encompasses true factual statements, which the tort of defamation does not cover. A notable example is the Tyler Clementi incident, in which a student committed suicide after his roommate secretly streamed his sexual encounter with another man.[70] Liability can arise only if the publication would be highly offensive to a reasonable person, and this requirement precludes recovery in many instances of cyber-invasion of privacy.[71] Another recognized category of invasion of privacy, which may apply to some cases of cyber-harassment, is intrusion "upon the solitude or seclusion of another or his private affairs or concerns."[72] It may occur in the digital rather than the physical world,[73] and does not require publication of any sort. Intrusion upon seclusion gives rise to liability if it is intentional and "highly offensive to a reasonable person."[74]

A third possible cause of action is intentional infliction of emotional distress (hereinafter IIED). The tort requires proof of four elements: (1) extreme or outrageous conduct, (2) intention or recklessness, (3) severe emotional harm, and (4) a causal link between the conduct and the harm.[75] As per the first requirement,

---

65. RESTATEMENT (SECOND) OF TORTS § 581A (AM. LAW INST. 1977).

66. Sumrall, *supra* note 2, at 1496.

67. Auerbach, *supra* note 2, at 1650, 1667.

68. Walther, *supra* note 3, at 545–46.

69. RESTATEMENT (SECOND) OF TORTS § 652D.

70. Lisa W. Foderaro, *Private Moment Made Public, Then a Fatal Jump*, N.Y. TIMES (Sept. 29, 2010), https://www.nytimes.com/2010/09/30/nyregion/30suicide.html [https://perma.cc/M5GL-6LW8].

71. Walther, *supra* note 3, at 545 n.90.

72. RESTATEMENT (SECOND) OF TORTS § 652B.

73. *See, e.g.*, Roberts v. CareFlite, No. 02-12-00105-CV, 2012 Tex. App. LEXIS 8371 (Oct. 4, 2012) (suing her employer for an invasion of privacy by intrusion upon seclusion after she was terminated for "unprofessional and insubordinate" Facebook activity—a comment on a friend's post).

74. RESTATEMENT (SECOND) OF TORTS § 652B; *see also* Valenzuela v. Aquino, 853 S.W.2d 512, 513 (Tex. 1993) (endorsing § 652B).

75. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 46 (AM. LAW INST. 2012); RESTATEMENT (SECOND) OF TORTS § 46 (AM. LAW INST. 1965); *see also*

liability can be imposed only if the conduct was "so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community."[76] While cyberbullying may be harmful, it does not ordinarily reach this bar. The severity-of-harm requirement may also be an insurmountable obstacle,[77] especially in the few jurisdictions that require physical harm.[78] Furthermore, in some jurisdictions, IIED is considered a "gap-filler" tort, created to permit recovery in "those rare instances in which a defendant intentionally inflicts severe emotional distress in a manner so unusual that the victim has no other recognized theory of redress."[79] If the gravamen of the claim is a wrong that another cause of action was meant to cover, IIED cannot be employed, whether or not the plaintiff succeeds on or even relies on the other cause of action.[80] Thus, in *Draker v. Schreiber*,[81] the court held that since the gravamen of the complaint was defamation, IIED was inapplicable, even though the defamation action failed.[82] To maintain a claim for IIED, the plaintiff had to allege facts independent of her defamation claim.[83]

A related cause of action is negligent infliction of emotional distress (hereinafter NIED). In most jurisdictions, a plaintiff relying on this theory must establish serious emotional harm, and prove that the defendant placed him or her in danger of immediate bodily harm and that the emotional harm resulted from the physical danger.[84] The severity-of-harm threshold may hinder liability for NIED in many cases of cyber-harassment, as it does with respect to IIED.[85] Additionally, the requirement of immediate physical danger, known as the "zone of danger" test, will preclude liability for NIED in most instances of cyberbullying, because potentially harmful speech in cyberspace does not typically involve physical danger. The zone-of-danger requirement may be satisfied in cases of cyber-incitement to violence which generates physical risk in the real world and in the relatively rare cases of pushing victims to commit suicide or self-harm.

Wal-Mart Stores, Inc. v. Canchola, 121 S.W.3d 735, 740–41 (Tex. 2003); Morgan v. Anthony, 27 S.W.3d 928, 929 (Tex. 2000).

76. RESTATEMENT (SECOND) OF TORTS § 46 cmt. d; *see also* Howell v. N.Y. Post Co., 612 N.E.2d 699, 702 (N.Y. 1993) ("[O]f the intentional infliction of emotional distress claims considered by this Court, every one has failed because the alleged conduct was not sufficiently outrageous.").

77. Auerbach, *supra* note 2, at 1670–71.

78. *See, e.g.*, Engel v. Buchan, 791 F. Supp. 2d 604, 609 (N.D. Ill. 2011) (noting that Missouri law requires a plaintiff to prove bodily harm to recover for IIED).

79. Hoffmann-La Roche, Inc. v. Zeltwanger, 144 S.W.3d 438, 447 (Tex. 2004).

80. *Id.* at 448.

81. Draker v. Schreiber, 271 S.W.3d 318 (Tex. App. 2008).

82. *Id.* at 323.

83. *Id.* at 323–24.

84. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 47 & cmt. b (AM. LAW INST. 2012).

85. Auerbach, *supra* note 2, at 1670–71.

Lastly, the prima facie tort, which the Supreme Court first recognized in *Aikens v. Wisconsin*,[86] is defined as infliction of intentional harm, resulting in damages, without excuse or justification.[87] Under the New York version, also endorsed in other jurisdictions,[88] the tort applies only if the defendant's conduct "would otherwise be lawful."[89] Thus, this cause of action is not available if the defendant's acts fall within one of the traditional tort categories.[90] Under section 870 of the Restatement (Second) of Torts, "liability may be imposed although the actor's conduct does not come within a traditional category of tort liability."[91] In other words, the tort may apply even if the conduct falls within an existing category of tort.[92] Either way, the prima facie tort is in effect a residual principle of intention-based liability, because the defendant's conduct should or may be "otherwise lawful."[93] The defendant's intent to cause harm makes the otherwise lawful act actionable; so the doctrine seems to punish bad motives, not wrongful conduct.[94] This feature has spawned criticism[95] and led to the rejection of the doctrine in many jurisdictions.[96]

According to a narrow but common interpretation of the intent element, there can be no recovery in prima facie tort, unless malevolence is the sole motive for defendant's otherwise lawful act or, in Justice Holmes's words, unless the defendant acts from "disinterested malevolence."[97] Put differently, the defendant does not aim

---

86. Aikens v. Wisconsin, 195 U.S. 194, 204 (1904) ("*[P]rima facie*, the intentional infliction of temporal damages is a cause of action, which, as a matter of substantive law, whatever may be the form of pleading, requires a justification if the defendant is to escape.") (italics added).

87. ATI, Inc. v. Ruder & Finn, Inc., 368 N.E.2d 1230, 1232 (N.Y. 1977); *see also* RESTATEMENT (SECOND) OF TORTS § 870 (AM. LAW INST. 1979) ("One who intentionally causes injury to another is subject to liability . . . if his conduct is generally culpable and not justifiable under the circumstances.").

88. Kenneth J. Vandevelde, *A History of Prima Facie Tort: The Origins of a General Theory of Intentional Tort*, 19 HOFSTRA L. REV. 447, 450, 494–95 (1990).

89. *ATI*, 368 N.E.2d at 1232; *see also* Burns Jackson Miller Summit & Spitzer v. Lindner, 451 N.E.2d 459, 467 (N.Y. 1983); Geri Shapiro, Note, *The Prima Facie Tort Doctrine: Acknowledging the Need for Judicial Scrutiny of Malice*, 63 B.U. L. REV. 1101, 1101 (1983) (discussing *ATI* and other cases).

90. Shapiro, *supra* note 89, at 1104; Vandevelde, *supra* note 88, at 450, 491–92.

91. RESTATEMENT (SECOND) OF TORTS § 870.

92. Vandevelde, *supra* note 88, at 450, 494.

93. Shapiro, *supra* note 89, at 1104.

94. *Id.*

95. *Id.* at 1104, 1107 ("This implication has evoked much criticism from courts that believe the law should punish only wrongful acts, and not wrongful thoughts . . . . The most frequent criticism of the prima facie tort doctrine is that courts should not make bad motives actionable.").

96. *See, e.g.*, Krause v. Hartford Accident & Indem. Co., 49 N.W.2d 41, 44 (Mich. 1951) ("Bad motive, by itself . . . is no tort. Malicious motives make a bad act worse, but they cannot make that a wrong which in its own essence is lawful. An act which does not amount to a legal injury cannot be actionable because it is done with a bad intent."); Teas v. Republic Nat'l Bank of Dallas, 460 S.W.2d 233, 242 (Tex. App. 1970) ("If an act be lawful . . . an improper motive does not render it unlawful . . . . Malicious motives make a bad case worse, but it cannot make that wrong which, in its own essence, is lawful."); Shapiro, *supra* note 89, at 1107–08.

97. Burns Jackson Miller Summit & Spitzer v. Lindner, 451 N.E.2d 459, 468 (N.Y. 1983) (quoting Am. Bank & Tr. Co. v. Fed. Reserve Bank of Atlanta, 256 U.S. 350, 358 (1921)); *see also* Shapiro,

to promote any personal interests by his or her conduct, except venting his or her ill will.[98] The Second Restatement of Torts adopted a less rigid approach: "If the only motive of the actor is a desire to harm the plaintiff, this fact becomes a very important factor"[99]—very important rather than decisive. These interpretations are sometimes criticized as making the "lack of excuse or justification" element redundant. If a justification exists, malevolence cannot be the sole motivation; so if the defendant also intended to promote a certain interest, the analysis stops at the intent element, and the justification element will not be examined.[100] An alternative interpretation of the intent element requires that malevolence be the primary or dominant motivation.[101] Another possible interpretation requires malevolence but not as the sole or dominant motivation. According to this approach, after establishing malice, the court must determine whether the malicious conduct may be excused or justified.[102] Cyberbullying will often satisfy the malevolence requirement, even under the narrow interpretation, and definitely under the more flexible approaches.

2. Legal Barriers

In many civil law and mixed jurisdictions, children under a certain age are exempt from liability. For example, the minimum age of liability is seven in Germany[103] and Portugal,[104] twelve in Israel,[105] and fourteen in Austria,[106] the Netherlands,[107] and Russia.[108] Age-based immunity might thwart many lawsuits of juvenile cyberbullying victims. By contrast, and with very few exceptions,[109] Anglo-American law does not normally set a minimum age for liability.[110] Rather, it imposes more lenient constraints on juvenile liability.

---

supra note 89, at 1117–18 (discussing the "disinterested malevolence" requirement); Vandevelde, *supra* note 88, at 491 (same).

98. RESTATEMENT (SECOND) OF TORTS § 870 cmt. i (AM. LAW INST. 1979).

99. *Id.*

100. Shapiro, *supra* note 89, at 1118–19.

101. *Id.* at 1123–25.

102. *Id.* at 1120–22.

103. BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], § 828, para. 1 (Ger.). The minimum age for liability is ten years in cases of traffic accidents.

104. Código Civil [Civil Code] § 488(2) (Port.).

105. Civil Wrongs Ordinance (New Version), 5733-1972 § 9(a), 4, (Isr.).

106. ALLGEMEINES BÜRGERLICHES GESETZBUCH [ABGB] [CIVIL CODE] § 153 (Austria).

107. Art. 6:164 BW (Neth.).

108. GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII [GK RF] [Civil Code] art. 26(2) (Russ.).

109. Georgia seems to be the exception, recognizing immunity from liability to minors under the age of thirteen. GA. CODE ANN. § 51-11-6 (West 2018) ("Infancy is no defense to a tort action so long as the defendant has reached the age of discretion and accountability prescribed by Code Section 16-3-1 for criminal offenses.").

110. RESTATEMENT (SECOND) OF TORTS § 895I (AM. LAW INST. 1979) ("One who is an infant is not immune from tort liability solely for that reason."); Donald Paul Duffala, Annotation, *Modern Trends as to Tort Liability of Child of Tender Age*, 27 A.L.R.4th 15, §§ 2[a], 3[a] (2019).

First, in some common law jurisdictions, children under a certain age, usually seven or five, are conclusively presumed to be incapable of negligence because they cannot recognize and appreciate risks.[111] In some jurisdictions, children under the same age cannot be held liable for intentional torts as well because of their limited cognitive and moral capacity.[112] Arguably, intent with respect to outcomes, as opposed to intent with respect to the conduct, should be treated like foreseeability of harm in negligence.[113] Currently, children under the age of seven are unlikely to take part in cyberbullying, but if this occurs, they cannot be liable for intentional torts or negligence in these jurisdictions.

Second, some jurisdictions recognize a rebuttable presumption, whereby children within a specific age range cannot be negligent. For example, in Alabama, Illinois, Kentucky, North Carolina, Pennsylvania, and Tennessee, a child between the ages of seven and fourteen is rebuttably presumed to be incapable of negligence.[114] In New Jersey, a rebuttable presumption applies to children of less than seven years of age.[115] Although rebuttable presumptions are not as detrimental to a victim's case as conclusive presumptions, they surely generate an evidentiary impediment.

Third, age is relevant in determining whether a child could form the mental attitudes which underlie the tort. In an action for negligence, if the actor is a child, the standard of conduct to which he or she must conform to avoid being negligent is that of a reasonable person of like age, intelligence, and experience under like circumstances.[116] In an action for an intentional tort, the age of the child is relevant

---

111. *See, e.g.*, Willoughby v. Stilz, 387 S.W.2d 10, 11 (Ky. 1965) ("[A] child under seven years of age is considered incapable of negligence."); Faia v. Landry, 249 So. 2d 317, 319 (La. App. 1971) (same); Queen Ins. Co. v. Hammond, 132 N.W.2d 792, 793 (Mich. 1965) (same); Burns v. Eminger, 261 P. 613, 615 (Mont. 1927) (same); Walston v. Greene, 102 S.E.2d 124, 125 (N.C. 1958) (same); DeLuca v. Bowden, 329 N.E.2d 109, 111–12 (Ohio 1975) (same); Dodd v. Spartanburg Ry. Gas & Elec. Co., 78 S.E. 525, 528 (S.C. 1913) (same); Von Saxe v. Barnett, 217 P. 62, 63 (Wash. 1902) (same); *cf.* Nielsen v. Bell, 370 P.3d 925, 929 (Utah 2016) (adopting a conclusive presumption for children under the age of five); RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 10(b) (AM. LAW INST. 2010) (same).

112. *See, e.g.*, Carey v. Reeve, 781 P.2d 904, 907 n.3 (Wash. Ct. App. 1989) (children under six years of age cannot form an intent to harm others).

113. *See* Country Mut. Ins. Co. v. Hagan, 698 N.E.2d 271, 278 (Ill. App. Ct. 1998) (explaining that children may be liable for intentional torts where the only intent required is an intent to perform the act, as in the case of battery, whereas children under the age of seven are not liable in negligence because they cannot foresee the consequences of their actions); Shiflet v. Segovia, 318 N.E.2d 876, 879 (Ohio Ct. App. 1974) (same).

114. Patrick v. Mitchell, 6 So. 2d 889, 890 (Ala. 1942); Appelhans v. McFall, 757 N.E.2d 987, 992 (Ill. App. Ct. 2001); *Willoughby*, 387 S.W.2d at 11; *Walston*, 102 S.E.2d at 125; Kuhns v. Brugger, 390 Pa. 331, 135 A.2d 395, 401 (Pa. 1957); Prater v. Burns, 525 S.W.2d 846, 852 (Tenn. Ct. App. 1975).

115. Bush v. N.J. & N.Y. Transit Co., 153 A.2d 28, 33 (N.J. 1959).

116. RESTATEMENT (SECOND) OF TORTS § 283A (AM. LAW INST. 1965); *see also* McGregor v. Marini, 256 So. 2d 542, 543 (Fla. Dist. Ct. App. 1972); M.M. v. Fargo Pub. Sch. Dist. No. 1, 783 N.W.2d 806, 813 (N.D. 2010); *Kuhns*, 135 A.2d at 401; Standard v. Shine, 295 S.E.2d 786, 787 (S.C. 1982); Elizabeth G. Porter, *Tort Liability in the Age of the Helicopter Parent*, 64 ALA. L. REV. 533, 558 n.123 (2013). This rule also applies in Australia and in England. *McHale v. Watson* (1966) 115 CLR

in determining whether the child knew with substantial certainty that his or her intentional act would cause a harmful or offensive contact.[117] Courts may conclude that the specific defendant was unable to form the necessary intent.[118] In jurisdictions with tender-years presumptions of no fault, these adjustments are made beyond the age covered by the presumptions,[119] and in all other jurisdictions they apply to all minors.

All three constraints pertain to fault-based liability, so children may be liable like adults under strict liability regimes.[120] Strict liability usually applies to especially dangerous activities, such as driving or product manufacturing, or to the ownership of dangerous things, such as dogs or weapons; thus, while a child may sometimes be the "keeper" of an animal or the manufacturer of a product, harmful activity subject to strict liability is less likely to involve juvenile perpetrators.[121] More importantly, all causes of action applicable to cyberbullying are fault-based.

3. Technological Barriers

A victim of juvenile cyber-wrongdoing seeking to sue the perpetrator might face a technological barrier because technology enables wrongdoers to mask their true identities.[122] A lawsuit against an anonymous tortfeasor requires a procedural tool to unmask his or her identity. To enable plaintiffs to do so, the law must first devise a process for ordering the relevant platform operator to turn over the wrongdoer's identifying information, usually an Internet Protocol (IP) address. Then, the plaintiff must identify the Internet Service Provider (ISP) linked to the relevant IP address (using the WHOIS directory), and request contact information of the user associated with this IP address.[123] Sometimes, the IP address will point to a public or a multiuser computer, and the plaintiff will need to turn to the

---

199, 210 (Austl.); Ken Oliphant, *Children as Tortfeasors Under the Law of England and Wales*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 147, 154–55 (Miquel Martín-Casals ed., 2006).

117. RESTATEMENT (SECOND) OF TORTS § 895I cmt. b (AM. LAW INST. 1979) ("The immaturity of the infant is, however, to be taken into consideration in determining, in the first instance, whether the tort has been committed at all. In intentional torts, the state of mind of the actor is an essential element . . . . A child may be of such tender years that he has no awareness of these matters and is in fact incapable of the specific intent that is required."); *see also* Garratt v. Dailey, 279 P.2d 1091, 1094 (Wash. 1955).

118. *E.g.*, Seaburg v. Williams, 161 N.E.2d 576, 578 (Ill. App. Ct. 1959) ("Based upon the evidence of defendant's age, capacity, intelligence and experience, we conclude that he lacked the mental and moral capacity to possess the intent to do the act complained of.").

119. *See, e.g.*, *Appelhans*, 757 N.E.2d at 992; *Kuhns*, 135 A.2d at 401.

120. *See* Miquel Martín-Casals, *Comparative Report*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 423, 434 (Miquel Martín-Casals ed., 2006) (concluding that in most legal systems children are subject to strict liability like adults).

121. Oliphant, *supra* note 116, at 157–58.

122. Areheart, *supra* note 43, at 41–42.

123. Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 328 (2008). ISPs usually obtain and retain such information for their ongoing operations, such as billing.

operator of this computer system (a library, a workplace, a café, etc.) to obtain information about the wrongdoer.[124] Some legal systems are reluctant to provide plaintiffs with unmasking abilities.[125] Even in legal systems that enable de-anonymization, tortfeasors may evade liability by using advanced anonymization tools, such as Tor,[126] by connecting through public hotspots which do not require registration or by chance when the relevant records are lost along the way.

American courts can order online platform operators to disclose information about anonymous wrongdoers. True, the right to anonymity is well established under American law, and in some instances—especially when pertaining to speech and assembly—it receives constitutional protection.[127] But when there is sufficient evidence to establish a cause of action against an anonymous user, courts enable the victim to apply for a John Doe subpoena, ordering a third party—here a platform operator or an Internet Service Provider—to divulge information it possesses about that user.[128] Some controversy exists about the standard of evidence for establishing the plaintiff's claim, which must be met prior to issuing such an order,[129] but this procedural tool's availability is undisputed.

4. Financial Barriers

Lawsuits against juvenile cyber-wrongdoers might be hindered by two kinds of financial difficulties—one relating to the victim and the other to the wrongdoer. First, civil litigation is costly. The plaintiff incurs court charges, attorneys' fees, witnesses' and experts' expenditures and remuneration, opportunity costs, and intangible harms.[130] These costs impact the tendency to sue, depending also on the probability of success and the claim-value,[131] and on the plaintiff's economic and

---

124. *Id.* (discussing the two-step process).

125. In Israel, for example, the Supreme Court refused to recognize a procedural tool for requesting disclosure of anonymous users' information. CA 4447/07 Mor v. Barak ITC–Int'l Telecom. Corp. 63(3) PD 664, 717 (2010) (Isr.).

126. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 S. CT. ECON. REV. 221, 234 (2006) (explaining that sophisticated wrongdoers can "conceal their tracks by routing messages through a convoluted path that is difficult for authorities to uncover"). In the related context of online anonymous copyright infringement, a federal district court explicitly admitted that "the technology that enables [wrongdoing] has outpaced technology that prevents it." Hard Drive Prods., Inc. v. Doe 1-90, No. C11-03825 HRL, 2012 U.S. Dist. LEXIS 45509, at *23 (N.D. Cal. Mar. 30, 2012).

127. A. Michael Froomkin, *Anonymity and the Law in the United States*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY, AND IDENTITY IN A NETWORKED SOCIETY 441, 442 (Ian Kerr et al. eds., 2009).

128. *See* Gleicher, *supra* note 123, at 325 (examining the efficacy of John Doe subpoenas).

129. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 600 (4th ed. 2011) (discussing the different standards); Gleicher, *supra* note 123, at 325, 337, 340–50 (same); *see, e.g.*, Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1096–97 (W.D. Wash. 2001) (quashing a subpoena request for identification of anonymous online users because the request failed to show that the information related to the core claim).

130. Ronen Perry, *Crowdfunding Civil Justice*, 59 B.C. L. REV. 1357, 1361 (2018).

131. Louis T. Visscher & Tom Schepens, *A Law and Economics Approach to Cost Shifting, Fee Arrangements and Legal Expense Insurance*, *in* NEW TRENDS IN FINANCING CIVIL LITIGATION IN

psychological conditions. Litigation costs might inhibit access to justice when (1) they exceed the claimant's expected benefit from litigation, (2) the victim does not have sufficient resources, or (3) the victim is unwilling to bear the costs due to risk-aversion and the uncertainties of the process.[132] Various methods have been devised to assist meritorious claimants. For example, attorneys' contingency fee arrangements, whereby lawyers' remuneration is contingent on success and calculated as a percentage of plaintiffs' recovery,[133] third-party litigation funding,[134] and recently even crowdfunding.[135] But these methods may prove inadequate where expected damages are limited and the costs of litigation—including the costs of tracking down anonymous culprits, litigating, and enforcing judgments—are substantial, as in many cases of cyberbullying.[136]

Second, juvenile wrongdoers are usually judgment-proof defendants.[137] Even if identified, sued, and held liable, they do not have the resources to adequately compensate their victims. Inability to pay damages might undermine the goals of civil liability, including corrective justice and deterrence.[138] However, at this stage it is notable primarily because the existence of a cause of action is futile if the victim cannot recover damages thereunder. The two financial barriers are clearly related: if the tortfeasor is known to be judgment-proof, expected damages are lower; and if litigation costs exceed expected damages, the victim is very likely to give up the lawsuit in the first place.

B. Real-Life Supervisors

1. Parents

Some of the difficulties associated with direct liability of juvenile cyber-wrongdoers may be overcome through secondary or indirect liability. The first category of potential defendants is wrongdoers' parents. The common law does not impose vicarious liability upon parents *qua* parents for their children's torts.[139] Thus, a parent may be vicariously liable only in one of two cases: (1) the child is his or her servant or agent, and the general common law principles of vicarious liability

---

EUROPE 7, 14 (Mark Tuil & Louis Visscher eds., 2005) ("[T]here is a critical probability of success and a critical value of the claim below which the plaintiff will not sue.").

132. Perry, *supra* note 130, at 1361.

133. *Id.* at 1364.

134. *Id.* at 1365–66.

135. *Id.* at 1368–70.

136. *See* Walther, *supra* note 3, at 546 (explaining that the relatively high litigation costs might deter cyberbullying victims from pursuing meritorious claims).

137. *See* Areheart, *supra* note 43, at 42 (noting that most cyberbullies are judgment-proof); Walther, *supra* note 3, at 546 (same).

138. *See infra* Section II.A.

139. Kaminski v. Fairfield, 578 A.2d 1048, 1051 (Conn. 1990); Corley v. Lewless, 182 S.E.2d 766, 768–69 (Ga. 1971); Wade R. Habeeb, Annotation, *Parents' Liability for Injury or Damage Intentionally Inflicted by Minor Child*, 54 A.L.R.3d 974, § 3 (2017).

apply;[140] or (2) a statute imposes vicarious parental liability,[141] either generally, as in Hawaii[142] and Louisiana,[143] or in limited contexts, such as malicious or willful causation of physical injury (with very low liability caps)[144] or wrongful driving.[145] A parent may also be directly liable if he or she participates in the child's wrongful conduct by directing or inducing it,[146] consenting thereto,[147] or ratifying it.[148]

Generally, though, parents' liability will hinge on their independent negligence.[149] Three theories of liability may be of use. The first is negligent

---

140. *See, e.g.*, Teagarden v. McLaughlin, 86 Ind. 476, 477–78 (1882) (holding a father-employer liable for harm caused by son-employee); Altoonian v. Muldonian, 177 N.E. 830 (Mass. 1931) (same); *see also* Porter, *supra* note 116, at 557; Habeeb, *supra* note 139, §§ 4–5.

141. *See* Michael A. Axel, *Statutory Vicarious Parental Liability: Review and Reform*, 32 CASE W. RES. L. REV. 559, 565–74 (1982) (discussing the history and nature of these statutes).

142. HAW. REV. STAT. ANN. § 577-3 (West 2019) ("The father and mother of unmarried minor children shall jointly and severally be liable . . . for tortious acts committed by their children . . . .").

143. LA. CIV. CODE ANN. art. 2318 (2019) ("The father and the mother are responsible for the damage occasioned by their minor child . . . ."); Held v. Wilt, 610 So. 2d 1103, 1104 (La. Ct. App. 1992).

144. *See, e.g.*, CAL. CIV. CODE § 1714.1 (West 2019) (limiting the parent's liability for any tort committed by the child to $25,000); CONN. GEN. STAT. ANN. § 52-572 (West 2019) (limiting liability to $5,000); GA. CODE ANN. § 51-2-3 (West 2019) (limiting liability to $10,000); KAN. STAT. ANN. § 38-120 (2019) (limiting liability to $5,000, unless the parent was negligent); MICH. COMP. LAWS ANN. § 600.2913 (West 2019) (limiting liability to $2,500); NEB. REV. STAT. ANN. § 43-801 (West 2019) (limiting liability to $1,000); NEV. REV. STAT. ANN. § 41.470 (West 2019) (limiting liability to $10,000); N.M. STAT. ANN. § 32A-2-27 (West 2019) (limiting liability to $4,000); N.C. GEN. STAT. ANN. § 1-538.1 (West 2019) (limiting liability to $2,000); OHIO REV. CODE ANN. §§ 3109.09–.10 (West 2019) (limiting liability to $10,000); WYO. STAT. ANN. § 14-2-203 (2019) (limiting liability to $2,000; applies only to property damage); *see also* Hanks v. Booth, 726 P.2d 1319 (Kan. 1986) (applying the Kansas provision); Alber v. Nolle, 645 P.2d 456, 458 (N.M. Ct. App. 1982) (applying the New Mexico provision); Cent. Mut. Ins. Co. v. Rabideau, 395 N.E.2d 367 (Ohio Ct. App. 1977) (applying the Ohio provision).

145. *See, e.g.*, ALASKA STAT. ANN. § 28.15.071 (West 2019); ARIZ. REV. STAT. ANN. § 28-3160 (2019); ARK. CODE ANN. § 27-16-702 (West 2019); N.M. STAT. ANN. § 66-5-11 (West 2019).

146. Porter, *supra* note 116, at 557; Habeeb, *supra* note 139, § 6.

147. Habeeb, *supra* note 139, § 7.

148. *Id.* § 8.

149. This is also true in most civil law jurisdictions. In some, the victim must establish the parent's fault. *See, e.g.*, Bertil Bengtsson, *Children as Tortfeasors Under Swedish Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 415, 417–18 (Miquel Martín-Casals ed., 2006); Susanna Hirsch, *Children as Tortfeasors Under Austrian Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 7, 40–41 (Miquel Martín-Casals ed., 2006) (discussing ALLGEMEINES BURGERLICHES GESETZBUCH [ABGB] [CIVIL CODE] § 1309 (Austria)). In others, a rebuttable presumption of fault exists. *See, e.g.*, Giovanni Comandé & Luca Nocco, *Children as Tortfeasors Under Italian Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 265, 278–79 (Miquel Martín-Casals ed., 2006) (discussing Codice civile [C.c.] §§ 2047-48 (It.)); Pieter De Tavernier, *Children as Tortfeasors Under Belgian Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 63, 85–88 (Miquel Martín-Casals ed., 2006) (discussing CODE CIVIL [C.CIV.] art. 1384(2), (5) (Belg.), whereby parents are liable for any damage caused by their minor children unless they can demonstrate they have not committed a wrongful conduct); Miquel Martín-Casals et al., *Children as Tortfeasors Under Spanish Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 369, 387-90 (Miquel Martín-Casals ed., 2006) (discussing Spanish law); Gerhard Wagner, *Children as Tortfeasors Under German Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 217, 235–37 (Miquel Martín-Casals ed., 2006) (discussing BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], § 832 (Ger.)).

entrustment of a dangerous instrument. The Second Restatement of Torts offers a relatively broad interpretation of this principle. Section 390 provides that a person who supplies a chattel for the use of another, when he or she knows or has reason to know that the other is likely, because of young age, to use it in a way creating unreasonable risk of physical harm to that other or to third parties, is liable for ensuing physical harm.[150] Put differently, a parent may be directly liable for the child's wrongdoing if he or she was negligent in entrusting to the child an instrument which, because of its nature, use, and purpose, is so dangerous as to constitute, in the hands of the child, an unreasonable risk to others.[151] Arguably, in the case of cyberbullying, liability can arise if a parent negligently entrusts a computer, a tablet, or a smartphone to a child, when the parent knows or should know that the child is likely to use the device to cyberbully his or her peers.[152]

The element of entrustment does not raise a special problem in the current context. "Entrustment" encompasses giving an item, such as a personal computer or a smartphone, to the child as a present, allowing the child to temporarily borrow the item, and allowing the item to be in such a position that the child could use it even without permission.[153] The element of actual or constructive knowledge is established if the person who receives the chattel belongs to a class which is notoriously incompetent to use it safely, lacks the individual training and experience necessary for safe use, previously acted in a way that makes a dangerous use of the chattel likely, or has a propensity or intent to misuse the chattel despite being able to use it safely.[154] If a child has a past record of cyber-wrongdoing (or even physical bullying), a tendency to harass or an expressed intent to do so, the parent knows or has reason to know of the risk. On the other hand, the element of physical harm limits the applicability of the doctrine in cyberbullying cases, which usually do not culminate in personal injury or death.

Moreover, although several jurisdictions follow the Restatement's broad language,[155] many do not, so an action for negligent entrustment in the case of cyber-wrongdoing may raise two additional difficulties. First, some jurisdictions require actual knowledge, rather than constructive knowledge, that the child's use of the chattel would expose a third party to an unreasonable risk of injury.[156] This does not preclude parental liability for juvenile cyber-wrongdoing, but surely curtails it. The plaintiff must establish the parent's actual knowledge that the child is likely to use the device unreasonably.[157] Second, many jurisdictions insist that the chattel

150. RESTATEMENT (SECOND) OF TORTS § 390 (AM. LAW INST. 1965).

151. Meier v. Schrock, 405 S.W.3d 31 (Mo. Ct. App. 2013).

152. Walther, *supra* note 3, at 558–59.

153. *Id.* at 560.

154. RESTATEMENT (SECOND) OF TORTS § 390 cmt. b.

155. *See, e.g.*, Killeen v. Harmon Grain Prods., Inc., 413 N.E.2d 767, 771 (Mass. App. Ct. 1980); Moning v. Alfono, 254 N.W.2d 759, 768 n.24 (Mich. 1977).

156. *See, e.g.*, Johnson v. Patterson, 570 N.E.2d 93, 96–97 (Ind. Ct. App. 1991); Walther, *supra* note 3, at 550–52.

157. Walther, *supra* note 3, at 558–62.

be "inherently dangerous."[158] Most courts have adopted a restrictive interpretation of this term, recognizing only automobiles and firearms as inherently dangerous.[159] If a parent gives the child access to a car or a gun, knowing that the child could not be trusted with such devices, and the child harms someone by misusing the device, then the parent can be sued for negligent entrustment.[160] In contrast, electronic devices and applications are not dangerous in the classical sense.[161] Thus, for example, the court in the seminal cyberbullying case of *Finkel v. Dauber*[162] held that a computer system is not "inherently dangerous."[163]

The second theory of liability is negligent supervision. In many states, when a child commits a tort, the parent is liable for failing to exercise reasonable care in controlling the child if two conditions are met: (1) the parent knows or has reason to know that he or she has the ability to control the child, and (2) the parent knows of or should know of the necessity and opportunity of exercising such control.[164] Traditionally, many courts have found no foreseeability and hence no duty of care unless the plaintiff showed that the parent-defendant knew, or at least should have known, of the child's dangerous propensity.[165] The Third Restatement of Torts aims to subsume such factors within a more general analysis of reasonable care.[166] The negligent supervision theory can be applied to cases of cyberbullying when the perpetrator's parents are aware or should be aware of the wrongdoing and can prevent it. For example, in *Boston v. Athearn*,[167] the court held that parents could be held liable for negligently failing to supervise their child's use of the family computer and Internet account to defame his peer (by faking and abusing a Facebook account under her name), at least after they were informed of his misconduct.[168] Note, however, that not all states recognize this doctrine. For instance, the court in *Finkel v. Dauber*[169] held that "there is no cause of action for negligent supervision of a

158. *See, e.g.*, Evans v. Shannon, 776 N.E.2d 1184, 1190 (Ill. 2002); Kennedy v. Baird, 682 S.W.2d 377, 378–79 (Tex. App. 1984); Walther, *supra* note 3, at 552–57.

159. *See, e.g.*, Wilbanks v. Brazil, 425 So. 2d 1123, 1125 (Ala. 1983) ("[A]ll cases arising under the negligent entrustment doctrine have involved entrustment of vehicles, boats, firearms, or explosives . . . ."); Brewster v. Rankins, 600 N.E.2d 154, 158 (Ind. Ct. App. 1992) (finding that a golf club is not an inherently dangerous instrument); Walther, *supra* note 3, at 553.

160. Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051, 1108 (2018).

161. Heller, *supra* note 50, at 173.

162. Finkel v. Dauber, 906 N.Y.S.2d 697 (Sup. Ct. 2010).

163. *Id.* at 702.

164. RESTATEMENT (SECOND) OF TORTS § 316 (AM. LAW INST. 1965); RESTATEMENT OF TORTS § 316 (AM. LAW INST. 1934); Heller, *supra* note 50, at 169–70; Habeeb, *supra* note 139, § 10.

165. RESTATEMENT (SECOND) OF TORTS § 316 reporter's note (AM. LAW INST. 1965) ("There must . . . be some specific propensity of the child, of which the parent has notice."). Many courts consider "dangerous propensity" a precondition for a finding of foreseeability. *See, e.g.*, Fuller v. Studer, 833 P.2d 109, 113 (Idaho 1992) (finding no dangerous propensity); Porter, *supra* note 116, at 558–61.

166. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 41 reporter's note to cmt c (AM. LAW INST. 2012); Porter, *supra* note 116, at 565–67, 569–70.

167. Boston v. Athearn, 764 S.E.2d 582 (Ga. Ct. App. 2014).

168. *Id.* at 587.

169. Finkel v. Dauber, 906 N.Y.S.2d 697 (Sup. Ct. 2010).

child, absent an allegation that the parent entrusted the child with a dangerous instrument which caused harm to a third party."[170] As a comparative note, some Canadian provinces impose liability based on negligent supervision with a reverse burden of proof through specific legislation.[171]

In most jurisdictions, the parents are not under any duty to supervise their child when he or she is at school or taking part in a school activity; only school personnel and the school itself can be held liable for failing to supervise a student who committed a wrong under these circumstances.[172] Still, in some Romance jurisdictions, the parents may be held liable for breach of a duty to educate the child, if lack of proper education results in wrongdoing at school.[173] In some Germanic jurisdictions, when the child is at school, the parents' duty to supervise is reduced to a duty to reasonably verify that the school exercises proper supervision (and this duty is presumably fulfilled if the school is public).[174]

The third and last theory of liability, which in essence is a generalization of the previous two, is negligent enabling of a tort.[175] Some jurisdictions hold a parent liable for an injury caused by the child if the parent's negligence made it possible for the child to cause the injury and probable that the child would do so.[176] Providing a child, especially an ill-disciplined adolescent, with unlimited and unsupervised Internet access may enable cyber-wrongdoing. Goldberg and Zipursky observe that "courts continue to resist the dilution of the circumscribed concept of negligent entrustment into the much broader concept of negligent enabling . . . . [T]hey reject the composite assertion . . . that carelessness increasing the risk of misconduct by another" calls for liability in negligence.[177] But while the idea of negligent enabling is open-ended and therefore controversial, courts have widely recognized such a

---

170. *Id.* at 702.

171. *See, e.g.*, Parental Liability Act, S.B.C. 2001, c 45, § 3, 6, 9 (Can.) (imposing liability for property damage caused by the child unless parents can establish non-negligence; limiting liability to CAD 10,000); The Parental Responsibility Act, S.M. 1996, c 61, § 3, 7 (Can.) (same); Parental Responsibility Act, S.O. 2000, c 4, § 2 (Can.) in conjunction with the Small Claims Courts Jurisdiction and Appeal Limit, O. Reg. 626/00, § 1 (Can.) (same, with a CAD 35,000 limit).

172. *See* Martín-Casals, *supra* note 120, at 465; Oliphant, *supra* note 116, at 163, 165–66.

173. *See, e.g.*, Comandé & Nocco, *supra* note 149, at 278, 283–84 (discussing "*culpa in educando*"); Maria Manuel Veloso, *Children as Tortfeasors Under Portuguese Law*, *in* CHILDREN IN TORT LAW, PART I: CHILDREN AS TORTFEASORS 311, 335 (Miquel Martín-Casals ed., 2006) (discussing "*culpa in eligendo*").

174. *See, e.g.*, Hirsch, *supra* note 149, at 47, 61; Martín-Casals, *supra* note 120, at 465; Wagner, *supra* note 149, at 247, 263.

175. *Cf.* Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 438–43 (1999) (discussing the concept and enabling situations).

176. Buelke v. Levenstadt, 214 P. 42, 44 (Cal. 1923); *see also* Langford v. Shu, 128 S.E.2d 210, 212–13 (N.C. 1962) ("A parent is liable for the act of his child if the parent's conduct was such as to render his own negligence a proximate cause of the injury complained of."); Condel v. Savo, 39 A.2d 51, 52 (Pa. 1944) ("[T]he parents may be liable . . . where the negligence of the parents makes the injury possible.").

177. John C.P. Goldberg & Benjamin C. Zipursky, *Intervening Wrongdoing in Tort: The Restatement (Third)'s Unfortunate Embrace of Negligent Enabling*, 44 WAKE FOREST L. REV. 1211, 1225 (2009).

general principle in parent-child settings.[178] A greater obstacle in the current context is that the principle has only been used with respect to physical harm.[179]

Parents' liability ameliorates some of the practical difficulties with the child's liability—legal obstacles associated with the defendant's age and the problem of judgment-proof defendants. However, the technological barrier of anonymity must be equally addressed when tort actions against wrongdoers' parents are concerned. If the victim cannot identify the wrongdoer, neither can he or she identify and bring an action against a parent, unless someone perpetrated the wrongdoing through the parent's electronic device, and it is unclear which child was the culprit. This observation is crucial for the construction of an efficient liability model.

2. Teachers, Schools, and Education Authorities

As with parents, the most plausible theory of liability in an action against educators and schools is independent negligence.[180] In all Western jurisdictions, common law and civil law alike, teachers and schools are under a duty to reasonably supervise students, and if failure to comply causes harm, it is actionable in tort.[181] This duty usually applies when the children are on school premises, even if they are not in class, or when they take part in out-of-school activities organized by the school.[182] To the extent that the educator in charge is employed by a private institution or a public authority, the employer's liability will usually be vicarious,[183] although the institution or the authority can be directly liable if fault can be attributed thereto.[184]

Negligent supervision actions may face several obstacles. For instance, in some jurisdictions, schools owe students a duty to properly supervise school personnel and students in order to prevent physical injury but not emotional harm, which is the prevalent outcome of cyberbullying.[185] Additionally, in most jurisdictions, school districts and public school employees may invoke governmental immunity in cases of negligence in policymaking or in the exercise of discretionary functions, as opposed to operational conduct.[186] The immunity does

178. *See* Habeeb, *supra* note 139, § 9.

179. *See id.*

180. *See* Fenn, *supra* note 27, at 2739–46 ("In cases where a victim of on-campus bullying by another student wishes to hold a school district or its employees liable, the victim must show negligence on the part of the school.").

181. *See, e.g.*, Rupp v. Bryant, 417 So. 2d 658, 666 (Fla. 1982); *see also* Martín-Casals, *supra* note 120, at 459 (reviewing the law in European jurisdictions).

182. Martín-Casals, *supra* note 120, at 459.

183. *See* RESTATEMENT (SECOND) OF AGENCY § 219 (AM. LAW INST. 1958).

184. Oliphant, *supra* note 116, at 166.

185. *See, e.g.*, Theno v. Tonganoxie Unified Sch. Dist. No. 464, 377 F. Supp. 2d 952, 968–69 (D. Kan. 2005) (applying Kansas law).

186. *See, e.g.*, CONN. GEN. STAT. § 52-557n (2019); 745 ILL. COMP. STAT. ANN. 10 / 2-201 (West 2018) (as interpreted in Albers v. Breen, 806 N.E.2d 667, 673 (Ill. App. Ct. 2004)); TENN. CODE ANN. § 29-20-205(1) (2019) (as interpreted in Bowers v. City of Chattanooga, 826 S.W.2d 427, 430–31 (Tenn. 1992)); Estate of Girard v. Town of Putnam, No. CV085002754-S, 2011 WL 78599,

not apply where the supervision of students generally or the specific failures are deemed "operational" rather than "discretionary."[187] In many jurisdictions, immunity cannot be invoked if the plaintiff establishes that the defendant was grossly negligent[188] or acted willfully.[189] In some, it is precluded "when the circumstances make it apparent to [a] public officer that his or her failure to act would be likely to subject an identifiable person to imminent harm."[190]

In the United States, federal legislation provides additional bases for liability. First, a victim of cyber-harassment at a public school can bring an action against the school pursuant to 18 U.S.C. § 1983,[191] where allowing the aggressor's misconduct violates the victim's constitutional rights.[192] For example, in *T.E. v. Pine Bush Central School District*,[193] Jewish students who suffered anti-Semitic harassment, including verbal and physical threats,[194] brought a lawsuit against the school district under § 1983 for the violation of the Equal Protection Clause.[195] The court denied a motion to dismiss, holding that to succeed in such an action, the plaintiff must satisfy three conditions: (1) the victim was harassed by other students based on membership in a protected group, such as race; (2) the harassment was known to the school; (3) the school's response was "clearly unreasonable in light of the known circumstances," to the extent that an intent to harass can be attributed to the school.[196] In contrast, it seems clear that violation of state statutes on bullying in general, and cyberbullying in particular,[197] does not provide a basis for a claim under § 1983.[198]

---

at *5 (Conn. Super. Ct. Jan. 28, 2011); Burns v. Gagnon, 727 S.E.2d 634, 646 (Va. 2012); Fenn, *supra* note 27, at 2742–43 (discussing the immunity).

187. *See* Wyke v. Polk Cty. Sch. Bd., 129 F.3d 560, 571 (11th Cir. 1997).

188. *See, e.g.*, *Burns*, 727 S.E.2d at 646–47 (explaining that an individual entitled to the protection of sovereign immunity may be liable if grossly negligent).

189. *See, e.g.*, Chisolm v. Tippens, 658 S.E.2d 147, 151 (Ga. Ct. App. 2008) (explaining that the immunity does not apply in the case of willful conduct).

190. Grady v. Town of Somers, 984 A.2d 684, 690 (Conn. 2009).

191. 42 U.S.C. § 1983 (2019) ("Every person who . . . subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law . . . .").

192. Liability of private schools under 42 U.S.C. § 1981 (2019) is more limited.

193. T.E. v. Pine Bush Cent. Sch. Dist., 58 F. Supp. 3d 332 (S.D.N.Y. 2014).

194. *Id.* at 339–50.

195. U.S. CONST. amend. XIV, § 1.

196. *T.E.*, 58 F. Supp. 3d at 368. *But cf.* R.S. *ex rel.* S.S. v. Bd. of Educ. of Hastings-On-Hudson Union Free Sch. Dist., 371 F. App'x 231, 234 (2d Cir. 2010) (finding, in a § 1983 claim for sexual harassment, that the third condition was not met).

197. *See supra* notes 25–26.

198. *See* O'Dell v. Casa Grande Elem. Sch. Dist. No. 4, No. CV-08-0240-PHX-GMS, 2008 U.S. Dist. LEXIS 100968, at *19–20 (D. Ariz. Dec. 12, 2008) (discussing Arizona anti-bullying legislation, holding that a violation of state law cannot be a basis for a § 1983 action because the section provides a remedy for "deprivation of rights secured by the Federal Constitution and Laws."); Chisolm v. Tippens, 658 S.E.2d 147, 152 (Ga. Ct. App. 2008) (discussing Georgia anti-bullying legislation, holding § 1983 does not apply to violations of state laws).

Second, in limited cases, a juvenile cyberbullying victim can bring an action against the school pursuant to Title VI of the Civil Rights Act of 1964, which prohibits a recipient of federal funds from discriminating on the basis of race, color, or national origin.[199] The United States Department of Education's regulations elaborate further that a recipient of federal funds may not, "on ground of race, color, or national origin . . . [r]estrict an individual in any way in the enjoyment of any advantage or privilege enjoyed by others receiving any service, financial aid, or benefit under the program."[200] Similarly, a recipient cannot "[d]eny an individual an opportunity to participate in the program through the provision of services or otherwise or afford him an opportunity to do so which is different from that afforded others under the program" on the basis of race, color, or national origin.[201] In the *T.E.* case, the court held that anti-Semitic harassment amounts to racial discrimination.[202] A school district can be liable under Title VI if four conditions are met:[203] (1) the school had substantial control over the circumstances, normally because the misconduct occurred during school hours and on school grounds; (2) the harassment was severe, pervasive, and objectively offensive and discriminatory, in the sense that it generated a "systemic effect of denying the victim equal access to an educational program or activity, and more than episodic"; (3) the school actually knew about the harassment (constructive knowledge is insufficient); and (4) the district was deliberately indifferent to the harassment, making its actions "clearly unreasonable in light of the known circumstances."[204] In the limited context of cyber-harassment based on race, color, or national origin, and perpetrated by public school students, school districts can be liable if the four conditions are met.

Third, in the appropriate cases, a juvenile cyber-harassment victim may bring an action against the (public) school based on Title IX of the Education Amendments Act of 1972,[205] which prohibits discrimination on the basis of sex (including sexual orientation[206]) in educational institutions receiving federal funding, or on the Rehabilitation Act of 1973,[207] which prohibits disability-based discrimination in such institutions. The analysis of claims under Title IV applies *mutatis mutandis* to claims under these two statutes, which cover additional categories of discrimination. For example, in *R.S. ex rel. S.S. v. Board of Education of Hastings-On-Hudson Union Free School District*,[208] a student sued the school district

199. 42 U.S.C. § 2000d (2019).

200. 34 C.F.R. § 100.3(b)(1)(iv) (2019).

201. *Id.* § 100.3(b)(1)(vi) (2019).

202. T.E. v. Pine Bush Cent. Sch. Dist., 58 F. Supp. 3d 332, 354 (S.D.N.Y. 2014).

203. *Id.* at 355.

204. *Id.* at 355–56.

205. 20 U.S.C. § 1681 (2019).

206. *See* Theno v. Tonganoxie Unified Sch. Dist. No. 464, 377 F. Supp. 2d 952, 963–65 (D. Kan. 2005) (holding on the basis of *Oncale v. Sundowner Offshore Servs., Inc.*, 523 U.S. 75 (1998) and its progeny that same-sex student-on-student harassment is actionable under Title IX).

207. 29 U.S.C. § 794 (2019).

208. R.S. *ex rel.* S.S. v. Bd. of Educ. of Hastings-On-Hudson Union Free Sch. Dist., 371 F. App'x 231 (2d Cir. 2010).

under Title IX for sexual harassment by another student, who sent her three harassing e-mails. The court held that the record was insufficient "to permit a reasonable jury to find that S.S. endured harassment so severe and pervasive as to have effectively denied her access to educational resources and opportunities."[209] In other words, the harassment did not satisfy the severity requirement, which sets a high threshold for recovery.

Lastly, victims of juvenile cyber-wrongdoing may occasionally sue the school district under state anti-discrimination legislation. For example, in *L.W. v. Toms River Regional Schools Board of Education*,[210] the Supreme Court of New Jersey held that the New Jersey Law Against Discrimination[211] recognizes a cause of action against a school district for student-on-student sexual-orientation harassment if the school district knew or should have known of the harassment but failed to take reasonable actions to end it.[212] Similarly, in *Doe v. Kansas City, Missouri School District*,[213] the Court of Appeals of Missouri held that the state's Human Rights Act[214] allows a claim against a school district for student-on-student sexual harassment if the district knew or should have known of the harassment but failed to take action.[215] Although these were real-life harassment cases, the same principles apply to cyber-harassment.

Schools' liability for juvenile cyber-wrongdoing may raise several problems. The most fundamental concern is that any duty to supervise and limit students' cyber-communications might infringe on their freedom of speech.[216] Students do not enjoy the same level of constitutional protection as adults due to the "special characteristics of the school environment."[217] Yet the boundaries of schools' supervision duties must be consistent with the boundaries of students' First Amendment rights. In *Tinker v. Des Moines Independent Community School District*,[218] the Supreme Court limited school districts' power to regulate and punish students' speech to instances in which on-campus expression "materially and substantially interfer[es] with the requirements of appropriate discipline in the operation of the

209. *Id.* at 233.

210. L.W. v. Toms River Reg'l Sch. Bd. of Educ., 915 A.2d 535 (N.J. 2007).

211. N.J. STAT. ANN. § 10:5-4 (West 2019) ("All persons shall have the opportunity to . . . obtain all the accommodations, advantages, facilities, and privileges of any place of public accommodation . . . without discrimination because of race, creed, color, national origin, ancestry, age, marital status, affectional or sexual orientation, familial status, disability . . . nationality, sex . . . . This opportunity is recognized as and declared to be a civil right.").

212. *L.W.*, 915 A.2d at 540.

213. Doe v. Kansas City, Mo. Sch. Dist., 372 S.W.3d 43 (Mo. Ct. App. 2012).

214. MO. REV. STAT. § 213.065(2) (2019) ("It is an unlawful discriminatory practice for any person, directly or indirectly, to refuse, withhold from or deny any other person . . . any of the accommodations, advantages, facilities, services, or privileges made available in any place of public accommodation . . . or to segregate or discriminate against any such person in the use thereof on the grounds of race, color, religion, national origin, sex, ancestry, or disability.").

215. *Doe*, 372 S.W.3d at 54.

216. Fenn, *supra* note 27, at 2749.

217. Morse v. Frederick, 551 U.S. 393, 396–97 (2007).

218. Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 509, 513 (1969).

school" or involves "invasion of the rights of others."[219] According to subsequent case law, schools can also regulate on-campus student expression when it is "offensively lewd and indecent" (and "unrelated to a political viewpoint"),[220] or might be reasonably perceived as bearing the school's imprimatur, such as a school newspaper or play,[221] or promotes criminal activity, such as drug use.[222] When a school unlawfully prevents *ex ante* or punishes *ex post* a student's potentially harmful cyber-communication, the latter can pursue an injunction[223] or claim damages for violation of his or her First Amendment rights under § 1983.[224]

An additional problem is that schools' power may not equally extend to off-campus activities.[225] For instance, in *Morse v. Frederick*, [226] the Supreme Court opined that had the offensively lewd and indecent speech discussed in a previous case been delivered "in a public forum outside the school context, it would have been protected." To be sure, some federal and state courts held that schools can regulate and discipline for off-campus cyber-wrongdoing which might materially and substantially disrupt school life, as per *Tinker*.[227] Still, it is unlikely that the

---

219. *Id.* at 513; Papandrea, *supra* note 4, at 1038–45 (discussing the *Tinker* test and its applications).

220. Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675, 685 (1986).

221. Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260, 271 (1988).

222. *Morse*, 551 U.S. at 397.

223. *See, e.g.*, Beussink v. Woodland R-IV Sch. Dist., 30 F. Supp. 2d 1175, 1182 (E.D. Mo. 1998) (awarding an injunction against a school that suspended a student who created a website critical of the school).

224. *See, e.g.*, J.C. v. Beverly Hills Unified Sch. Dist., 711 F. Supp. 2d 1094 (C.D. Cal. 2010) (discussing a claim against a school for suspending a student who posted a video of her friends talking in a disparaging fashion about a classmate); Evans v. Bayer, 684 F. Supp. 2d 1365, 1367, 1374, 1377 (S.D. Fla. 2010) (discussing a lawsuit against a school for suspending a student who created a Facebook page to share students' hatred for a teacher); Layshock *ex rel.* Layshock v. Hermitage Sch. Dist., 496 F. Supp. 2d 587, 600 (W.D. Pa. 2007) (finding a school liable for disciplining a student who created a parody profile of the school's principal on an internet website after school hours).

225. *See Layshock*, 496 F. Supp. 2d at 596 (explaining that schools' authority over off-campus expression is much more limited than expression on school grounds); Kristopher L. Jiles, *Trigger Fingers Turn to Twitter Fingers: The Evolution of the* Tinker *Standard and its Impact on Cyberbullying amongst Adolescents*, 61 HOW. L.J. 641, 655 (2018) (same); Daniel Marcus-Toll, Tinker *Gone Viral: Diverging Threshold Tests for Analyzing School Regulation of Off-Campus Digital Student Speech*, 82 FORDHAM L. REV. 3395, 3416–19 (2014) (same); Papandrea, *supra* note 4, at 1028–30 (same); Poole, *supra* note 2, at 252 (same).

226. Morse v. Frederick, 551 U.S. 393, 405 (2007).

227. *See, e.g.*, Doninger v. Niehoff, 527 F.3d 41, 48–50 (2d Cir. 2008) ("[A] student may be disciplined for expressive conduct, even conduct occurring off school grounds, when this conduct 'would foreseeably create a risk of substantial disruption within the school environment,' at least when it was similarly foreseeable that the off-campus expression might also reach campus."); Wisniewski v. Bd. of Educ. of the Weedsport Cent. Sch. Dist., 494 F.3d 34, 38–39 (2d Cir. 2007) ("We have recognized that off-campus conduct can create a foreseeable risk of substantial disruption within a school [citations omitted]."); O.Z. v. Bd. of Trs. of the Long Beach Unified Sch. Dist., No. CV 08-5671, 2008 WL 4396869, at *2–3 (C.D. Cal. Sept. 9, 2008) (applying *Tinker* to off-campus YouTube video calling to kill teacher); J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847, 869 (Pa. 2002) (holding that the communication contained in a "Teacher Sux" website caused actual and substantial disruption of the work of the school); *see also* MINN. STAT. § 121A.031(a)(3) (2018) (applying to

school would be allowed to regulate conduct which is neither carried out on its premises nor has a significant impact on its activities.[228] Punishing off-campus cyber-wrongdoing without legal authority may give rise to claims not only for infringements of the freedom of speech but also for Due Process violations.[229]

C. Virtual Supervisors

1. The American Model

An additional layer in any civil law response to cyberbullying is secondary or indirect liability of virtual supervisors, namely platforms that enable juvenile cyber-activity and cyber-wrongdoing, such as Facebook, Gmail, Instagram or YouTube. In the United States, however, it is almost impossible to bring a lawsuit against a virtual supervisor for wrongful user-contributions, even if it knew about their wrongful nature. The explanation goes back to the traditional distinction in defamation law among three types of intermediaries: (1) common carriers, such as telephone companies, which only transmit information and are not liable for defamation;[230] (2) distributors, such as bookstore owners, which distribute content without having control over it and are liable only if they knew or had reason to know about the defamatory nature of the publication;[231] and (3) publishers, such as newspapers, which exercise significant control over published content and are subject to strict liability.[232] In the context of online defamation, this framework generated skewed incentives. In *Cubby, Inc. v. CompuServe Inc.*,[233] the court held that CompuServe, which provided users with access to a virtual newsletter but did not review its content, was a mere distributor and therefore not liable for false and defamatory statements made therein.[234] Conversely, in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[235] the court found that Prodigy, a bulletin board operator that exercised some editorial control over user-generated content, was a publisher, and could be held liable for defamatory statements made by an anonymous user

---

off-campus cyberbullying that "substantially and materially disrupts student learning or the school environment").

228. Jiles, *supra* note 225, at 658–59.

229. *See, e.g.*, J.C. *ex rel.* R.C. v. Beverly Hills Unified Sch. Dist., 711 F. Supp. 2d 1094 (C.D. Cal. 2010) (holding that a student's Due Process was violated when she was suspended after an off-campus posting of a video disparaging a schoolmate); Poole, *supra* note 2, at 254–55.

230. Sewali K. Patel, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 651 (2002).

231. *Id.* at 651–52.

232. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 184 (4th ed. 2011).

233. Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

234. *Id.* at 141.

235. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133, 137.

with respect to a brokerage firm.[236] The joint reading of *Cubby* and *Stratton Oakmont* incentivized platform operators to avoid moderating online discourse because moderating exposed them to the risk of liability, whereas not moderating protected them from liability.[237]

Pressures from the Internet industry quickly led to the enactment of section 230 of the Communications Decency Act of 1996,[238] whereby providers of "interactive computer services" should not be considered publishers of "any information provided by another information content provider."[239] In *Zeran v. America Online, Inc.*,[240] the court held that section 230 "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[241] In particular, a message board operator could not be found liable for defamatory postings by an anonymous user, even though the operator had relevant knowledge after a certain point and would have been considered a publisher under traditional defamation law.[242] The court explained that imposing liability on platform operators just because they had knowledge about the wrongful content would defeat the purposes of section 230: promoting free speech on the one hand, and encouraging platforms' self-regulation on the other.[243] If platform operators were subject to knowledge-based liability, receiving a notification about a potentially wrongful statement would require making a "careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information."[244] The vast number of postings would create "an impossible burden in the Internet context."[245] Because platform operators would be liable only for the publication of information and not for its removal, they would have a strong incentive to simply remove content upon notification.[246]

Following *Zeran*, section 230 has provided online platforms, be they publishers or distributors under traditional law,[247] with effective immunity from

236. *Id.* at *4–5; *see also* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 650–51 (2014) (discussing the impact of *Stratton Oakmont*). Some of the statements about the firm were later found to be true, but it was too late for the defendant. *See* Joe Nocera, *Sex and Drugs and I.P.O.'s: Martin Scorsese's Approach in 'The Wolf of Wall Street*,*'* N.Y. TIMES (Dec. 19, 2013), https://www.nytimes.com/2013/12/22/movies/martin-scorseses-approach-in-the-wolf-of-wall-street.html [https://perma.cc/L37B-VN8D].

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

238. Communications Decency Act § 230 (codified as amended at 47 U.S.C. § 230 (2018)).

239. 47 U.S.C. § 230(c)(1).

240. *Zeran*, 129 F.3d 327.

241. *Id.* at 330.

242. *Id.* at 330–32.

243. *Id.* at 333.

244. *Id.*

245. *Id.*

246. *Id.*

247. *See* Barrett v. Rosenthal, 146 P.3d 510, 519 (Cal. 2006) ("There is even less reason to

liability for user-generated content.[248] The immunity covers all kinds of platforms, including social networking websites and applications, such as Facebook or Twitter,[249] search engines, such as Google and Yahoo,[250] operators of online business-review systems, such as Yelp,[251] e-commerce platforms, such as Amazon,[252] and operators of online message boards[253] and chat rooms.[254] Furthermore, the immunity applies to all relevant causes of action, including defamation, privacy invasions, intentional infliction of emotional distress, and civil rights violations.[255] As noted above, the immunity applies even if the platform knew or should have known about the wrongdoing[256] or acted negligently with respect to user wrongdoing.[257]

2. Alternatives and Calls for Reform

The American position on this matter is exceptional. In the European Union, for example, a victim of online defamation can frequently bring an action against the platform. Article 14 of the E-Commerce Directive[258] provides that some intermediaries, such as hosting service providers, are liable only if they knew about the wrongful statement and failed to remove it following the victim's request (a

---

suppose that Congress intended to immunize 'publishers' but leave 'distributors' open to liability, when the responsibility of publishers for offensive content is greater than that of mere distributors.").

248. However, empirical studies have shown that more than one-third of such claims survive the section 230 defense, and accordingly websites often have to engage in long and expensive legal battles. *See* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 493 (2010); Chander, *supra* note 236, at 655.

249. Caraccioli v. Facebook, Inc., 167 F. Supp. 3d 1056, 1065–66 (N.D. Cal. 2016) (holding that Facebook "provides an interactive computer service" for the purposes of section 230).

250. Stayart v. Yahoo! Inc., 651 F. Supp. 2d 873, 885 (E.D. Wis. 2009) (holding that "Yahoo! should be entitled to immunity because it acted as an interactive computer service").

251. Kimzey v. Yelp Inc., 21 F. Supp. 3d 1120, 1123 (W.D. Wash. 2014) ("Yelp qualifies as an 'interactive computer service' within the meaning of the CDA.").

252. Joseph v. Amazon.com, Inc., 46 F. Supp. 3d 1095, 1105–07 (W.D. Wash. 2014) (concluding that Amazon is an interactive computer service provider).

253. DiMeo v. Max, 248 F. App'x. 280, 282 (3d Cir. 2007) (holding that an online message board operator is an interactive computer service provider).

254. Doe v. Am. Online, Inc., 783 So. 2d 1010, 1013–17 (Fla. 2001) (holding that America Online, the operator of a chat room in which a third party posted obscene images of the plaintiff's son, is immune under section 230).

255. *See* Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321 (11th Cir. 2006) ("The majority of federal circuits have interpreted the CDA to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 171 (2014) (listing relevant causes of action); Chander, *supra* note 236, 651 ("[Section 230] largely immunized online service providers from secondary liability for most torts committed through their service."). For an extensive list of cases, see Chander, *supra* note 236, at 653 n.58.

256. CITRON, *supra* note 255, at 171.

257. Green v. Am. Online, Inc., 318 F.3d 465, 471 (3d Cir. 2003).

258. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L 178) 1, 14 (July 17, 2000).

notice-and-takedown regime). This means, first, that knowledge can generate liability. Moreover, many platforms are not considered intermediaries for these purposes, and may be liable even in the absence of knowledge about the wrongful content. In the case of *Delfi AS v. Estonia*,[259] the European Court of Human Rights held that a news website was liable for defamation in anonymous user comments.[260] The court agreed that the website was a publisher rather than an intermediary, and that it was not exempt from the duty to monitor or from liability despite implementing a notice-and-takedown system.[261] In mid-June 2015, the Grand Chamber of the court upheld the earlier decision, possibly limiting its application to news portals.[262]

A more structured approach was endorsed in the United Kingdom, where the Defamation Act links the platform's liability to the speaker's unavailability.[263] Section 5(2) stipulates that a website operator is generally not liable for a defamatory statement posted on the website if it was not the one who posted that statement.[264] However, the defense can be defeated (and the operator exposed to liability) if the victim had insufficient information to identify and bring proceedings against the speaker, the victim gave notice of the complaint, and the operator did not properly respond to the complaint.[265] A proper response requires obtaining the speaker's contact information and providing it to the victim or removing the defamatory content.[266]

Some commentators advocated replacing section 230 with a notice-and-takedown regime, which is not only comparable to the European model,[267] but has also been applied in the United States to copyright infringement under the Digital Millennium Copyright Act (DMCA).[268] According to the DMCA, where an Internet service provider offers system caching, information storage, or information location tools, and it receives actual notice of the infringing material, it must remove the content or risk liability through the loss of immunity.[269] Others proposed a more limited reform, using a notice-and-takedown model only with respect to cyber-wrongdoing against children. When a platform operator is notified

259. Delfi AS v. Estonia, 2013 Eur. Ct. H.R. at para. 94.

260. *Id.* at paras. 28, 50, 94. *See also* Mart Susi, *International Decision:* Delfi AS v. Estonia, 108 AM. J. INT'L L. 295 *passim* (2014) (discussing the *Delfi* decision).

261. *Delfi*, 2013 Eur. Ct. H.R. at paras. 28, 50.

262. Delfi AS v. Estonia, 2015-II Eur. Ct. H.R. 319, paras. 62, 115, 159.

263. Defamation Act 2013, c. 26 (U.K.).

264. *Id.* § 5(2).

265. *Id.* § 5(3)–(4).

266. *Id.* § 5(3)(c), (5).

267. A notice-and-takedown regime was also adopted in non-European jurisdictions. *See, e.g.*, Harmful Digital Communication Act 2015, s 24 (N.Z.) ("No civil or criminal proceedings may be brought against an online content host in respect of the content complained of . . . if the online content host—(a) receives a notice of complaint about the specific content; and (b) complies with [a takedown process].").

268. Areheart, *supra* note 43, at 43.

269. 17 U.S.C. § 512(c)–(d) (2018).

that a child is being harassed through the platform, the operator would be obliged to remove the offending content or cut off the offender's access to the site.[270] Yet none of these proposals have been seriously considered by Congress, so the absolute immunity holds.

II. ECONOMIC ANALYSIS

A. The Wrongdoer

1. Outline

At first glance, a cyber-wrongdoer's liability is a special case of direct tort liability, so its economic justifications should be similar.[271] Efficient deterrence entails internalization by the wrongdoer of the social harm caused by his or her wrongful (that is, inefficient) conduct.[272] Only if expected liability is equivalent to the expected externalized cost[273] will the potential injurer internalize that cost and take cost-effective precautions.[274] In the context of juvenile cyber-wrongdoing, three attributes of the wrongdoers undermine the deterrent effect of liability: (1) inability to compensate; (2) limited cognitive, emotional, and social capacity; and (3) possible anonymity.

2. Inability to Compensate

Children and adolescents are generally judgment-proof defendants: even if found liable, they do not have the resources to compensate their victims.[275] If injurers are unable to fully compensate for harms caused, they will not internalize the social cost of their conduct. From their perspective, the expected expense may be considerably lower than the expected (social) harm, so the incentive for choosing the optimal level of care is impaired.[276] For example, assume that there is a probability of 0.02 that A's conduct will cause a $100,000 loss to B, and that A can reduce the probability of harm to 0.01 by adopting a certain precaution for $800.

---

270. Poole, *supra* note 2, at 245–50, 260.

271. *See, e.g.*, Alain Sheer & Asghar Zardkoohi, *An Analysis of the Economic Efficiency of the Law of Defamation*, 80 NW. U. L. REV. 364 (1985) (analyzing the goals and consequences of defamation law from an economic perspective).

272. Alan D. Miller & Ronen Perry, *The Reasonable Person*, 87 N.Y.U. L. REV. 323, 328 (2012); Ronen Perry, *Economic Loss, Punitive Damages, and the Exxon Valdez Litigation*, 45 GA. L. REV. 407, 426 (2011); Ronen Perry, *Re-Torts*, 59 ALA. L. REV. 987, 990, 994–95 (2008); Ronen Perry, *Strike-Out*, 68 ALA. L. REV. 445, 472 (2016).

273. In cases of negligence-based liability, expected liability may exceed expected externalized cost.

274. Miller & Perry, *supra* note 272, at 346.

275. Steven Shavell, *The Judgment Proof Problem*, 6 INT'L REV. L. & ECON. 45, 45 (1986) (defining judgment-proof defendants).

276. *See* Kyle D. Logue, *Solving the Judgment-Proof Problem*, 72 TEX. L. REV. 1375, 1375 (1994); Shavell, *supra* note 275, at 45; Comment, *The Case of the Disappearing Defendant: An Economic Analysis*, 132 U. PA. L. REV. 145, 157–59 (1983).

The cost of care ($800) is lower than the ensuing reduction in expected harm ((0.02−0.01)×$100,000=$1,000), so the law needs to incentivize A to take this precaution. Now assume that the expected value of A's assets during the subsequent litigation is $30,000 and that A is risk-neutral. Liability would not provide an adequate incentive for choosing the optimal level of care. Under a negligence rule, the expected sanction for failing to take the efficient precaution would be only 0.02×$30,000=$600, whereas the cost of precaution is $800. Under a strict liability regime, A would only save (0.02−0.01)×$30,000=$300 by taking an $800 precaution. Either way, A will not take the necessary precaution.[277]

As law and economics literature demonstrates, primary wrongdoers' liability is inefficient, and supervisors' liability may be desirable, if the wrongdoer is judgment-proof.[278] Specifically, one of the main justifications for employers' vicarious liability is that employees are frequently judgment-proof defendants. Employees' deterrence is sub-optimal, so an alternative liability model is necessary to avoid inefficient conduct.[279] The same rationale applies *a fortiori* to minors, who rarely have any assets. Given juvenile wrongdoers' inability to pay,[280] imposing liability on them would frequently be inefficient. Liability would not deter potential wrongdoers and only entail considerable administrative costs. A substantive defense may be justified, at least if efficient conduct can be secured through another liability model.

3. Limited Cognitive, Emotional, and Social Capacity

Children and adolescents might not be able to fully grasp the wrongfulness of their conduct, and even when they do, they might not be able to rationally respond to the risks.[281] The reasons may vary across age groups. Young children might be unable to predict the negative consequences of their conduct,[282] undermining any attempt to incentivize care through internalization of risk. Even when they can evaluate the risks, they might be unable to determine whether the likelihood of negative consequences makes their conduct morally undesirable and legally

277. Note that the incentive to take care is sharper under a negligence rule, because injurers can avoid liability entirely by choosing the proper level of care rather than only reduce its probability. Shavell, *supra* note 275, at 47.

278. Alan O. Sykes, *The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines*, 101 HARV. L. REV. 563 *passim* (1988) [hereinafter Sykes, *The Boundaries*]; Alan O. Sykes, *The Economics of Vicarious Liability*, 93 YALE L.J. 1231 *passim* (1984) [hereinafter Sykes, *The Economics*].

279. Sykes, *The Boundaries*, *supra* note 278, at 567–68.

280. *See* Areheart, *supra* note 43, at 42–43 (noting that most cyberbullies are judgment-proof); Walther, *supra* note 3, at 546 (same).

281. Areheart, *supra* note 43, at 43.

282. *See, e.g.*, Jodie M. Plumert & David C. Schwebel, *Social and Temperamental Influences on Children's Overestimation of Their Physical Abilities: Links to Accidental Injuries*, 67 J. EXPERIMENTAL CHILD PSYCHOL. 317, 318 (1997) ("[I]mmature cognitive skills such as errors in judging danger or the inability to foresee consequences may put children at risk for accidents.").

wrong;[283] and even if they fully realize the risks, and conclude that the risks make the conduct wrongful, civil liability might not be the sort of sanction that deters wrongdoing. Children would not be very impressed by a story about a judicial process in which they may be required to pay an amount of money they cannot predict and do not possess. Still, young children pose a lesser risk of cyberbullying. They are more closely supervised by adults, and less likely to have access to electronic means of communication and to use them to communicate with peers.

Adolescents raise a different and much greater problem, not only because they have access to electronic means of communication and intensively use them, but also because they are more inclined to irrationally take risks.[284] Research shows that by mid-adolescence, around the age of fifteen, individuals' cognitive capacity to make rational decisions, involving individual cost-benefit analysis, is similar to that of adults under neutral conditions.[285] However, under emotional stimuli, adolescents are more prone to acting irrationally, making emotion-based decisions with inadequate cognitive oversight, and ignoring risks that adults would take into account.[286] Adolescent risk-taking generally, and offensive conduct in particular, can be partly understood as arising from a "maturity gap" between cognitive and intellectual development on the one hand, and emotional and psychosocial development on the other.[287] Emotional and social deficiencies might overwhelm their capacity for rational choice and lead to reckless and potentially harmful conduct.[288]

Several phenomena contribute to this inclination to take risks. First, a substantial body of research demonstrates that adolescents are more sensitive to rewards, more inclined to reward-seeking than adults (and children), give more weight to rewards, particularly social rewards, and therefore discount risks in making choices.[289] Quick and considerable development of the neurobiological socioemotional system around the time of puberty leads to an increase in

---

283. *See, e.g.*, Nancy Eisenberg-Berg, *Development of Children's Prosocial Moral Judgment*, 15 DEVELOPMENTAL PSYCHOL. 128 (1979) (finding that elementary school children's reasoning "tended to be hedonistic, stereotyped, approval and interpersonally oriented, and/or involved the labeling of others' needs.").

284. *See, e.g.*, Brooke A. Ammerman et al., *Risk-Taking Behavior and Suicidality: The Unique Role of Adolescent Drug Use*, 47 J. CLINICAL CHILD & ADOLESCENT PSYCHOL. 131, 132 (2018) ("[I]t is generally agreed that adolescence is a developmental period marked by the emergence and escalation of risk-taking . . . and that these behaviors increase from early to late adolescence."); Natasha Duell et al., *Age Patterns in Risk Taking Across the World*, 47 J. YOUTH & ADOLESCENCE 1052, 1065 (2018) ("[A]dolescents demonstrate a heightened propensity, or inherent inclination, to take risks"); Laurence Steinberg, *A Social Neuroscience Perspective on Adolescent Risk-Taking*, 28 DEVELOPMENTAL REV. 78, 79 (2008) ("[A]dolescents engage in more risky behavior than adults.").

285. Elizabeth Scott et al., *Brain Development, Social Context, and Justice Policy*, 57 WASH. U. J.L. & POL'Y 13, 29, 32–33, 34–35, 37–38 (2018).

286. *Id.* at 30, 34–37.

287. *Id.* at 20.

288. *Id.* at 33.

289. *Id.* at 13, 15, 20, 21–23; Steinberg, *supra* note 284, at 83.

reward-seeking, which peaks at around fifteen, and then starts to decrease.[290] Consequently, adolescents are shortsighted: they seek immediate rewards and discount future consequences of their deeds.[291] Additionally, their sensitivity to rewards undermines their impulse control.[292]

Second, research shows that sensation seeking increases from childhood to adolescence, peaks in the late adolescence years, and subsequently decreases.[293] Sensation seeking is the attraction to varied, novel, complex, and intense experiences, and the readiness to "take physical, social, legal, and financial risks for the sake of such experiences."[294] Sensation-seeking individuals underestimate or accept risks, including legal and financial risks, as the price for the reward provided by the experience.[295] Adolescents, as sensation seekers, might overlook or undervalue risks and negative consequences of novel and thrilling activities, including various forms of bullying, thereby making irrational decisions.[296]

Third, adolescents are more impulsive.[297] The system of impulse control and emotional regulation develops gradually and slowly during adolescence and is not fully mature until the early to mid-twenties.[298] In adolescence, this system "can be overwhelmed by emotional and social responses, contributing to short-sighted choices" without forethought and consideration of long-term costs.[299] Adolescents might, therefore, act impulsively in the face of potentially harmful consequences and legal sanctions. The Supreme Court observed the limited deterrent effect of legal sanctions on teenagers in the context of capital punishment, holding that "[t]he likelihood that the teenage offender has made the kind of cost-benefit analysis that attaches any weight to the possibility of execution is so remote as to be virtually nonexistent."[300] In a subsequent case, the Court added that "[a] lack of maturity and an underdeveloped sense of responsibility are found in youth more often than in

290. Laurence Steinberg, *A Dual Systems Model of Adolescent Risk-Taking*, 52 DEVELOPMENTAL PSYCHOBIOLOGY 216, 216, 220 (2010).

291. Scott et al., *supra* note 285, at 21, 23–24 (2018).

292. *Id.* at 35.

293. K. Paige Harden et al., *Developmental Differences in Reward Sensitivity and Sensation Seeking in Adolescence: Testing Sex-Specific Associations with Gonadal Hormones and Pubertal Development*, 115 J. PERSONALITY & SOC. PSYCHOL. 161, 161–62 (2018); Scott et al., *supra* note 285, at 31.

294. MARVIN ZUCKERMAN, BEHAVIORAL EXPRESSIONS AND BIOSOCIAL BASES OF SENSATION SEEKING 27 (1994); Marvin Zuckerman, *Sensation Seeking*, *in* HANDBOOK OF INDIVIDUAL DIFFERENCES IN SOCIAL BEHAVIOR 455, 462 (Mark R. Leary & Rick H. Hoyle eds., 2009).

295. ZUCKERMAN, *supra* note 294, at 27.

296. *Id.*

297. For definitions of impulsivity, see F. Gerard Moeller et al., *Psychiatric Aspects of Impulsivity*, 158 AM. J. PSYCHIATRY 1783, 1783 (2001) (explaining that impulsivity is swift action without forethought and conscious judgement).

298. Scott et al., *supra* note 285, at 13, 16, 21, 26–28, 31; Steinberg, *supra* note 290, at 216, 220–21.

299. Scott et al., *supra* note 285, at 26, 50.

300. Thompson v. Oklahoma, 487 U.S. 815, 837 (1988).

adults and are more understandable among the young. These qualities often result in impetuous and ill-considered actions and decisions."[301]

Fourth, adolescents are more "sensitive to external social stimuli," particularly peer pressure.[302] "Recent research indicates that a network of brain systems governing thinking about social relationships undergoes significant changes in adolescence in ways that increase individuals' concern about the opinion of other[s]," mostly peers.[303] Susceptibility to peer pressure, especially pressure to engage in antisocial behavior, increases during early adolescence, peaks around age fourteen, and declines thereafter.[304] This susceptibility combines with adolescents' greater exposure to peer pressure. Adolescents spend more time with peers than children and adults, and use more intensive peer pressure to foster group solidarity and uniformity and to distinguish group members from nonmembers.[305] Peer pressure may encourage misconduct when the peers are also reward seeking, sensation seeking, and impulsive, as is the case with adolescents.

Even without any pressure, "the mere presence of peers activates the brain's reward [centers] to a much greater extent among adolescents," and increases their preference for immediate rewards, and inclination to take risks and behave in an antisocial manner.[306] In fact, even if peers are not present, adolescents' conduct is affected by anticipated peer response: they are more likely than adults to try impressing their peer group.[307] Peer pressure, presence, or even anticipated endorsement can overcome incentives (moral, monetary, or other) to avoid wrongdoing. Unsurprisingly, therefore, the riskiest "behavior in which adolescents engage, [including] delinquency, substance use, and reckless driving, takes place in the company of peers."[308] Peer impact was identified by the Supreme Court as one of the features undermining legal attempts to deter adolescent misconduct through legal sanctions and justifying a more lenient legal response to juvenile wrongdoing.[309]

---

301. Roper v. Simmons, 543 U.S. 551, 569 (2005) (quoting Johnson v. Texas, 509 U.S. 350, 367 (1993)).

302. Scott et al., *supra* note 285, at 13, 15–16, 20, 24–25.

303. *Id.* at 24; Laurence Steinberg & Kathryn C. Monahan, *Age Differences in Resistance to Peer Influence*, 43 DEVELOPMENTAL PSYCHOL. 1531, 1531 (2007) (observing that "there is little doubt that peers actually influence each other and that the effects of peer influence are stronger during adolescence than in adulthood").

304. Steinberg & Monahan, *supra* note 303, at 1531.

305. *Id.* at 1531.

306. Kaitlyn Breiner et al., *Combined Effects of Peer Presence, Social Cues, and Rewards on Cognitive Control in Adolescents*, 60 DEVELOPMENTAL PSYCHOBIOLOGY 292, 292 (2018) ("Adolescents showed diminished cognitive control to positive social cues when anticipating a reward in the presence of peers relative to when alone, a pattern not observed in older participants."); Scott et al., *supra* note 285, at 41–42, 43–44; Steinberg, *supra* note 284, at 85, 90–92 (explaining that peers make risky activities even more rewarding).

307. Scott et al., *supra* note 285, at 50–51.

308. Steinberg & Monahan, *supra* note 303, at 1531.

309. Roper v. Simmons, 543 U.S. 551, 569 (2005) ("[J]uveniles are more vulnerable or susceptible to negative influences and outside pressures, including peer pressure.").

4. Anonymity

As explained above, technology facilitates anonymous misconduct, and this is indeed very common among adolescents.[310] To bring an action against an anonymous wrongdoer, the victim needs to (1) obtain the perpetrator's IP address from the platform operator, and (2) obtain the wrongdoer's identity from the ISP, as identified by the IP address. As these two steps jeopardize both the anonymous user's freedom of speech and his or her right to privacy, the legal process is cautious and complex, hence very costly. Moreover, sophisticated users can hide their IP addresses.[311] Even when the real IP address used for wrongdoing can be ascertained, it may be very difficult to attribute the tort to a specific person if the tortfeasor was connected to a publicly accessible router[312] or—perhaps illegally—to another person's private router.[313] An action against the wrongdoer may also be impossible if neither the platform nor the ISP retains a log of users' activities for a long enough period (as actually occurred in *Zeran*).[314] Finally, a legal disclosure mechanism would often be restricted by territorial boundaries, enabling anonymous wrongdoers using foreign websites or foreign ISPs to get off scot-free. For example, the Supreme Court of Virginia examined the "territorial limits of [its] subpoena power."[315] It vacated a John Doe subpoena issued at the request of a Virginia carpet-cleaning business to a California-based business-rating website (Yelp), which published anonymous users' negative reviews of the plaintiff, because the statements were published outside its jurisdiction.[316] Had the defamatory statements been published in a different country, rather than a different state, the plaintiff would have faced even greater obstacles.

---

310. Areheart, *supra* note 43, at 41–42; Calvert, *supra* note 9, at 20; Grant, *supra* note 2, at 173–74, 198–99; Auerbach, *supra* note 2, at 1643–45; King, *supra* note 12, at 852; Poole, *supra* note 2, at 243, 259; Sumrall, *supra* note 2, at 1479–80.

311. *See supra* note 126.

312. This was one of the reasons for denying a John Doe a subpoena in the copyright infringement case of *VPR Internationale v. Does 1-1017*, No. 11-2068, 2011 U.S. Dist. LEXIS 64656, at *4 (C.D. Ill. Apr. 29, 2011) ("The list of IP addresses attached to VPR's complaint suggests . . . a similar disconnect between IP subscriber and copyright infringer. The ISPs include a number of universities, . . . as well as corporations and utility companies.").

313. *See, e.g.*, Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks*, NBC NEWS (Apr. 24, 2011, 5:52:36 PM), http://www.nbcnews.com/id/42740201/ [https://perma.cc/Z9TZ-28MH] (describing cases in which homeowners were accused of downloading child pornography but it later transpired that other parties had connected to the homeowners' wireless routers to commit the offenses).

314. Zeran v. Am. Online, Inc., 129 F.3d 327, 329 n.1 (4th Cir. 1997). The cost of information retention is correlated with the amount of daily traffic and the required duration of retention. More importantly, retention laws should not infringe basic rights. On April 8, 2014, the European Court of Justice held that the EU Data Retention Directive, Directive 2006/24/EC, which required telecom companies to store user data for up to two years, was invalid because it infringed on the right to privacy and the right to the protection of personal data. Case C-293/12, Dig. Rights Ir. Ltd. v. Minister for Commc'ns, Marine and Nat. Res., 2014 E.C.R. 238.

315. Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., 770 S.E.2d 440, 444 (Va. 2015).

316. *Id.* at 445–46.

If identification of a potential defendant is technically impossible, this party will not internalize the social costs of the undesirable conduct; the mere existence of a cause of action will not generate any deterrent effect.[317] If identification is possible, but its costs are prohibitively high, the victim might be deterred from bringing or continuing a valid lawsuit, undermining any deterrent effect of liability.[318] If the victim is capable of and willing to establish the wrongdoer's identity, the wrongdoer will internalize the costs of the wrongdoing, and efficient deterrence will be achieved (subject to the caveats concerning juvenile wrongdoers); but the administrative costs might outweigh the benefits in terms of cost-reducing deterrence, making the entire process inefficient.[319] Finally, even if identification costs are lower than the benefits in terms of deterrence, their magnitude might render another party (for example, a virtual supervisor) a more cost-effective target for enforcement efforts.

B. Real-Life Supervisors

1. The Economic Justification for Liability

The classical economic justification for supervisors' liability has two complementary components.[320] The first is the likelihood that the supervised would not be incentivized to avoid wrongful conduct by the prospect of liability, for example, because he or she is judgment-proof, or because of a limited cognitive, emotional, and social capacity. This component explains why primary wrongdoers' liability is insufficient. The second component is the supervisor's ability to take cost-effective measures to prevent wrongful conduct by the supervised. Supervisors can normally take two kinds of measures: (1) direct monitoring of the supervised, accompanied by reminders of the standard of conduct;[321] and (2) creating an incentive structure for proper conduct.[322] In the juvenile cyber-wrongdoing context, this may translate into educating children about the limits of cyber-activity, monitoring their activity, and implementing a reward-and-punishment system within the supervisor-child relationship. The important inquiry is always whether the cost of any measure is lower than the ensuing reduction in expected harm.

Two questions arise at this juncture. First, which of the child's real-life supervisors should bear the burden? Second, what kind of liability rule should be used? The first question requires identification of the cheapest cost avoider, namely the supervisor who can obtain the necessary information about the misconduct and take measures to prevent it at the lowest cost. Cheapest avoiders of real-world

317. Ronen Perry & Tal Z. Zarsky, *Who Should Be Liable for Online Anonymous Defamation?*, 82 U. CHI. L. REV. ONLINE 162, 167 (2015).

318. *Id.*

319. *Id.*

320. Sykes, *The Boundaries*, *supra* note 278, *passim*; Sykes, *The Economics*, *supra* note 278, *passim.*

321. Sykes, *The Boundaries*, *supra* note 278, at 569 (discussing employers' liability).

322. *Id.* at 570 (discussing employers' liability).

misconduct of others would normally be identified on the basis of temporal and spatial proximity. Schools were best situated to respond to children's wrongdoing during schooltime, and parents (or caregivers) were the least cost avoiders at other times. Technology has somewhat changed this reality, as parents may be the only supervisors with access to electronic equipment used by their children. For example, if students harass their peer using instant messaging applications on their mobile phones, the school's access to the content may be strictly limited. The proposed liability model assumes that control over the electronic equipment used by the wrongdoer is a key factor. This point will be elaborated below.[323]

As regards the preferable rule, the starting point is that both strict-vicarious and negligence-based liability can incentivize supervisors to take risk-reducing measures when their cost is lower than the expected harm they can prevent.[324] Law and economics literature provides some guidelines for choosing between the two. A negligence-based regime has an advantage where the supervisor could not have reasonably done anything to prevent the child's wrongdoing, because imposition of liability in such circumstances (required under a strict liability rule) has no benefit from a deterrence perspective and generates considerable administrative costs.[325] Negligence-based liability does not have a similar weakness, because unavailability of reasonable precautions entails no liability. Admittedly, substantiating negligence is a costly process, and factual and legal uncertainties might result in over-deterrence and redundant, costly litigation. Yet litigation with no benefit in terms of deterrence is less likely under a negligence rule. Strict-vicarious liability may have an advantage over a negligent-supervision rule in terms of deterrence when "there is a significant risk of under-detection of the failures of the [supervisor's] preventive measures."[326]

2. Power Without Information

Reasonably educating children not to abuse technology to harm others, and responding decisively when cases of cyber-wrongdoing are detected, should not be very costly for real-life supervisors. But while these measures may somewhat reduce the risk of cyber-wrongdoing, they are inadequate. The main problem here is that real-life supervisors, especially parents, have considerable power to affect the conduct of supervised children, but lack the information necessary for exercising such control. There are several reasons for this.

First, supervisors of a school-age child cannot be reasonably expected to monitor in real time every deed and every word of that child. Such monitoring would disrupt other activities that supervisors carry out. Constant real-time monitoring may be cost-justified where the supervised poses a significant risk to

323. *See infra* Section II.D.3.

324. Strict liability also induces efficient activity levels, whereas a classical negligence rule does not.

325. Catherine M. Sharkey, *Institutional Liability for Employees' Intentional Torts: Vicarious Liability as a Quasi-Substitute for Punitive Damages*, 53 VAL. U. L. REV. 1, 4 (2019).

326. *Id.* at 5.

himself or herself (as in the case of toddlers) or to others (as in the case of inmates), but seems excessive and unrealistic in the case of school-age children. Thus, parents and school personnel rarely witness children's cyber-activity as it unfolds and cannot immediately respond to misconduct. Second, whether we consider constant real-time monitoring or mere periodic review of the child's cyber-activity, detecting misconduct entails examination of stacks of content, taking different forms (text, pictures, videos, etc.), continuously created on various platforms, not only by the specific child, but also by multiple correspondents. Supervisors usually have work, household commitments, and leisure activities, which limit the time and energy they can dedicate to such examination. The cost of performing this task would be prohibitively high. Third, even if a supervisor could reasonably review all cyber-communications, the content would often be unintelligible due to the use of adolescent cyber-slang or group-speak, an esoteric subtext, or an unknown real-life background. Adult supervisors lack the expertise to readily understand children's social interaction in the digital realm when revealed to them. Fourth, the supervisor's ability to monitor the child's cyber-activity may be subject to privacy-related constraints. Under privacy law, school employees have limited access to students' cyber-communications. Parents, who do have access, may be justifiably hesitant to invade children's privacy. Psychologists advocate authoritative parenting, which "involves active engagement with the teenager's life but not excessive monitoring, which [can either] generate intense opposition or inhibit development of the [teen's] ability to make autonomous choices."[327] Fifth, adolescents can conceal some of their cyber-activity, for example, by deleting conversations or application logs, using password protected websites, or operating fake profiles. Finally, the burden of obtaining information may be exacerbated when the supervisor is simultaneously responsible for more than one person. Parents may have more than one child, and schools have hundreds of students. In conclusion, monitoring is very costly in the absence of a concrete substantiated complaint about a specific child's misbehavior.

High information costs may have undesirable outcomes. If supervisors cannot practically become aware of the child's wrongdoing, they will not know when they need to react. Imposing liability will not incentivize them to take any measures to prevent or stop the wrongdoing. In such a case, a claim against the supervisor will have a high administrative cost with no benefit in terms of harm prevention. If obtaining information is possible, but its cost exceeds the supervisor's expected liability, the supervisor will choose not to obtain the necessary information, without which he or she cannot and will not respond to the child's (unknown) wrongdoing. Again, liability will have a high administrative cost and no benefit in terms of harm prevention. If information costs plus the costs of harm prevention measures are lower than expected liability, imposing liability will induce economically justified action by the supervisor. Yet it might not be efficient overall if the net social benefit

327. Scott et al., *supra* note 285, at 38–39.

of the supervisor's prevention efforts, namely expected harm minus the cost of the measures taken, including the high information cost, is lower than the administrative cost of the claim.

3. Anonymity

Courts cannot impose liability on an unidentified party, and if the juvenile cyber-wrongdoer is anonymous, his or her real-life supervisors will also be unknown. The high cost of identifying an anonymous wrongdoer is a problem that imposing liability on a real-life supervisor cannot solve, because the cost of identifying the supervisor may be just as high. Admittedly, imposing liability on a supervisor entails identification of the supervisor, not the specific wrongdoer. An identified supervisor can be found liable for allowing cyber-wrongdoing by an unidentified child using the supervisor's equipment, such as a school computer or router. Still, the wrongdoer's anonymity will normally mask the supervisor's identity, so imposing liability on either will require a costly unmasking process. To bring an action against an anonymous wrongdoer's supervisor, the victim must obtain the wrongdoer's IP address from the platform operator and then obtain the wrongdoer's or the supervisor's identity from the ISP.[328] This is a costly process. Most tactics used by the tortfeasor to conceal his or her identity, apart from using the supervisor's multiuser computer or router to anonymously connect to the Internet, will further hinder the supervisor's identification.[329] Service providers' data retention limits are another hurdle.[330]

If supervisors have reason to believe that their identification is technically impossible, they will not be incentivized to take cost-effective measures to prevent cyber-wrongdoing. If identification is possible, but its costs are very high, victims might be deterred from bringing or continuing valid lawsuits, and supervisors will not internalize the harm.[331] If the victim can easily establish the wrongdoer's identity, the wrongdoer or the supervisor will internalize the costs of the wrongdoing, and efficient deterrence will be achieved; but the administrative costs might outweigh the benefits in terms of cost-reducing deterrence, making the entire process inefficient. Finally, even if identification costs are lower than the benefits in terms of deterrence, their magnitude might render another party (for example, a virtual supervisor) a more cost-effective target for enforcement efforts.

328. *See supra* Section II.A.4.

329. *Id.*

330. *Id.*

331. The impact is related to supervisors' perception of the likelihood that supervised children mask their identities when harming others.

C. Virtual Supervisors

1. The Economic Justification for Liability

Imposing liability on juvenile cyber-wrongdoers might not provide efficient deterrence at a reasonable administrative cost. Minors' inability to compensate their victims, grasp the wrongfulness of their conduct, and rationally respond to the prospect of liability, and the high cost of identifying anonymous wrongdoers, prevent internalization of the social costs of wrongdoing or make efficient deterrence wasteful due to the administrative cost. Imposing liability on real-life supervisors can help control juvenile misconduct but might involve high information costs and is also hampered by anonymity. Under these circumstances, virtual supervisors' liability should be considered.

Imposing liability on virtual supervisors can incentivize them to take the necessary precautions to prevent cyber-wrongdoing. The benefits are clear. First, virtual supervisors are less likely to be judgment-proof or lack the cognitive, emotional, and social skills to understand the potential impact of the conduct and its legal consequences. Second, when the wrongdoer and the real life-supervisor are anonymous, the administrative cost of litigating a case against them might be significantly higher than that of pursuing an action against a virtual supervisor. Third, parties who are jointly liable for a particular harm have an interest in reducing their own shares of the burden. Because any difficulty in identifying and suing the wrongdoer or the real-life supervisor will result in greater expected liability for the virtual supervisor, the latter has an incentive to facilitate the identification of anonymous wrongdoers and their real-life supervisors. To do so, virtual supervisors may take various measures, such as preventing contributions by unidentified users, collecting and retaining user information, and volunteering this information in the case of a lawsuit (subject to applicable law).[332]

2. Inefficiencies of Liability

Imposing liability on virtual supervisors has its weaknesses. First and foremost, the cost of precautions available to platform operators may be high. The strictest supervision model is specific monitoring. Human monitoring of user-generated content entails hiring and training staff to review such content and distinguish between lawful and unlawful content. The cost per item is not trivial, and it is incurred with respect to all user-generated content—as opposed to the administrative cost of an action against the wrongdoer or a real-life supervisor (including identification costs, where applicable), which is incurred only in the rare case of a legal complaint about a specific wrongful contribution. "Automated monitoring requires the development and implementation of technologies that

332. Virtual supervisors might not be very keen to drag their users into court because this may harm their business. But the ability to share the burden will surely result in some increase in the likelihood of data collection.

preclude [wrongful contributions] while allowing legitimate speech. Once the mechanism has been developed, it can be implemented at a very low marginal cost."[333] However, the costs of continued development of the necessary tools cannot be ignored. Moreover, "automated systems are still expected to make more judgment mistakes than trained humans, and human correction mechanisms [may be] costly."[334]

An alternative supervision model is the "notice-and-takedown" procedure, whereby platform operators remove user-generated content when notified that this content is suspected of being wrongful.[335] They can either allow the publisher of removed content to contest the removal, and individually investigate wrongful-removal complaints, or automatically restore the content upon the publisher's assumption of full legal responsibility for the publication. The main advantage of this method is that it significantly reduces monitoring costs. But an automatic notice-and-takedown system enables anyone with the desire to silence another's speech to do so easily and to engage in mass censorship,[336] whereas integrating human discretion would turn it into a costly selective-monitoring system.[337]

If supervision costs exceed its benefits in terms of preventing harmful conduct, virtual supervisors' liability will not incentivize supervisors to take measures to prevent wrongful user conduct. Under a negligence-based rule, supervisors will not be liable at all for failing to take the supervisory measures; and under a strict-liability regime, they will prefer bearing liability to taking such measures. Either way, virtual supervisors' liability will not prevent cyber-wrongdoing. Even if harm-prevention benefits exceed supervision costs, the net benefit may be too low to justify the administrative cost of a liability rule. Virtual supervisors might also try to save on monitoring costs without being exposed to liability through extreme and socially undesirable measures—from an immoderate takedown policy to prevention of user contribution. These steps would inhibit information flow, progress, and innovation.

Second, most user-generated content is legitimate and socially beneficial. Users "create positive externalities enjoyed by advertisers, information providers, merchants, friends, and acquaintances."[338] Yet intermediary liability makes platform operators internalize the expected harms caused by relatively rare wrongful

333. Perry & Zarsky, *supra* note 317, at 168.

334. *Id.*

335. *See supra* notes 268–70 and accompanying text.

336. Cecilia Ziniti, Note, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 606 (2008). By analogy, "empirical evidence indicates that more than a quarter of [Digital Millennium Copyright Act] takedown notices are either on shaky legal grounds or address cases in which no copyrights are violated." *Id.* at 605.

337. Perry & Zarsky, *supra* note 317, at 169.

338. Lichtman & Posner, *supra* note 126, at 225.

user-contributions, without capturing the full social benefits of their activities.[339] This may result in over-deterrence in the form of excessive monitoring and overzealous censorship by platform operators.[340]

Third, even if virtual supervisors choose the proper level of care, uncertainties may arise with respect to the wrongful nature of each contribution. These uncertainties force virtual supervisors to choose between two types of potential errors: (1) false negatives, namely, mistaking unlawful publication for lawful; and (2) false positives, namely, mistaking lawful publications for unlawful.[341] A false negative carries the risks of litigation and liability, whereas a false positive does not. Acting on a false positive does not seem to have a real cost at all, as removal is almost costless. This imbalance induces virtual supervisors to remove suspicious yet lawful speech: to avoid liability, companies would rather err on the side of caution, and silence speech.[342] "In addition, they may be induced to block provocative users, disable user contributions, or reduce demand for Web 2.0 technologies, thus impeding progress and innovation."[343]

Note further that concurrent liability of the wrongdoer, a real-life supervisor, and a virtual supervisor, as European Union law currently permits, has two additional disadvantages. First, to the extent that several parties are at risk of being liable and that each has a somewhat different perception of what constitutes wrongdoing, imposing liability on all may restrict freedom of speech more than singling out one defendant.[344] Second, a combination of wrongdoers', real-life supervisors', and virtual supervisors' liability may result in an aggregation of the implementation costs of all. Virtual supervisors will be led to monitoring user-generated content at a high cost that could be saved under an exclusive real-life supervisors' liability regime. At the same time, lawsuits will still be brought against anonymous wrongdoers and real-life supervisors at high administrative costs that could be saved under an effective virtual supervisors' liability regime.

---

339. Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 917–18, 921 (2002).

340. *Id.* at 917–18. *See also* Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1, 13 n.30 (2003) ("ISPs do not fully share the benefits its subscribers derive from placing material . . . on the network. As a result, imposing liability on ISPs for subscribers' infringing material induces ISPs to overdeter, purging any material that a copyright holder claims is infringing.").

341. Perry & Zarsky, *supra* note 317, at 169.

342. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) ("Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not . . . . Thus, [indirect liability] . . . has a chilling effect on the freedom of Internet speech.").

343. Perry & Zarsky, *supra* note 317, at 170.

344. The set of statements considered defamatory by either party is the union of the set of statements considered defamatory by the speaker and the set of statements considered so by the virtual supervisor, which is equivalent to or larger than each set individually.

3. Information Without Power

An additional set of problems with virtual supervisors' liability is a mirror image of one of the apparent problems with real-life supervisors' liability. Real-life supervisors have the skills and ability to affect the child's conduct but lack the information necessary for exercising such control. In contrast, virtual supervisors may have very easy access to the harmful content, which is necessary for preventing juvenile wrongdoing, but lack the skills and ability to affect the juvenile's conduct. Regarding skills, although platforms can use algorithms to identify potentially harmful statements—the costs of deciding whether these statements are actually wrongful may be much higher for them than they are for real-life supervisors. The puerile and often naive nature of juvenile communications, the intricacies and nuances of specific social interactions and their real-life background, the inability to discuss content with the child, and the extent of content going through the platform make virtual supervision inaccurate, with a systematic bias in favor of false positive findings of wrongfulness. Imposing liability, either under a full-monitoring theory or a notice-and-takedown model, may result in a severe chilling effect.

As regards ability, three concerns arise. First, each platform has access to contributions made on its own service. It is incapable of monitoring the user's activity on other platforms and in real life or evaluating the cumulative effect of the user's contributions and actions on the victim. Second, each platform can respond to wrongdoing only by restricting the use of its own service. It can prevent, through screening algorithms, certain kinds of expression, remove tortious material (based on monitoring or notification), warn users, and even suspend or terminate recidivists' accounts, but they cannot do much more than that. Virtual supervisors, as opposed to real-life supervisors, have no control over the wrongdoer's actions in other venues. For example, a social networking platform can remove harmful content but has nothing to do against recirculation of the same content through e-mail. Third, a virtual supervisor cannot educate or discipline children and adolescents, thereby reducing the risk of cyber-harassment in general and the risk of continued harassment of the specific victim in particular.

D. A Proposed Model for Juvenile Cyber-Wrongdoing

1. Primary Liability Not Useful but Not Barred

The preceding analysis has shown that imposing liability on a juvenile wrongdoer does not provide the required incentives for harm prevention, because of minors' inability to compensate victims, their limited cognitive, emotional, and social capacity, and the frequent use of anonymity. Children and adolescents can be incentivized to act properly, but not through civil liability. Supervising and responding to their conduct is clearly a more effective method for preventing harm. Supervisors' liability (direct negligence-based or strict-vicarious) can incentivize supervisors to take cost-effective measures, and one needs to determine which supervisor is best equipped to bear this burden.

Although primary wrongdoers' liability is economically insufficient, it should not be barred. First, if the perpetrator is incapable of compensating, comprehending the wrongfulness of the conduct, or rationally responding to the risks, the victim will not have an incentive to bring an action anyway. With no prospect of recovery, either because the defendant is judgment-proof or because of the difficulties in establishing fault, initiating litigation seems pointless. The ability to pursue a claim against the primary wrongdoer should be maintained for the rare cases in which suing is economically reasonable. Inviting courts to decide on a case-by-case basis if pursuing the claim is economically reasonable would involve high administrative costs and not provide much greater accuracy than simply relying on victims' common sense. Second, in some jurisdictions and circumstances, bringing an action against the juvenile wrongdoer along with a claim against the supervisor may enable or reduce the costs of administering the latter. For example, if parents' liability is vicarious, an action against the child (in addition to a lawsuit against the parents) may help establish the wrong for which vicarious liability can be imposed. Similarly, if the wrongdoer is anonymous, imposing liability on the real-life supervisor would often entail identification of the primary wrongdoer, and this will depend on the existence of a *prima facie* cause of action against him or her.[345]

2. Reducing Information Costs: Basic Models

The cornerstone of the proposed models is a comparison between real-life and virtual supervisors. While real-life supervisors' liability can generate the required incentives to prevent harmful conduct, it raises several questions and concerns. To begin with, liability must be imposed on the least cost avoider. In the information age, the choice no longer hinges on time and space. Thus, for example, parents who buy mobile phones for their children may be better equipped to supervise and respond to the children's cyber-activity even during schooltime and on school premises. More importantly, while real-life supervisors have the ability to educate and discipline, and even stop concrete incidents of cyberbullying, they do not have the capacity to monitor children in real time, to overcome children's concealment efforts, to cope with the amounts of content produced, and to effortlessly understand it, and may be further limited by privacy-related constraints. In addition, if a child commits a wrong anonymously, it will be equally difficult to identify the real-life supervisor.

Imposing liability on virtual supervisors can generate incentives to prevent cyber-wrongdoing when primary wrongdoers' liability fails and save identification costs in cases of anonymous wrongdoing. However, the cost of accurate supervision is very high; liability for the negative externalities of operating a platform with no reward for the positive externalities of such operation generates over-deterrence; and the asymmetry between the legal outcomes of false negative determinations of wrongfulness (liability) and false positives (no-liability) encourages silencing in cases

345. *See supra* notes 128–29 and accompanying text.

of uncertainty. Moreover, virtual supervisors may have easy access to the harmful content, which is necessary for preventing the child's wrongdoing, but lack the skills and ability to affect the child's conduct. They cannot easily determine whether the publication of a certain item is wrongful (increasing the risk of a chilling effect); they cannot get the full picture of the juvenile interaction, respond beyond the confines of the specific platform, and educate or discipline children.

At this stage, let us make two simplifying assumptions, which will be relaxed in subsequent sections. First, assume that there is only one category of real-life supervisors, namely parents. Second, assume that the wrongdoer is readily identifiable. The comparison can now be restated thus: real-life supervisors may acquire a fuller picture of the interaction and respond in numerous ways to curtail cyberbullying; but they do not have the capacity to monitor children in real time, to cope with the amounts of content produced, and to overcome concealment efforts, and may be further limited by privacy-related constraints. In contrast, virtual supervisors have easy access to content generated through their own services but lack the ability to effectively prevent or curtail juvenile misconduct. Even if virtual supervisors had full access to users' cyber-activity, an unlikely scenario from economic and privacy law perspectives, they would be unable to effectively control cyberbullying. If parents had quick and inexpensive access to a roughly accurate risk analysis of their children's cyber-activity, they would not only be cheaper cost avoiders than any virtual supervisor, but also cost-effective risk avoiders. This outcome can be pursued in at least two ways.

The first model is algorithmic data collection and analysis by virtual supervisors and automatic transfers of information about suspected wrongdoing to users' parents. Two questions arise at this point: Is this model feasible, and how can liability rules secure the proper incentives? As regards feasibility, the answer lies in the technological realm. Each operator of a platform that might be used by children and adolescents for cyber-wrongdoing can enable designated adults (usually users' parents) to receive notifications about suspected abuse. This may require registration, possibly password protected, from within each application used by a child. Once the parent registers, he or she can be notified about any algorithmically identified suspicion at a negligible cost. Platform operators would only need to implement reasonable screening algorithms, as many already do, and leave any decision regarding the wrongfulness of the conduct and the proper response to parents, reducing the risk of an industry chilling effect. Presumably, with time, operating systems installed on devices used by children will further facilitate the transfer of information by enabling parents to provide their contact information once, to be shared with all or specifically selected applications.

As regards liability rules, the law first needs to incentivize virtual supervisors to create a notification system, to collect and analyze relevant information, and to send notifications when appropriate. A platform operator should thus be held liable if it does not establish a notification system, does not apply a reasonable monitoring algorithm, or does not alert the designated adult when the algorithm identifies a

suspicion. The law also needs to incentivize the parent to verify that all applications used by the child on a smartphone, a tablet, a laptop, or a desktop designate the parent as the person to be notified in case of abuse. A parent should be held liable for cyber-wrongdoing by his or her child when the parent did not opt-in to the notification service of the application used for the particular wrongdoing or failed to take reasonable measures to address suspected misconduct when notified. If parents are liable for failing to opt in, operating system developers will be incentivized to provide a tool for reducing the hassle and risk of parental default to make their product attractive for customers. The development of an operating system feature, enabling parents to provide their contact information only once, will probably occur without further legal intervention.

The main problem with the first model is that it is platform specific. Parents would be unable to monitor activity on applications used only on devices beyond their control, such as school desktop computers. More importantly, while parents will be alerted about their children's abuse of native applications, such as Facebook or WhatsApp, they would have no control over cyber-wrongdoing through web applications, such as posts and comments on blogs and online forums,[346] online reader responses, or webmail. A related but easily soluble problem is that parents would be unable to supervise the child's activity on a specific platform before realizing that the child is actually using it and requesting notification of abuse, especially if the child removes the application or closes the browser window immediately after the abuse. The operating system feature described above can solve this problem by automatically linking any new application to the parents' contact information. Lastly, platform-specific models might be deficient to the extent that platform operators have no presence in the relevant jurisdiction. If liability is practically unenforceable, it has no deterrent effect.

The second model hinges on the use of data collection and analysis tools by the parents to reduce their own information costs. The same two questions arise: Is this model feasible, and how can liability rules secure the proper incentives? Parental cyber-surveillance tools are already available. Parents can obtain full access to the child's browser history, e-mails, social networking activity, instant messaging, text messaging, and the like, through special surveillance applications and services, such as Monqi, mSpy, Spyzie, and TeenSafe. Surveillance tools seemingly suffer from two major weaknesses. First, although they provide access to information, parents still need to review a large quantity of content, taking different forms, continuously created on various platforms, not only by the specific child but also by his or her peers. Parents do not have the time and energy to carry out this task. Second, many parents would not want to so blatantly invade their child's privacy and so strictly limit his or her autonomy. Presumably, these two problems can be solved with algorithmic data collection and analysis. Instead of perusing all content,

346. As in the case of D.C. v. R.R., 106 Cal. Rptr. 3d 399, *rev. denied*, No. S181558, 2010 Cal. LEXIS 6052 (June 17, 2010).

which is both impractical and disrespectful of the child's privacy, parents would seek to rely on algorithmic tools, which would analyze all data and inform them of dubious activity that requires additional scrutiny. Surveillance applications already offer keyword and illicit content alerts, and application vendors can gradually develop and offer more complex data analysis and notification features. Replacing full human monitoring with algorithmic data collection and analysis tools will reduce parents' information costs and parent-child friction over infringement of privacy. This is also preferable to notifications following data collection and analysis by individual platforms, which only access fragments of the full picture. Of course, if parents use these tools, there is no need for direct communication between platforms and parents with respect to possible abuse of these platforms on monitored devices.

Parents may have a sufficiently strong incentive to use advanced surveillance applications to protect their own children. Many parents already do, and this is encouraged by experts in various disciplines.[347] In theory, legal incentives to acquire and employ these tools may be redundant. However, given the cost of using these applications, which may include a nontrivial price tag as well as parental time and energy, parents' overconfidence in their children's virtue, and the common reluctance to constrain privacy, internalization of the expected costs to others of the child's activity may be necessary. To incentivize parents to reasonably use advanced surveillance applications, the law should impose liability when failure to employ such tools results in juvenile cyber-wrongdoing, in addition to standard liability for not taking reasonable precautions upon learning about the risk. The remaining question is what would incentivize vendors to develop and offer advanced data collection and analysis features. If parents could be held liable for failing to efficiently monitor their children's cyber-activity, they would be willing to pay a certain premium for features that ease detection of cyber-wrongdoing, thereby reducing the cost of monitoring and the risk of liability. Parents' willingness to pay will create incentives for competing application vendors.

The main problem with the second model is that it is device specific. While parents will obtain information about their children's abuse of a specific device under surveillance, they will have no control over cyber-activity on other devices, such as school or library computers. The likelihood of ongoing abuse through devices that the parents cannot access is not very high, but this possibility should not be ignored. The next Section will address this concern. Furthermore, using

347. *See, e.g.*, Meltem Dinleyci et al., *Media Use by Children, and Parents' Views on Children's Media Usage*, 5 INTERACTIVE J. MED. RES. e18 (2016) ("Encouraging parents to monitor children's media carefully can have a wide range of health benefits for children."); Douglas A. Gentile et al., *Protective Effects of Parental Monitoring of Children's Media Use: A Prospective Study*, 168 JAMA PEDIATRICS 479, 480 (2014) ("Many negative effects of both the amount and content of media may be mitigated by parental monitoring of children's media use."); Dick Uliano, *Police: Parents Need to Monitor Kids' Cellphone Use*, WTOP (Nov. 21, 2017, 8:09 PM), https://wtop.com/local/2017/11/police-parents-need-monitor-kids-cellphone-use/ [https://perma.cc/X6UU-LK99].

advanced surveillance applications currently involves a real outlay for the parents (in the form of monthly service fees), as opposed to the first model which has no direct monetary cost for them. Holding parents negligent for failing to take the more costly measure may not be defensible given its limited and speculative marginal benefit: the added ability to oversee the use of web applications on parent-controlled devices minus the lost ability to oversee the use of supervised applications on third-party devices.[348]

	Device under parents' control	Device not under parents' control
Apps under parents' control	Model 1, Model 2	Model 1
Apps not under parents' control	Model 2	Neither

Table 1. Coverage by Proposed Models

3. Relaxing the First Assumption

The previous Section made two simplifying assumptions: (1) there is only one category of real-life supervisors, and (2) the wrongdoer is readily identifiable. These assumptions will now be relaxed in turn. The first inquiry, then, is how the preceding analysis must change if there is more than one category of real-life supervisors, for example, parents and school personnel. The first model proposed for reducing the cost of monitoring children's cyber-activity is platform specific. It will keep parents informed about their children's activity on some applications regardless of time and space constraints. The parent will receive notifications of abuse through various platforms, even if the child accesses these platforms on devices beyond the parent's reach. However, parents will not obtain information about cyber-wrongdoing through unsupervised communication methods, such as webmail, or any communication method used solely on devices beyond their reach. If this model is adopted, the legal system must incentivize those who can acquire such information to do so and respond reasonably.

Regardless of the specific technological tool used to reduce data collection and analysis costs, any institution allowing many children to access cyberspace through its electronic equipment must require individual identification. In the case of cyber-wrongdoing, the source of the content will be detectable. If the institution fails to enforce individual identification, it must be held liable for any cyber-wrongdoing perpetrated by unidentified users through its equipment.

Now, reducing information costs concerning cyber-activity beyond the parents' control may take several forms. To begin with, a school representative can serve as the designated adult for receiving notifications about students' abuse of

348. From an aggregate welfare perspective, developing platform-specific data collection and analysis tools may be more costly than developing advanced parental surveillance tools. Nevertheless, platform operators may ultimately use less costly off-the-shelf software and services based on the same technologies used by parental surveillance applications.

applications on school computers, unless parents have already assumed this role for the specific applications. Upon notification, the school can endeavor to stop the wrongdoing, *inter alia*, by informing the wrongdoer's parents. In addition to incentivizing virtual supervisors to establish algorithmic data analysis and notification systems, as explained above,[349] the law will need to incentivize schools to obtain the necessary information from platforms used on school devices. They should be held liable for cyber-wrongdoing by students if they did not opt in to the notification service of the abused application (unless the parents are already the designated adults) or failed to take reasonable measures to address suspected wrongdoing when notified. This combination of platform-specific data analysis and notification systems will cover any abuse of native applications. Nonetheless, it has two weaknesses. First, it keeps all activity through web applications covert. Second, granting schools access to students' cyber-activity outside of school is legally problematic.[350]

Alternatively, owners or operators of devices accessible by children can be incentivized to employ user-specific surveillance tools, such as Securly, by holding them liable for any cyber-wrongdoing resulting from failing to do so. They should also be liable if the surveillance application notified them of possible wrongdoing, and they failed to take reasonable measures to prevent harm.[351] Informing the parents, who may have a fuller knowledge and understanding of the situation, and obtaining their feedback, is a necessary step in devising the proper response. While schools may be constrained in searching students' personal devices, there does not seem to be a substantive legal obstacle to monitoring school devices.[352] The problems with this model are that it does not cover abuse of web applications on parent-controlled devices and involves wasteful double scrutiny of cyber-activity on school devices through parentally-monitored applications.

The second model proposed for reducing the cost of parental monitoring of children's cyber-activity is device specific. Parents using surveillance applications gain access to the child's cyber-activity only through devices under the parents' control. Parents are unable to monitor any activity on "external" devices, even if the child uses platforms that are also installed on devices with parental surveillance. Requiring owners or operators of devices accessible by children to request user identification and employ user-specific surveillance tools may solve the problem. If the surveillance application notifies the device owner of a potential misdeed, the owner can immediately respond. Frequently, informing the child's parents may be

349. *See supra* Section II.D.2.

350. *See supra* notes 225–29 and accompanying text.

351. Theoretically, schools can prohibit or block any use of potentially harmful applications on school computers. This will protect the school from liability for students' abuse of its equipment, but cannot be legally required. It is unjustified economically and pedagogically but within school prerogative.

352. *See* Emily F. Suski, *Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority Under Cyberbullying Laws*, 65 CASE W. RES. L. REV. 63, 70–87, 119 (2014) (discussing the different levels of school surveillance authority).

a reasonable response. The parents, after receiving all relevant information, are expected to take reasonable measures to prevent harm. This combination of device-specific data collection and analysis tools is the most comprehensive method for reducing information costs, as it covers all applications on all devices. Channeling all information to the parents enables the least cost avoiders to assess the risks and take cost-effective measures to reduce them.

	Device under parents' control	Device not under parents' control
Apps under parents' control	Model 1, Model 2	Model 1, School monitoring
Apps not under parents' control	Model 2	School monitoring

Table 2. Coverage with More Than One Supervisor

4. Relaxing the Second Assumption

An additional complication arises in the case of anonymous cyber-wrongdoing. Courts cannot impose liability on an unidentified party, and if the juvenile cyber-wrongdoer is anonymous, his or her real-life supervisors will usually be unknown. One option is to foreclose virtual supervisors' liability but enable courts to order cyber service providers to disclose information about anonymous wrongdoers and their real-life supervisors (the American model).[353] Yet the costs of identifying an anonymous wrongdoer might be prohibitively high, and imposing liability on real-life supervisors would not normally reduce these costs.[354] A second option is to impose strict or negligence-based liability on virtual supervisors for abuse of their platforms while preventing identification of anonymous users (the Israeli model).[355] This saves identification costs when the wrongdoer is anonymous but entails high monitoring and error costs as discussed above.[356] A third option is to simultaneously enable identification of anonymous wrongdoers and recognize virtual supervisors' liability (the European model).[357] However, to the extent that two or more parties may be liable and that each has a different perception of what constitutes wrongdoing, imposing liability on all may restrict freedom of speech more than singling out one defendant.[358] Moreover, concurrent liability of real-life and virtual supervisors may result in an aggregation of the implementation costs of the two regimes. Virtual supervisors will be led to monitor user-generated content at a high cost that could be saved under an exclusive real-life supervisors' liability regime. At the same time, lawsuits will be brought

353. Perry & Zarsky, *supra* note 317, at 163–65, 175.
354. *See supra* Sections II.A.4, II.B.3.
355. Perry & Zarsky, *supra* note 317, at 167–68, 175.
356. *See supra* Section II.C.2.
357. Perry & Zarsky, *supra* note 317, at 170–71, 175.
358. *See supra* note 346.

against anonymous wrongdoers and real-life supervisors at high administrative costs that could be saved under an effective virtual supervisors' liability regime.

The fourth option is the most efficient adjustment to the basic liability model: it minimizes identification costs and facilitates parental liability while saving virtual supervisors' monitoring and error costs. This adjustment is based on the English defamation model, whereby the cyber-wrongdoer is exclusively liable, but if he or she is not reasonably reachable, the platform operator may become liable. The virtual supervisor is liable if the victim has insufficient information to identify the wrongdoer, the victim gave notice of the complaint, and the virtual supervisor did not properly respond.[359] A proper response requires obtaining the wrongdoer's contact information and providing it to the victim or removing the wrongful content.[360] Under this "residual liability" regime, virtual supervisors can avoid liability and monitoring altogether by (1) obtaining user identification data, at least when a content analysis algorithm identifies suspected cyber-wrongdoing, or (2) removing content generated by unreachable users on notification of its harmful potential. This will save all monitoring costs and prevent over-deterrence caused by non-internalization of the economic benefits of Web 2.0 technologies and by the asymmetric legal response to judgment errors. Additionally, by incentivizing virtual supervisors to take measures to reduce the cost of identifying anonymous wrongdoers, this method will facilitate parental liability which induces efficient parental supervision. Theoretically, if virtual supervisors under a residual liability regime allow postings by unreachable wrongdoers, they might still need to monitor to avoid liability. Even so, monitoring will be limited to content generated by unidentifiable users, so the cost will be much lower than in the case of liability for any abuse. Presumably, virtual supervisors will allow anonymous contributions only if the benefit (for instance, increasing traffic) exceeds the costs.

CONCLUSION

Cyberbullying has become a notorious epidemic, culminating in widely publicized suicides.[361] Whether a new and distinct problem or an old one in a new guise,[362] the technological setting has undoubtedly generated new challenges and, at the same time, new opportunities for legal response. This Article provides systematic legal and economic analyses of an underexplored regulatory tool: civil liability. The analysis on both levels is based on a trichotomy of potential defendants—primary wrongdoers, real-life supervisors, and virtual supervisors.

Part I discussed applicable law with a comparative touch. Section A examined common law causes of action that can be used in lawsuits against primary

359. Defamation Act 2013, c. 26, § 5(3)–(4) (U.K.).

360. *Id.* § 5(3)(c), (5).

361. *See supra* notes 1–2 and accompanying text.

362. *See* Dieter Wolke et al., *Cyberbullying: A Storm in a Teacup?*, 26 EUR. CHILD & ADOLESCENT PSYCHIATRY 899 (2017) (finding that cyberbullying neither increases the number of bullying victims significantly nor exacerbates the psychological and psychosocial impact of bullying).

wrongdoers, including an independent tort of cyberbullying, defamation, invasion of privacy, intentional and negligent infliction of emotional distress, and the prima facie tort. It pinpointed possible difficulties in establishing these causes of action and, more generally, in pursuing claims against tech-savvy minors —age-related legal constraints, anonymity, and low expected recovery. Section B turned to the two main categories of real-life supervisors: parents and schools. It examined several theories of parental liability, including negligent entrustment of a dangerous instrument, negligent supervision, and negligent enabling of a tort, and identified their particular limits along with the general difficulty associated with anonymous misconduct. Section B then analyzed common law and statutory bases of school and school personnel liability, including negligent supervision, § 1983, and Title VI, and explained that such liability is subject to constitutional and legal constraints on school regulation of student speech and off-campus activity. Section C showed that under American law, virtual supervisors are immune from liability for wrongful user-contributions. It presented the European Union framework and the English model, as well as local calls for reform.

Part II evaluated the different regimes from an economic perspective and laid the foundations for a technology-powered model. Section A explained that primary wrongdoers' liability cannot achieve efficient deterrence because of minors' inability to compensate victims, limited cognitive, emotional, and social capacity, and frequent use of anonymity. Section B discussed real-life supervisors, focusing on the gap between their considerable power to affect supervised children's conduct and the high cost of information necessary for exercising that power. Section C showed that virtual supervisors' liability may be inefficient due to the high cost of monitoring, non-internalization of the economic benefits of the participatory web by service providers, and an asymmetry between false negative and false positive determinations of wrongfulness. Additionally, it argued that virtual supervisors can easily access relevant information but lack the power to affect juvenile conduct.

Lastly, Section D constructed an efficiency-oriented model which integrates technological tools to reduce information costs. First, primary tortfeasors' liability is economically insufficient, but should not be barred. Second, to incentivize parents to reasonably use advanced surveillance applications, the law should impose liability when failure to employ such tools results in juvenile cyber-wrongdoing, in addition to standard liability for not taking reasonable precautions upon learning about the risk. Third, schools should be liable for cyberbullying through school devices if they failed to (1) enforce reliable identification of users, (2) employ advanced surveillance tools, or (3) take reasonable measures to prevent harm upon notification of possible misconduct. Fourth, a virtual supervisor is liable if the victim has insufficient information to identify the wrongdoer, the victim gave notice of the complaint, and the virtual supervisor did not properly respond.

Reports on the high prevalence of cyberbullying, together with rare but salient deaths, have led legislators, policymakers, and academics to an understandable

pursuit of appropriate solutions. Regrettably, while delegation of power to educational institutions and criminalization of cyber-misconduct are relatively common, at least in public discourse, the potential impact of civil liability has been downplayed. This Article has put it under the spotlight, without contesting the possible need for a more comprehensive framework.