*Harvard Journal of Law & Technology*
Volume 31, Number 1 Fall 2017

# TAKING OUT OF CONTEXT

*Michal Lavi* *

## TABLE OF CONTENTS



---

* Ph.D., Cheshin Post-Doctoral Fellow, Hebrew University of Jerusalem, Faculty of Law & Research Fellow, HUJI Cyber Security Research Center (H-CSRC), Law & Cyber Program.

I am most grateful to Tal Zarsky for valuable and insightful comments and guidance in previous stages. I further thank Jonathan Lewy for his helpful input. In addition, I thank the participants of the Annual Private Law Association Conference (College of Management). Last but not least, I thank Alex Harding, Evan Tallmadge and their colleagues on the Harvard Journal of Law and Technology (JOLT) for thoughtful comments and suggestions and for outstanding editorial work.

## I. INTRODUCTION

Herbert Simon once said that "wealth of information creates poverty of attention."[1] This statement has never been more accurate than today. The internet revolutionized communications and eased the diffusion of information. Virtually anyone can post messages or publish ideas on a whim, thus increasing the amount of content online at an exponential rate.[2]

Websites that offer platforms for creating content are known as online or internet intermediaries. These entities utilize technologies that allow users to sort through vast amounts of information and share content beyond the scope of a single platform. They design tools for consuming news feeds and updates, aggregating information from dif-

1. Herbert Simon, Speech at the Johns Hopkins University and Brookings Institution Symposium: Designing Organizations for an Information-Rich World, *in* COMPUTERS, COMMS., AND THE PUB. INT. 37, 40 (Martin Greenberger ed., 1971).

2. *See* Seth F. Kreimer, *Censorship by Proxy: the First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 1, 16–17 (2006).

ferent sources and linking to additional content.[3] That, in turn, affects how users allocate their attention, and understand the content.[4]

Intermediaries also function as gatekeepers and private regulators of information.[5] They can direct users to content, organize the flow of information and accelerate or withhold ideas. New technologies allow intermediaries to take users' content out of the context in which it was expressed and influence what is seen, what is valued, and what is disseminated.[6] Thus, they take an essential part in shaping online discourse,[7] and may even influence election results and democracy.[8] The influence of intermediaries raises a series of challenges that can be explored broadly, but this article focuses on one particular aspect: the

---

3. *See* DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 146–47 (2015); KARINE NAHON & JEFF HEMSLEY, GOING VIRAL 126–27 (2013).

4. *See* Reed Martin & Henry Holtzman, *Newstream, A Multi-Device, Cross-Medium and Socially Aware Approach to News Content*, ASS'N. COMPUTING MACHINERY, 83, 89 (2010).

5. *See* ZEYNEP TUFEKCI, TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST 134 (2017) (explaining that intermediaries function as gatekeepers through a platform's policy, algorithms, and affordances); *see also* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, U.C. DAVIS L. REV., (forthcoming 2018) available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038939 [https://perma.cc/82VX-HZQZ] (" . . . [T]hese companies are the governors of these digital communities, and if you have an account and use the service, you are part of the governed."); Nick Hopkins, *Revealed: Facebook's Internal Rulebook on Sex Terrorism and Violence*, GUARDIAN (May 21, 2017), https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence [https://perma.cc/P9X7-G6HE] (describing in detail Facebook's secret rules and guidelines for deciding what its 2 billion users can post on the site. This is one way in which intermediaries govern speech); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. (forthcoming 2017) (explaining how platforms actually moderate users' content and referring to intermediaries as the new governors in the digital era).

6. *See* CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 147 (2016) ("Internet companies vie to achieve platform status, so that they have a monopoly over users' experience, and thus can monetize and control it."); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 68–79 (2015); JACOB SILVERMAN, TERMS OF SERVICE: SOCIAL MEDIA AND THE PRICE OF CONSTANT CONNECTION 84 (2015) ("[S]ocial networks . . . have the power to influence what rises to the top."); *see generally* James Grimmelmann, *The Virtues of Moderation,* 17 YALE J. L. & TECH. 42 (2015).

7. *See* Yochai Benkler, *Degrees of Freedom, Dimensions of Power,* 145 DAEDALUS 18, 19 (2016) (explaining that online intermediaries have the capacity to alter the behaviors, beliefs, outcomes, or configurations of end users).

8. *See* Owen Hughes, *Fake Election Coverage Got More Facebook Engagement Than Real News in Final Months, Says Buzzfeed,* INT'L BUS. TIMES (Nov. 17, 2016), http://www.ibtimes.co.uk/fake-election-coverage-got-more-facebook-engagement-real-news-final-months-says-buzzfeed-1592107 [https://perma.cc/PS7L-BV7A] (discussing the promotion of fake stories and how elections were influenced by Facebook); *see also* Jonathan Zittrain, *Engineering Elections*, 127 HARV. L. REV. 335–36 (2014) (describing the election experiment: some Facebook users were encouraged to click on a button if they voted and their newsfeed indicated that. Others weren't shown the graphic sign. Researchers cross-referenced everyone's name with actual voting records and found that people who saw a sign that their friends voted were more likely to vote. This experiment illustrates how intermediaries can influence voting rates and even election results.).

direct liability they hold for disseminating user-generated defamatory content.

Consider the following examples:

(1) A review website that rates hotels containing a variety of users' reviews: positive, lukewarm, and negative. These reviews may also defame the hotels' staff. An intermediary from another platform tracks the website by using RSS protocol.[9] This enables the intermediary to display on its own website what had been added in the review website, including the defamatory comments.[10]

(2) An intermediary of a complaints website publishes on Twitter specific posts created by users and emphasizes specific words in them.[11]

(3) An intermediary of a review website allows users to vote for "the review of the day." The most ranked review is automatically published on the home page of the website. Sometimes, the "review of the day" includes defamatory comments.[12]

(4) An intermediary of a review website creates a public profile on Twitter and posts links to defamatory reviews. As a result, followers on Twitter are only exposed to defamatory reviews that were posted on the website.

(5) An intermediary of a website for rating hotels posts on its homepage a list of "The Dirtiest Hotels." It includes anecdotal negative reviews and adds negative titles to them.[13]

---

9. *See RSS (Rich Site Summary)*, WIKIPEDIA, https://en.wikipedia.org/wiki/RSS [https://perma.cc/MQW5-N8L5]; *see also* Kathy E. Gill, *Blogging, RSS and the Information Landscape: A Look at Online News*, http://www.ra.ethz.ch/CDstore/www2005-ws/workshop/wf10/gill.pdf [https://perma.cc/A55L-AUPG] ("RSS allows users to easily syndicate (feed) content headlines or blurbs; other web sites can publish this information at no cost to either party . . . . The feed becomes as a form of free advertisement for the original publisher and also allows the ideas embodied in that feed to easily spread throughout the Internet.").

10. *See* MATTHEW COLLINS, COLLINS ON DEFAMATION 99, ¶ 4.125 (2014). ("[A]ggregation involve[s] the display, within one web page or via a special application, of content from one or more other web pages or online sources.").

11. *See* Roca Labs, Inc. v. Consumer Opinion Corp., 140 F. Supp. 3d 1311, 1315 (M.D. Fla. 2015).

12. *See generally* YELP, http://www.yelp.com [https://perma.cc/YAW8-ZZGY] (the voting system on the popular website, Yelp). The "like" button on Facebook also extends the exposure of popular posts. *See* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU 149–50 (2011).

13. *See, e.g.*, Seaton v. TripAdvisor, LLC, 728 F.3d 592, 594 (6th Cir. 2013) (noting that TripAdvisor's "2011 Dirtiest Hotels" list contained quotes from reviews); GW Equity, LLC v.

The expressions that were disseminated are defamatory. Victims of the offensive speech could file a libel suit against the intermediaries for enhancing the dissemination of the defamatory content.[14] They may argue that repeating the content and increasing its availability exacerbated their harm. This article focuses on whether the law should regulate intermediaries' liability for disseminating defamation that was published by users, how the courts should treat it, and which standards of liability should be used.

The examples mentioned above represent common online strategies for disseminating user-generated content. These examples are not theoretical and courts discuss them regularly.[15] Yet, the scope of liability for dissemination remains unclear. Scholars and policymakers lack a systematic understanding of how content dissemination influences internet users, let alone how the law should respond. This article aims to meet this challenge. It provides a comprehensive framework for intermediaries' liability for disseminating user-generated defamatory content. It entails a nuanced, context-specific analysis that will not impede or be affected by technological advances. It is designed for judges and policymakers who wish to promote just and efficient decisions. Keeping these goals in mind, the article proceeds as follows:

Part II explores how spreading user-generated content affects its availability and magnitude. Drawing on network theory, psychology, marketing, and information systems, it maps the main archetypes of dissemination. This roadmap illustrates how intermediaries can amplify the severity of damage caused by defamatory content.

Part III reviews traditional defamation laws on libelous repetition offline and argues that it does not accommodate the challenges of the digital era. Afterwards, it overviews the regulatory regimes governing different traditional forms of media. It demonstrates that different entities in the distribution chain are governed by different regulatory regimes. Following this analysis, the article argues that differential standards of liability should regulate different types of online activities. Afterwards, it will overview the law governing intermediaries' liability in different countries. It will demonstrate that different courts reach different conclusions regarding liability, causing legal incon-

---

Xcentric Ventures, LLC, No. 3:07-CV-976-O, 2009 WL 62173, at *6 (N.D. Tex. Jan. 9, 2009) (noting a review website may add tags to the ranked business such as "fraud" or "rip-off"); Icon Health & Fitness v. ConsumerAffairs.com, No. 1:16-cv-00168-DBP, 2017 WL 2728413, at *1 (D. Utah June 23, 2017) (the intermediary of a review website omitted the positive reviews of business that did not pay a fee to the platform).

14. *See infra* Part III.D.

15. *See, e.g.*, Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398, 403–05 (6th Cir. 2014); Batzel v. Smith, 333 F.3d 1018, 1021–22 (9th Cir. 2003); Diamond Ranch Acad., Inc. v. Filer, No. 2:14-CV-751-TC, 2016 WL 633351, at *2 (D. Utah Feb. 17, 2016).

sistency. Finally, it shall focus on normative considerations from a wider perspective.

Part IV suggests that intermediaries' liability should be imposed through the prism of context. It offers an innovative framework that differentiates between intermediaries who disseminate content that is consistent with the original context and intermediaries that take it out of context. Binding intermediaries' liability with a breach of context, it outlines nuanced guidelines for deciding the scope of liability depending on the breach of context. These guidelines apply different liability regimes to different types of dissemination. It also addresses objections and challenges to the proposed guidelines.

## II. DISSEMINATION OF DEFAMATION AND HARM

### *A. Bouncing, Highlighting, and Other Influences on the Flow of Information*

Multidisciplinary research addresses three main factors that influence the flow of information and its diffusion. First, the research locates the source of the message and determines whether it is an influential hub or opinion leader in the social network;[16] second, it identifies the context of the message and the way it is represented;[17] third, it pinpoints the audience and the social structure in a given network that forms the context of the situation.[18] These contextual factors have more influence on the flow of information than the individuals who compose the network, and arguably have even more influence than the content of the message itself. [19]

---

16. Everett M. Rogers & David G. Cartano, *Methods of Measuring Opinion Leadership*, 26 PUB. OPINION Q. 435, 435 (1962) ("Opinion leaders" are individuals who "exert an unequal amount of influence on the decisions of others."); *see also* MALCOLM GLADWELL, THE TIPPING POINT: HOW LITTLE THINGS CAN MAKE A BIG DIFFERENCE 60 (2002) (referring to a "maven" as "one who accumulates knowledge."); CHARLES KADUSHIN, UNDERSTANDING SOCIAL NETWORKS: THEORIES, CONCEPTS, AND FINDINGS 145–46 (2011) (describing "opinion leaders" and "influentials"); ELIHU KATZ & PAUL LAZARSFELD, PERSONAL INFLUENCE: THE PART PLAYED BY PEOPLE IN THE FLOW OF MASS COMMUNICATION 25 (2d ed. 1955); EVERETT M. ROGERS, DIFFUSION OF INNOVATION 27 (5th ed. 2003). When an influential hub in a social network spreads a message, the likelihood for it to spread further increases manifold.

17. *See* GLADWELL, *supra* note 16, at 89; Jonah Berger & Katherine Milkman, *What Makes Online Content Viral*, 49 J. MARKETING RES. 192, 201 (2012) ("[O]nline content that evoked high-arousal emotions was more viral . . . ."); Joseph E. Phelps et al., *Viral Marketing or Electronic Word-of-Mouth Advertising: Examining Consumer Responses and Motivations to Pass Along Email*, 44 J. ADVERT. RES. 333, 345 (2004) ("[M]essages that spark strong emotion — humor, fear, sadness, or inspiration — are likely to be forwarded.").

18. *See* GLADWELL, *supra* note 16, at 158; KADUSHIN, *supra* note 16, at 146–48; Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 855, 889 (2016).

19. *See* Philip G. Zimbardo, *The Journey from the Bronx to Stanford to Abu Ghraib*, *in* JOURNEYS IN SOCIAL PSYCHOLOGY: LOOKING BACK TO INSPIRE THE FUTURE 85, 101–02

All five examples mentioned in the introduction demonstrate different ways for disseminating user-generated content and influencing its context. Online content may bounce to another site,[20] and be highlighted to enhance its importance.[21] Intermediaries are central hubs of influence; when they disseminate content they may be perceived as the source of the message and thus influence its magnitude.[22] Disseminating, bouncing, and highlighting users' generated content change its representation and causes a framing effect; in other words, these are biases that affect the reaction towards the content.[23] Furthermore, the content's meaning may change when it is given to a different audience than originally intended, thus, affecting the context of the situation. As content circulates online, it tends to grab users' attention and is perceived as a more credible source of information because the number of persons exposed to it increases.[24] The more times people hear it (especially from different venues), the more likely they are to believe it.[25] Consequently, it is more likely that recipients will further spread the information.[26] Furthermore, dissemination increases the likelihood of the content to rise in Google's search results, thus leading to greater exposure.[27]

---

(Robert Levine et al. eds., 2008); *see generally* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011).

20. *See* EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 73–74 (2013) (explaining that information can be collected for one purpose and used for another purpose on another website and referring to this phenomenon as "bouncing"). Similar to collecting data and using it out of context, this article will refer to intermediaries that bounce information that was published in one context and use it on another online setting.

21. *See id.* (explaining that highlighting occurs when some pieces of disclosed information take on an unintended disproportionate role in defining a person's reputation and hinder other, more pertinent pieces).

22. *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 148 (2017) ("Massively intermediated, platform-based media infrastructures have reshaped the ways that narratives about reality, value, and reputation are crafted, circulated, and contested.").

23. *See* KAHNEMAN, THINKING, *supra* note 19, at 363–76; RICHARD H. THALER, MISBEHAVING: THE MAKING OF BEHAVIORAL ECONOMICS 185 (2015). On the framing effect, see Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCI. 453, 457–58 (1981).

24. *See* NICHOLAS DIFONZO & PRASHANT BORDIA, RUMOR PSYCHOLOGY: SOCIAL AND ORGANIZATIONAL APPROACHES 225 (2007); Gordon Pennycook et al., *Prior Exposure Increases Perceived Accuracy of Fake News* (Aug. 26, 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958246 [https://perma.cc/YDX8-XQFG].

25. *See* CASS R. SUNSTEIN, CONSPIRACY THEORIES & OTHER DANGEROUS IDEAS 25–27 (2014); *see generally* CASS R. SUNSTEIN, ON RUMORS: HOW FALSEHOODS SPREAD, WHY WE BELIEVE THEM, WHAT CAN BE DONE (2009).

26. *See generally* Mark Granovetter*, Threshold Models of Collective Behavior*, 83 AM. J. SOC. 1420 (1978).

27. *See* SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 20–21 (2011).

### *B. Dissemination of Defamation Online: A Roadmap*

Dissemination replicates content and enhances its diffusion. It influences the context of information and the magnitude and credibility ascribed to it. In the internet age, dissemination of content is very common and is mediated by technology. The following sections will map several methods of dissemination that intermediaries utilize. This part will focus on three main categories, differentiate between them, and demonstrate their harm potential: (1) *"Full Dissemination"* — distributing content, or linking to the entirety of that content without discriminating between particular content items; (2) *"Selective Dissemination"* — choosing a particular message or post from a broader webpage or passage and repeating it[28]; (3) *"Adoption of Defamation"* — endorsing or reinforcing users' defamatory content.

When intermediaries disseminate libelous speech, the harm may be severe because individuals tend to ascribe more weight to negative content than positive. This is known as the "negativity bias" and the greater power of bad events.[29] Due to this bias, negative expressions are given more weight than others. Therefore, even if other users in the social network try to counter the defamation, the negative hearsay could outweigh the positive expressions. The defamatory remarks could continue to spread rapidly and harm a person's reputation.

Due to the potential harm of disseminating defamatory content by intermediaries, comprehensive theoretical analysis of their liability is indispensable. The three categories form a descriptive roadmap and provide a solid understanding of dissemination and its influence. This roadmap focuses on the main methods of dissemination and does not purport to encompass all of them. Although more types of dissemination may develop as technology advances, by mapping their main forms and understanding their effects, updating future changes should be an easy task.

#### 1. Full Dissemination

*An online intermediary tracks updates of ratings from a review website by utilizing RSS protocol. Some of the reviews are defamatory.*

*An online intermediary links to another website that includes defamation.*

---

28. This category takes multiple forms. Selective dissemination may be based on users' requests to receive updates on particular topics or depend on users' signaling. Deep direct links, on the other hand, direct users to a specific selected passage without replicating it on the intermediary's own site.

29. *See generally* Roy Baumeister et al., *Bad Is Stronger Than Good*, 5 REV. GEN. PSYCHOL. 323 (2001) (reviewing studies of negativity bias).

Intermediaries can spread users' content without selecting specific content items for dissemination. The intermediary may disseminate overall users' content from one section of the platform to another location or platform, which includes different recipients and social structures.[30] For example, the intermediary can import content from another platform by utilizing RSS protocol,[31] or by copying overall content from one platform to another.[32] Similarly, it may use a link and connect to another platform.[33] In this case, the link is only a gateway to another platform, thus the intermediary does not repeat the content.

Full dissemination may include defamation. It increases the exposure to the content because it reproduces the original content or enhances its availability. Thus, a larger audience will be exposed to the content. Yet, since the intermediary does not select particular content items for dissemination, full dissemination does not enhance the magnitude of defamatory content. It does not specifically direct users to the defamatory speech, and it has only marginal influence on the source of the message and its context. Thus, one should not expect that the defamation would inflict greater harm in comparison to the harm of the original source of the message.

2. Selective Dissemination

*The intermediary "pissedconsumer.com" tweets specific defamatory posts from its platform.*[34]

*A manager of a public Facebook page selects to disseminate specific posts at his discretion.*[35]

Intermediaries may select particular messages, or posts from a larger database and disseminate them. Consequently, users are likely to grant them much more attention.[36] Selecting particular content for

30. *See* Lavi, *supra* note 18, at 894 (discussing different recipients and social structures).

31. *See generally RSS*, *supra* note 9.

32. *See* Universal Communication Systems, Inc. v. Lycos Network 478 F.3d 413 (1st Cir. 2007).

33. *See* DAVID A. POTTS, CYBERLIBEL: INFORMATION WARFARE IN THE 21ST CENTURY? 39–41 (2011) (describing how links allow navigating from one platform to another. The intermediary does not control the content. Therefore, every change, or correction of the content will be displayed to the users who click on the link. Basic links, as opposed to deep direct links, do not direct users to specific items.).

34. *See* Roca Labs, Inc. v. Consumer Opinion Corp., 140 F. Supp. 3d 1311, 1315 (M.D. Fla 2015).

35. *See, e.g.*, *Israeli Facebook Page Camouflages Sponsored Content*, YNET (Jan. 14, 2015, 7:18 PM), http://www.ynetnews.com/articles/0,7340,L-4615200,00.html [https://perma.cc/5UYY-P9MY] (describing "Statusim Metzayitzim" (Tweeting Statuses), one of the most popular pages in Israel with 718,000 followers. Commercial entities paid the page's managers to promote specific user-generated content. In some cases, they paid to promote negative and defamatory content against competitors.).

36. *See* Batzel v. Smith, 333 F.3d 1018, 1038–39 (9th Cir. 2003) (Gould, J., dissenting).

dissemination changes its context.[37] The recipient of the content understands that it is worthy of dissemination because the intermediary, a central hub of influence and power, selected it.[38]

Selecting particular defamatory content for dissemination changes the context of the message. It leads to a "framing effect",[39] which focuses the attention to it and influences its interpretation and the magnitude ascribed to it. Selection of only specific types of content provides users incomplete information and may lead to false impressions. For example, an intermediary of a review website that disseminates to Twitter only negative reviews on a product may lead users to avoid this product. However, this decision is based on incomplete information and might have been different had the intermediary disseminated all the reviews. Providing users with partial information may lead to inefficient consumer choices. Selective dissemination also presents content out of context from its original social network to a different audience.

Today, technological tools allow intermediaries to receive personal information on their users through data mining, and they can personalize the dissemination.[40] Thus, they can display different types of content to different audiences by using complex algorithms and artificial intelligence (AI).[41]

Selection of defamatory content for dissemination enhances its magnitude and exacerbates the gravity of harm. It also increases the likelihood of users to spread the defamatory speech, because the more people have access to it, the more likely they are to believe the speech.[42] Thus, it may generate informational and reputational cas-

---

37. *See id.*

38. *See id.*

39. *See generally,* Tversky, *supra* note 23, at 457–58 (studying the framing effect); *see* NAHON & HEMSLEY, *supra* note 3, at 49–52 (describing how selective dissemination leads to a framing effect. The selection can include purely defamatory content or a mixture of content including defamatory content. This influences the degree of framing).

40. *See generally* Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data*, 64 STAN. L. REV. ONLINE 70 (2012); Colin Bennett, *Voter Surveillance, Micro-Targeting and Democratic Politics: Knowing How People Vote Before They Do* (April 11, 2014) (unpublished manuscript) (on file with University of Victoria, Department of Political Science) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605183 [https://perma.cc/27A9-73DH] (discussing data mining in politics).

41. *See* James Grimmelmann, *The Law and Ethics of Experiments on Social Media Users*, 13 COLO. TECH. L.J. 219, 223 (2015) (describing how a few years ago, Facebook used algorithms for distributing specific types of content to users' feeds); Adam D.I. Kramer, et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. 8788, 8788 (2014); *see also* Balkin, *Algorithmic Society*, *supra* note 5 (describing digital infrastructure owners' use of algorithms and artificial intelligence to shape people's lives and opportunities).

42. *See* DIFONZO, *supra* note 24.

cades and lead to an extensive diffusion of ideas through the network.[43]

*a) Selective Dissemination Following Users' Requests or Signals*

*An intermediary allows users to receive updates containing specific keywords of their choice from its website via e-mail or RSS. Some updates could include defamation.*[44]

*The intermediary "Yelp" allows users to vote for "the review of the day."*[45] *The selected review is loaded to the homepage of the platform. Some of the selected reviews are defamatory.*

Selective dissemination may depend on users. Some intermediaries allow users to receive updates on specific topics. They may also allow them to vote for reviews or "like" posts. Content that receives many votes is disseminated and gets tremendous attention. This often leads to the dissemination of defamatory content, which exacerbates the severity of its harm.[46] Yet, by voting for a review or liking a post, the user expresses his own original view or speech.[47] An algorithm calculates the weight of votes, and the intermediary's part is only functional.[48]

*b) Deep Direct Linking*

*The intermediary links directly to defamatory content.* [49]

Technology allows direct links to particular expressions by using deep inline linking. [50] In contrast to basic links, which expose users to the entire context in which a message is expressed, deep linking di-

---

43. *See generally* Granovetter, *supra* note 26.

44. *See* Courtney v. Vereb, No. 12-655, 2012 WL 2405313, at *1 (E.D. La. June 25, 2012).

45. *See* YELP, http://www.yelp.com/ [https://perma.cc/YAW8-ZZGY].

46. *See infra* Part II.B.2. (discussing selective dissemination by intermediaries).

47. *See, e.g.*, Bland v. Roberts, 730 F.3d 368, 386 (4th Cir. 2013); Ira P. Robbins, *What Is the Meaning of "Like"?: The First Amendment Implications of Social-Media Expression*, 7 FED. CTS. L. REV. 127, 127 (2013).

48. *See* Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1517–24 (2013) (discussing the functionality doctrine).

49. *See, e.g.*, Shrader v. Biddinger, 503 F. App'x 650, 650 (10th Cir. 2012); Vazquez v. Buhl, 90 A.3d 331, 334 (Conn. App. Ct. 2014).

50. *See* Eugene R. Quinn, Jr., *Web Surfing 101: The Evolving Law of Hyperlinking,* 2 BARRY L. REV. 37, 45 (2001); Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 MINN. L. REV. 609, 632 (1998); Nicole Downing, Note, *Using Fair Use to Stop a Copyright Troll from Threatening Hyperlinks,* 12 N.C. J.L. & TECH. 155, 158 (2011); Matthew Scherb, Note, *Free Content's Future Advertising, Technology, and Copyright*, 98 NW. U.L. REV. 1787, 1808 (2004).

rects users' attention to specific content, frames that content, and enhances its importance.[51] As a result, users are not exposed to the entire social context in which the message was originally expressed.[52] Yet, most deep links allow users to navigate through the screen and thus see the entire context.[53] Furthermore, linking to content does not replicate it and instead exposes users to changes and corrections in the original content. Thus, it may result in less severe harm in comparison to actual dissemination of defamation.

3. Adoption of Defamation

*An intermediary publishes a list based on negative and defamatory users' ranking, titled: "TripAdvisor Lifts the Lid on America's Dirtiest Hotels."*[54]

An intermediary can mix its own content with user-generated posts, which are defamatory in nature.[55] The content added by the intermediary may be neutral,[56] yet, in some cases, it is not. For example, the intermediary can adopt user-generated defamatory rankings by making its own additions to the content.[57] The additions made by the intermediary to users' messages or posts focus the public's attention to them, enhance their magnitude, and influence their context. An intermediary that adopts content functions as a social actor, and users may perceive the intermediary as the source of the message.[58] Consequently, they may ascribe to the message more weight and credibility than they otherwise would.[59] By mixing its own content with the user-generated content, the intermediary influences the context and the social dynamics of the recipients. The adoption of content increases the likelihood of spreading the new combined content. As a result, the gravity of harm caused by the adoption is significant.

---

51. *See* POTTS, *supra* note 33, at 41.

52. *See id.*

53. *See* Scherb, *supra* note 50.

54. *See* Seaton v. TripAdvisor, LLC, 728 F.3d 592, 594 (6th Cir. 2013).

55. Samuel J. Morley, *How Broad is Web Publisher Immunity Under § 230 of The Communication Decency Act of 1996?*, 84 FLA. B.J. 8, 23 (2010).

56. For example, adding a title or link to "see users' reviews."

57. For example, an intermediary may add titles such as "All the Truth About," "The Dirtiest Hotels," "Rip-off," and "Con-artists" to users' ranking. *See* POTTS, *supra* note 33, at 260–61; *See TripAdvisor*, 728 F.3d. at 594; GW Equity v. Xcentric Ventures, No. 3:07-CV-976-O, 2009 WL 62173, at *5 (D. Tex. Jan. 9, 2009).

58. *See generally* B.J. FOGG, PERSUASIVE TECHNOLOGY: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO (2003).

59. *See* KENT GREENFIELD, THE MYTH OF CHOICE 116 (2011).

4. Interim Summary

Intermediaries, who disseminate user-generated defamatory content, influence the perception of the message and its context. They also expand the crowd of recipients and alter the form of publication. Different methods of dissemination effect reputational harm in different ways. When the same expressions are disseminated, the gravity of harm inflicted by selective dissemination is more significant in comparison to full dissemination. In addition, the gravity of harm resulted by adoption of defamation may exceed the harm of selective dissemination. Examining the ramifications of dissemination, their influences on context and the gravity of harm, takes the first step towards providing a theoretical framework and guidelines for deciding the liability of intermediaries.

Table 1: Types of Dissemination

| **Type of Dissemination** | **Examples** | **Implications** |
|---|---|---|
| Full Dissemination | • Reproducing content and disseminating without selecting specific items for dissemination.<br>• RSS that publishes feeds from a passage of a website to another platform (In contrast to publishing feeds related to specific words).<br>• Basic links | • Enhancing the dissemination of content and increasing the exposure to it. |
| Selective Dissemination | • Selecting specific messages or posts and disseminating on Twitter.<br>• Disseminating anecdotal negative reviews to the front page of the platform. (TripAdvisor)<br>• Voting systems: dissemination based on users' choices<br>• Yelp ("the review of the day")<br>• Facebook ("like" button)<br>• Deep-direct linking | • Signaling that the information is worthy of dissemination (reinforcing the source of the message)<br>• Framing defamation (influencing the context of the message).<br>• Influencing the quantity and magnitude of defamatory content.<br>• A larger audience (a change in the context of situation).<br>• The likelihood for users to spread defamation increases. |

| | | |
|---|---|---|
| Adoption | • Adding defamatory headlines to content: "The Dirtiest Hotels," TripAdvisor<br>• Adopting users' defamatory content-thedirty.com. | • Users are likely to perceive the intermediary as the source of the message.<br>• Titles and headlines that adopt content frame it and change the context of the message.<br>• Adoption of defamation influences social dynamics of the recipients and increases the likelihood of spreading the defamatory content. |

## III. INTERMEDIARIES' LIABILITY FOR DEFAMATION: THE LAW, NORMATIVE ANALYSIS, AND A CALL FOR CHANGE

### *A. Liability for Defamation Offline*

The debate on liability for repeating defamation is not new. Section 578 of the Restatement (Second) of Torts[60] subjects the republisher of defamation to the same liability as the original publisher. Responsibility for publication is not excused by the fact that the disseminator merely passed on the defamatory statement without endorsement.[61] This repetition rule is a long-standing common law principle and it applies in many countries.[62]

This rule aims to disincentivize repetition because the last utterance may cause as much harm as the first.[63] Another rationale for imposing liability on republishers is preventing a delay in the dissemination of ideas. Exempting repetition from liability deters first publishers of controversial articles that might result in a defamation suit. In contrast, if the original publishers *and* the republishers are both

60. *See* RESTATEMENT (SECOND) OF TORTS § 578 (AM. LAW INST. 1977).

61. *See* Barry v. Time, Inc., 584 F. Supp. 1110, 1122 (N.D. Cal. 1984) ("American courts have traditionally refused to distinguish between publishers and republishers of defamatory statements, on the theory that 'tale bearers are as bad as tale makers.'" (quoting McDonald v. Glitsch, 589 S.W.2d 554, 556 (Tex. Civ. App. 1979))).

62. *See, e.g.*, COLLINS, *supra* note 10, at ¶ 4.96–4.97; GATLEY, LIBEL AND SLANDER §11.4 (Patrick Milmo et al. eds., 11th ed. 2006); POTTS, *supra* note 33, at 302 (on the repetition rule in Canada); Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 588 (2001).

63. *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113 (5th ed. 1984); Matt C. Sanchez, Note, *The Web Difference: A Legal and Normative Rationale Against Liability for Online Reproduction of Third Party Defamatory Content*, 22 HARV. J.L & TECH. 301, 303 (2008).

liable for defamation, there is no longer an incentive for a first publisher to hold back. As a result, news gets out faster.[64]

Repetition of defamation is considered a publication on its own and gives a new cause of action, even if the disseminator states the source.[65] However, courts will not impose liability on the one who repeats if he enjoys privileges or defenses. Privileges can be absolute or qualified.[66] Absolute privileges completely immunize the defendant from liability.[67] Thus, for example, truth is an absolute defense and it only requires proof that the statement was substantially true.[68] Qualified privileges relieve a defendant of liability for defamation to protect his interest, the public's interest, or the interests of others.[69]

Generally, there are four categories of qualified privileges.[70] The first is "the public interest privilege, to publish materials to public officials on matters within their public responsibility."[71] The second is "the privilege to publish to someone who shares a common interest in defense of oneself or in the interest of others."[72] The third is fair comment, which "protects the defendant's statement of opinion about matters of public interest, provided the defendant truly stated the facts upon which the opinion was based."[73] The fourth is "the privilege to make a fair and accurate report of public proceedings and public documents."[74] Indeed, "qualified privileges are conditional, such that a defendant may forfeit them by exceeding the scope of the privilege, engaging in excessive publication, or publishing with an improper purpose."[75] Due to defenses and privileges, in some circumstances courts may not hold the republisher of defamation responsible.

To conclude, different circumstances of dissemination may lead to different conclusions of liability.

---

64. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 246 (9th ed. 2014).

65. *See* KEETON, *supra* note 63.

66. *See id.* at § 114–116.

67. *See id.* at § 114 (stating that these absolute privileges apply, for example, to statements made during judicial and legislative proceedings). Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting § 230 Immunity*, 30 BERKELEY TECH. L.J. 1505, 1515 (2015).

68. *See* Maheu v. Hughes Tool Co., 569 F.2d 459, 459–65 (9th Cir. 1977); KEETON, *supra* note 63, at § 116; Browne-Barbour, *supra* note 67; *see also* RESTATEMENT (SECOND) OF TORTS § 581A, cmt. f. (AM. LAW INST. 1977).

69. *See* RESTATEMENT (SECOND) OF TORTS §§ 585, 594, 595, 598 (AM. LAW INST. 1977).

70. *See* Browne-Barbour, *supra* note 67, at 1515–16.

71. *See id.* (quoting DAN B. DOBBS ET AL., THE LAW OF TORTS § 554 (2014)).

72. *Id.*

73. *Id.* (quoting DAN B. DOBBS ET AL., THE LAW OF TORTS § 567 (2014)). This privilege was adopted in England. The Defamation Act of 2013 provides defenses for truth and honest opinions. *See* Defamation Act of 2013, ch. 26, §§ 2, 3.

74. Browne-Barbour, *supra* note 67, at 1515–16 (quoting DAN B. DOBBS ET AL., THE LAW OF TORTS § 548 (2014)).

75. *Id.* at 1516.

### *B. Online Dissemination*

Repeating speech online is different from offline. New technologies allow the dissemination of ideas to a broad audience easily and quickly.[76] The internet revolution minimizes the costs of dissemination and fuels the distribution of ideas, information, and rumors. Online practices of cutting-and-pasting, aggregating, sharing, and linking to content are unlike anything that was known before. The public benefits from this revolution in public dialogue.[77] However, it may exacerbate reputational harm. It also challenges policymakers and the courts.[78] Defamation laws seem inadequate to respond to the challenges of dissemination of user-generated defamatory content. Thus, there is a need to rethink the proper interpretation of the law and the normative regulations it emits. How should the law respond to dissemination of defamation online? Should it be treated as offline publication? Should online disseminators bear responsibility?

Online communications are based on the process of spreading information from other sources. Once a single actor introduces a piece of information online, users disseminate it. This offers the opportunity for greater depth of commentary and discussion than traditional media.[79] The immense public dialogue opened by online dissemination allows discussion of great speed and depth on the issues of the day. Thus, it is different from dissemination offline.

One might argue that imposing liability on disseminators of defamation would chill valuable dialogue and speech. Due to the compelling benefits of online dissemination, special protections are warranted. Furthermore, unlike traditional media outlets, it is difficult to expect most of the disseminators online to correctly judge the credibility of the content they repeat. Imposing liability on them may deter dissemination of content, restrict valuable dialogue, and curb free speech.[80] Therefore, one may argue that those who disseminate defamation should not bear liability at all.

---

76. Everyone can forward an e-mail or share information in social networks by simply clicking on the "share" or the "re-tweet" button. Thus, within milliseconds a message can travel around the world and be viewed by millions of users.

77. *See* Sanchez, *supra* note 63, at 309, 316.

78. The article will focus on these challenges in Section III.D, *infra*. *See, e.g*, Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003); Vazquez v. Buhl, No. FSTCV126012693S, 2012 WL 3641581 (Conn. Super. Ct. July 17, 2012); *aff'd*, 90 A.3d 331 (Conn. App. 2014); Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398 (6th Cir. 2014).

79. *See* Sanchez, *supra* note 63, at 316; Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535, 562–66 (2004) (discussing the importance of copying for free speech and democracy).

80. Sanchez, *supra* note 63, at 317.

The digital age allows ideas to spread exponentially and reach a global audience by the click of a button.[81] Ideas that spread on the internet are not ephemeral and are accessible and searchable via Google or another search engine.[82] In light of these characteristics, the dissemination of defamation online increases the severity of reputational harm. This is even more true when online intermediaries disseminate content, due to their centrality and power, which influences the interpretation of content and the likelihood of spreading it further.[83]

### *C. On Three Traditional Standards of Liability and Online Intermediaries*

Liability for a publication extends beyond the author to all those who participate in its preparation and communication.[84] Traditionally, the law discerned between the original author and those who disseminated the publication. Before the internet age, the common law identified three types of intermediaries and classified their liability accordingly: publisher, distributor, and common carrier. Their scope of liability is determined based on the amount of editorial control and discretion over the defamatory content.[85]

Primary publishers are those who own and operate print media, such as newspaper and book publishers, as well as owners of broadcast media, such as radio and television stations.[86] They face strict liability for defamation whether or not they are the original authors of the statement, for "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it."[87] The reason for holding publishers responsible is that they exert editorial control over content and devote time and money in vetting stories for publication. This often conveys a sense of authority among readers. Consistent with this perception, courts treat primary publishers as if

---

81. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 61–62 (2014); LEE RAINE & BARRY WELLMAN, NETWORKED: THE NEW SOCIAL OPERATING SYSTEM 67 (2012).

82. DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 11–12 (2014); Daniel J. Solove, *Speech Privacy and Reputation on the Internet*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATIONS 16 (Saul Levmore & Martha Nussbaum eds., 2010).

83. On the power of intermediaries, see *supra* note 22.

84. *See* COLLINS, *supra* note 10, ¶ 4.36.

85. Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 144 (2008).

86. *See id.*; Virginia A. Fitt, *Crowdsourcing the News: News Organization Liability for iReporters*, 37 WM. MITCHELL L. REV. 1839, 1851 (2011) (rebroadcasters of user-generated content are generally liable and are considered to have endorsed the content).

87. *See* Browne-Barbour, *supra* note 67, at 1520 n.114. Restatement (Second) of Torts § 578 (AM. LAW INST. 1977).

they have adopted the statements they published as their own.[88] Consequently, they benefit from the protection of the First Amendment but are also subject to liability.[89]

In contrast to publishers, the law considers distributors as passive conduits of information. Although they can control the content they disseminate, in most cases they do not exercise control over it and do not know what is disseminated. Prescreening the content they deliver would impose too heavy a burden on them. It is difficult to expect them to invest time and effort to that end. In light of their limited control over content, a bookseller who only delivers defamation of third parties is subject to liability only if he knew, or should have known of the defamatory nature of the message.[90] Knowledge, or imputation of knowledge, is generally found when the defendant exercises editorial control over content.[91] Distributors may still face liability if they continue to disseminate defamation after they are made aware of it.[92]

Common carriers such as telephone companies differ from primary publishers and distributors. Since they have no editorial control over the statements they carry and are required by regulations to offer their services to anyone on just and reasonable terms without discrimination,[93] they traditionally enjoyed immunity for defamatory statements conveyed on their networks.[94]

The internet is fundamentally different from traditional media, both in its architecture and in its applications. Consequently, policymakers must address the normative standard of liability for intermediaries who disseminate users' content in comparison to traditional categories of liability.

---

88. Knowing selection of that repertoire distinguishes primary publishers from carriers that merely move information without identifying or selecting the content they carry. *See* Lavi, *supra* note 18, at 865; Wu, *supra* note 48, at 1521. There are exceptions to this rule. Courts may not impose liability on broadcasters of third parties' recorded programs when they did not exercise editorial control and did not know or have a reason to know of the defamation they contained. *See* Auvil v. CBS 60 Minutes, 800 F. Supp. 928 (E.D. Wash. 1992); William E. Buelow III, *Re-Establishing Distributor Liability on the Internet: Recognizing the Applicability of Traditional Defamation Law to Section 230 of the Communications Decency Act of 1996*, 116 W. VA. L. REV. 313, 322–25 (2013) (discussing *Auvil*).

89. *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 636 (1994); Ciolli *supra* note 85, at 145; Wu, *supra* note 48, at 1521; Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 258 (2006).

90. *See* Ciolli, *supra* note 85, at 145; Browne-Barbour, *supra* note 67, at 1511.

91. *See* Church of Scientology v. Minn. State Med. Ass'n Found., 264 N.W.2d 152, 156 (Minn. 1978); Henry H. Perritt, Jr., *Tort Liability, the First Amendment and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65, 99–100 (1992).

92. *See* Ciolli, *supra* note 85, at 145.

93. On common carriers, see James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 251 (2002); Eli M. Noam, *Beyond Liberalization II: The Impending Doom of Common Carriage*, COLUM. UNIV. WORKING PAPERS SERVER PROJECT. (Mar. 15, 1994), http://www.columbia.edu/dlc/wp/citi/citinoam11.html [https://perma.cc/J67H-UTFR].

94. *See* Ciolli, *supra* note 85, at 145; Lavi, *supra* note 18, at 865.

Online intermediaries can exercise editorial control over users' content and at times even elect to disseminate specific statements. Thus, they are very different from common carriers. One may argue that online intermediaries resemble traditional publishers due to their ability to control and disseminate content to a wide audience. However, the analogy is inaccurate. Unlike the traditional publisher, who brings content to public awareness, users' generated content is already in the public domain and dissemination by online intermediaries only extends its availability. Additionally, the liability of traditional publishers stems from the influence and authority ascribed to them.[95] In contrast, anyone can spread content online. As a result, people usually ascribe less authority to online intermediaries in comparison to traditional publishers. Furthermore, online intermediaries may lack the resources of traditional media entities and would find it nearly impossible to operate if the law forced them to verify the truth of the information they plan to disseminate.[96]

It must be stated that not all online intermediaries select particular content for dissemination. Technologies allow intermediaries to track content from other websites automatically, without manual selection and without predicting in advance what type of content is disseminated.[97] Moreover, as mentioned above, selective dissemination may depend on users' choices and votes. In such cases, there is no direct causal link between the intermediary and the dissemination of content.

Distributors and online intermediaries are comparable in some ways. However, unlike distributors, who usually have no knowledge of what they disseminate, many intermediaries select content for dissemination and control the content they transmit. For example, intermediaries can selectively tweet passages of users' posts to Twitter.[98] For this reason, online intermediaries do not fit neatly into the categories of traditional intermediaries, and different types of online dissemination justify different types of regulation.

### *D. Republication and Online Intermediaries — A Comparative Perspective*

#### 1. United States

In the United States, lawsuits against online intermediaries are usually blocked. Section 230(c)(1) of the Communications Decency

95. Lavi, *supra* note 18, at 862.

96. *See* Sanchez, *supra* note 63, at 308.

97. Automatic dissemination can be a result of the use of RSS protocols. *See RSS*, *supra* note 9.

98. *See* Roca Labs, Inc. v. Consumer Op. Corp., 140 F. Supp. 3d 1311, 1320 (M.D. Fla. 2015).

Act[99] ("CDA") directs that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[100] Under this subsection, titled "[p]rotection for 'Good Samaritan' blocking and screening of offensive material,"[101] Congress declared that online intermediaries could never be treated as publishers for material they did not develop.[102] Courts have interpreted § 230 broadly and repeatedly shielded web enterprises from lawsuits in a plethora of cases.[103] Thus, lawsuits seeking to hold an intermediary liable for its exercise of a publisher's editorial functions — such as deciding whether to publish, withdraw, postpone, screen, or alter content — are barred.[104] Intermediaries maintain their immunity as distributors and as publishers. This immunity applies even when the intermediary knew of the defamatory content and did not remove it.[105]

If the intermediary is responsible in whole or in part for the "creation or development"[106] of content, courts may find it to be an information content provider.[107] Section 230 does not define "creation" or "development," hence the line between the service itself and creation of information is blurred, and the scope of liability is ambiguous.[108]

---

99. 47 U.S.C. § 230(c)(1) (2012).

100. *Id.* The CDA defines information content provider as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." § 230(f)(3).

101. 47 U.S.C. § 230(c). Section 230(c)(2) was enacted in order to encourage intermediaries to screen harmful content. It requires intermediaries who screen content to do so in good faith. *Id.* Yet, no intermediary has lost its immunity because it did not make a good faith filtering decision. *See* Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 U.C. IRVINE L. REV. 659, 665 (2012); *see e.g.*, Joseph v. Amazon.com, Inc., 46 F. Supp. 3d 1095 (W.D. Wash. 2014); Zhang v. Baidu.com Inc., 10 F. Supp. 3d 433 (S.D.N.Y. 2014).

102. § 230(c)(1); Cecilia Ziniti, *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, 584–85 (2008).

103. *See e.g.*, Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 254 n.4 (4th Cir. 2009); Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997); Caraccioli v. Facebook, Inc., 167 F. Supp. 3d 1056, 1064–65 (N.D. Cal. 2016), *aff'd* Caraccioli v. Facebook, Inc., No. 16-15610, 2017 WL 2445063 (9th Cir. June 6, 2017); Glob. Royalties, Ltd. v. Xcentric Ventures, LLC, 544 F. Supp. 2d 929, 932 (D. Ariz. 2008); Giordano v. Romeo, 76 So. 3d 1100 (Fla. Dist. Ct. App. 2011); *see also* Anupan Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 653-55 (2014); Lavi, *supra* note 18, at 867–70.

104. *See Zeran* 129 F.3d at 332; Levitt v. Yelp! Inc., Nos. C-10-1321 EMC, C-10-2351 2011 WL 5079526, at *5–6 (N.D. Cal. Oct. 26, 2011), *aff'd* 765 F.3d 1123 (9th Cir. 2014); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 719 (Ct. App. 2002) (publishers supplementing content).

105. *See Zeran*, 129 F.3d at 330–31.

106. § 230(f)(3).

107. *See* Zak Franklin, *Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites*, 102 CALIF. L. REV. 1303, 1316 (2014); *see also* Anupan Chander & Uyên P. Lê, *Free Speech*, 100 IOWA L. REV. 501, 514 (2015).

108. *See* Ken S. Myres, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 191–192 (2006).

Most courts exempt intermediaries from liability for disseminating users' content.[109]

Yet, some courts may still consider dissemination as "creation or development" of content in some circumstances, and thus, the ambiguity remains. The following sections will review main judicial decisions regarding different forms of dissemination.

*a) Selective Dissemination.*

In *Batzel v. Smith*,[110] the court discussed liability for selective dissemination of users' content. An operator of a website and an electronic listserv included a third party's defamatory email to a newsletter, with only minor edits.[111] The Ninth Circuit debated his responsibility for doing so and shielded him from liability.[112] The court concluded that the operator of the listserv should not be held responsible if a reasonable person in his position would have believed the third party provided the information for the purpose of distribution.[113] Thus, it held that the listserv operator was an "interactive computer service provider" under § 230, and could be immune from liability, despite his editorial control over the listserv messages.[114]

Judge Gould dissented from the majority's analysis. He explained that by providing immunity to parties that disseminate writings whose authors intended to publish, the court developed a rule that encourages spreading harmful lies with impunity.[115] He also referred to selective dissemination and concluded that selection of particular information on the internet forms the impression that it is worthy of dissemination.[116] The focus should not be on the author's intent, but on the de-

109. *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, 461–62 (2010); Charles F. Marshall & Eric M. David, *Prior Restraint 2.0: A Framework for Applying Section 230 to Online Journalism*, 1 WAKE FOREST J.L. & POL'Y 75, 81–82 (2011).

110. 333 F.3d 1018 (9th Cir. 2003).

111. *Id.* at 1022 ("Cremers published Smith's e-mail message to the Network, with some minor wording changes, on the Network listserv.").

112. *See id.*

113. *See id.* at 1034.

114. *See id.* at 1031; Marshall & David, *supra* note 109, at 82; Amanda Groover Hyland, *The Taming of the Internet: A New Approach Third-Party Internet Defamation*, 31 HASTINGS COMM. & ENT. L.J. 79, 102 (2008).

115. *See Batzel* 333 F.3d at 1038 (Gould, J., dissenting). For similar criticism of the immunity for online republication, see Samsel v. Desoto County School District, 242 F. Supp. 3d 496, 539 (N.D. Miss. 2017) ("It seems likely that, if upheld as the law by appellate courts, more and more individuals will become aware of the broad immunity offered by the CDA and seek to abuse it . . . . [I]t should not be difficult for an individual possessing even minimal tech saavy [sic] to make an anonymous post or email defaming another and then forward his own post or email to a targeted audience, under the guise of a 'look what I read on the internet' email.").

116. *See Batzel*, 333 F.3d at 1039.

fendant's acts. Thus, a defendant who has actively elected to disseminate defamatory content should not be entitled to immunity.[117]

The majority's broad interpretation of § 230 in *Batzel* is prevalent. In most cases, courts apply the immunity to intermediaries who selectively disseminate users' content.[118] Courts also apply broad immunity to users who selectively disseminate third parties' defamatory content.[119] This broad interpretation was criticized in legal scholarship. Some scholars claimed that Congress did not intend to extend § 230 to those who behave like traditional publishers when they select content for publication.[120] On the other hand, other scholars thought that such broad immunity is necessary to prevent chilling effects and protect valuable speech.[121]

*b) Selective Dissemination Following Users' Requests or Signals.*

Broad immunity is usually enforced in cases of selective dissemination following users' requests or signals. In *Courtney v. Vereb*,[122] the intermediary of the review website "Angie's List" provided copies of posted reviews, including defamation, to consumers upon their request via fax.[123] Despite the fact that the intermediary disseminated the posts offline, the court applied the immunity.[124]

This broad interpretation also applies to dissemination following users' votes or signals when the intermediary's part is only functional.

---

117. *See Batzel*, 333 F.3d at 1039 (Gould, J., dissenting).

118. *See, e.g.*, Roca Labs, Inc. v. Consumer Op. Corp., 140 F. Supp. 3d 1311, 1320 (M.D. Fla. 2015) (exempting the intermediary "pissedconsumer.com" from liability for tweeting excerpts of users' posts, emphasizing specific words in the posts and omitting much of the original posts in order to fit within Twitter's character limit); O'Kroley v. Fastcase, Inc., 831 F.3d 352, 355 (6th Cir. 2016) (exempting Google from liability for posting excerpts of websites appearing in search results). There have been some cases in which courts did not apply the immunity. In those cases, the disseminator also adopted the content, which may be the reason for not extending immunity. *See, e.g.*, Diamond Ranch Acad., Inc. v. Filer, No. 2:14-CV-751-TC, 2016 WL 633351, at *21–22 (D. Utah Feb. 17, 2016).

119. *See, e.g.*, Barrett v. Rosenthal, 146 P.3d 510, 529 (Cal. 2006).

120. *E.g.*, Joshua N. Azriel, *Social Networking as a Communications Weapon to Harm Victims: Facebook, Myspace, and Twitter Demonstrate a Need to Amend Section 230 of the Communications Decency Act*, 26 J. MARSHALL J. COMPUTER & INFO. L. 415, 424 (2009); Stephanie Blumstein, *The New Immunity in Cyberspace: The Expanded Reach of the Communications Decency Act to the Libelous "Re-Poster"*, 9 B.U. J. SCI. & TECH. L. 407, 417–18 (2003); Andrea L. Julian, Comment, *Freedom of Libel: How an Expansive Interpretation of 47 U.S.C. § 230 Affects the Defamation Victim in the Ninth Circuit*, 40 IDAHO L. REV. 509, 519 (2004); Jae Hong Lee, Note, *Batzel v. Smith & Barrett v. Rosenthal: Defamation Liability for Third Party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 474 (2004) ("It seems reasonable to assume that if Congress had wanted to grant immunity from distributor liability, it would have done so explicitly."); Melissa A. Troiano, Comment, *The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs*, 55 AM. U. L. REV. 1447, 1468 (2006).

121. *See* Sanchez, *supra* note 65, at 317.

122. No. 12-655, 2012 WL 2405313 (E.D. La. June 25, 2012).

123. *Id.* at *5.

124. *Id.* at *6.

In *Obado v. Magedson*,[125] the court applied § 230 to a search engine that generated an autocomplete system and completed users' search terms with defamatory expressions.[126] The court noted that this system does not strip the search engine from the CDA's protection because such autogenerated terms indicate that other websites and users have connected the plaintiff's name with certain terms.[127]

*c) Linking to Defamation*

Courts also immunized intermediaries for linking to defamatory content.[128] The first judicial decisions that applied immunity for linking referred to search engines, which produce a list of hyperlinks in response to users' search queries.[129] Later on, courts extended the immunity to intermediaries that operated networks of websites, which were linked to each other by determining that a link is not a publication; rather, it is simply a means of access to the referenced article.[130] Many courts concluded that displaying a hyperlink is not the same as restating the allegedly defamatory material.[131] In *Shrader v. Bidding-*

125. No. 13-2382(JAP), 2014 WL 3778261 (D.N.J. July 31, 2014) *aff'd*, 612 F. App'x 90 (3d Cir. 2015).

126. *Id.* at *6. The service itself describes how it works: "Search predictions are generated by an algorithm, automatically without human involvement. The algorithm is: Based on several factors, like how often others have search for a term. Designed to show the range of information on the web. You might see predictions related to a variety of popular topics." *Search Using Autocomplete*, GOOGLE, https://support.google.com/websearch/answer/106230?hl=en [https://perma.cc/EB7U-4F6F].

127. *See Obado*, 2014 WL 3778261, at *6. On "autocomplete" and defamation, see Michael L. Smith, Essay, *Search Engine Liability for Autocomplete Defamation: Combating the Power of Suggestion*, 13 U. ILL. J.L. TECH. & POL'Y 313, 326–36 (2013); see also Arwa Mahdawi, *Google's Autocomplete Spells Out Our Darkest Thoughts*, GUARDIAN (Oct. 22, 2013, 5:39 PM), https://www.theguardian.com/commentisfree/2013/oct/22/google-autocomplete-unwomen-ad-discrimination-algorithms [https://perma.cc/H6VT-2SXP], *cited in* Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1034 (2017) (reviewing FRANK PASQUALE, THE BLACK BOX SOCIETY (2015)) (focusing on a related context of racist completion results and explaining that the autocomplete function reflects hidden biases that exist in society and reflects "questions that large numbers of people are asking 'when they think no-one is looking'"). *See generally* Kacy Popyer, Note, *CACHE-22: The Fine Line Between Information and Defamation in Google's Autocomplete Function,* 34 CARDOZO ARTS & ENT. L.J. 835 (2016) (arguing that intermediaries should not bear liability for defamatory completion).

128. *See, e.g.,* Ardia, *supra* note 109, at 462 (citing Donato v. Moldow, 865 A.2d 711, 725–26 (N.J. Super. Ct. App. Div. 2005)).

129. *See* Parker v. Google, Inc., 422 F. Supp. 2d 492, 501 (E.D. Pa. 2006), *aff'd*, 242 F. App'x 833 (3d Cir. 2007); *see also* Getachew v. Google, Inc., 491 F. App'x 923, 926 (10th Cir. 2012); Mmubango v. Google, Inc., No. 12-1300, 2013 WL 664231, at *3 (E.D. Pa. Feb. 22, 2013).

130. *See, e.g.*, *In re* Phila. Newspapers, LLC, 690 F.3d 161, 175 (3d Cir. 2012); Salyer v. S. Poverty Law Ctr., Inc., 701 F. Supp. 2d 912, 916–18 (W.D. Ky. 2009); Life Designs Ranch, Inc. v. Sommer, 364 P.3d 129, 138 (Wash. Ct. App. 2015).

131. *See, e.g.*, *In re* Phila. Newspapers, LLC, 690 F.3d at 175; Bittman v. Fox, No. 14 C 08191, 2016 WL 2851566, at *6 (N.D. Ill. May 16, 2016); Life Designs Ranch, Inc. v. Sommer,

*er*[132] the court went further and determined that the CDA's immunity applies even if the link directed users to a specific defamatory post.[133]

*d) Adoption of Defamation*

Liability for adoption of defamation may be a different question. In this regard, judicial decisions are inconsistent, leading to confusion. In *Barrett v. Rosenthal*,[134] the court stated that "[a]t some point, active involvement in the creation of a defamatory Internet posting would expose a defendant to liability as an original source."[135] Following this decision, in *MCW, Inc. v. Badbusinessbureau.com, LLC*,[136] the court held the intermediary responsible for adding titles to user-generated defamatory posts, since by doing so the intermediary participated in the process of "developing information."[137] In *Diamond Ranch Academy, Inc. v. Filer*,[138] the defendant summarized and aggregated complaints written by third parties about the plaintiff on her website.[139] The defendant did not explicitly or implicitly clarify that she was quoting others.[140] In addition, she added her own comments.[141] The court explained that the defendant was not entitled to § 230 immunity for the statements she authored.[142] In addition, it implied that the lack of reference to third parties could result in loss of immunity.[143]

---

364 P.3d at 138 (quoting Doctor's Data, Inc. v. Barrett, 170 F. Supp. 3d 1087, 1137 (N.D. Ill. 2016)).

132. No. 10-cv-01881-REB-MJW, 2012 WL 976032 (D. Colo. Feb. 17, 2012).

133. *Id.* at *9.

134. 146 P.3d 510 (Cal. 2006).

135. *Id.* at 527 n.19.

136. No. Civ.A.3:02-CV-2727-G, 2004 WL 833595 (N.D. Tex. 2004).

137. *Id.* at *10; *see also* Whitney Info. Network, Inc. v. Xcentric Ventures, LLC, No. 2:04CV47FTM33SPC, 2005 WL 1677256 (M.D. Fla. July 14, 2005). The court in *Whitney Information Network* differentiated between intermediaries that add defamatory headlines to content, and users that select headlines out of the intermediaries' suggestions. *See also* Morley, *supra* note 55, at 23.

138. No. 2:14-CV-751-TC, 2016 WL 633351 (D. Utah Feb. 17, 2016).

139. *Id.* at *2.

140. *Id.* at *21.

141. *Id.*

142. *Id.* at *22 ("DRA's allegations focus on publications that are, at a minimum, summaries of third-party statements with Ms. Filer's editorial comments and her own opinion. Ms. Filer is not entitled to the exemption in the CDA for statements in articles she authored."); *but see* Jeff Kosseff, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution Over Two Decades*, 18 COLUM. SCI. & TECH. L. REV. 1, 27–28 (2016).

143. *Diamond*, 2016 WL 633351, at *22; Eric Goldman, *Section 230 Doesn't Protect Summaries of Third Party Remarks — Diamond Ranch Academy v. Filer*, TECH. & MARKETING L. BLOG (Feb. 19, 2016), http://blog.ericgoldman.org/archives/2016/02/section-230-doesnt-protect-summaries-of-third-party-remarks-diamond-ranch-academy-v-filer.htm [https://perma.cc/U8CF-7ERD]; *see also* Kosseff, *supra* note 142 (criticizing the court's perplexing reasoning).

However, in similar cases, other courts have reached different conclusions.[144] In *Vazquez v. Buhl*,[145] the court extended the immunity to an editor of a website who linked to articles containing defamation, referred to them as a "big reveal" and urged viewers to read them.[146] The court summarized that it is immaterial whether the defendant amplified or endorsed defamation because he did not play a role in its composition.[147]

A major legal battle on adoption of defamation by a website occurred in *Jones v. Dirty World*.[148] In this case, the intermediary "thedirty.com" added brief nasty remarks and tags to users' posts and disseminated the selected submissions.[149] These posts offended many individuals including Sara Jones, the plaintiff.[150] The lower court decided not to grant immunity to the intermediary because it developed, invited, encouraged, and adopted defamatory content.[151] On appeal, the Sixth Circuit applied a narrow interpretation of § 230, concluding that adoption or ratification theory abuses the concept of responsibility.[152]

When the court strips an intermediary of its § 230 immunity, defenses or other privileges may still exempt it from liability. For example, in *Seaton v. TripAdvisor,*[153] the intermediary of a review website

---

144. *See, e.g.*, Torati v. Hodak, No. 155979/12, 2014 WL 2620345, at *4 (N.Y. Sup. Ct. June 11, 2014). The intermediary added headings at the beginning of a posted complaint, including the logo, "Don't let them get away with it — let the truth be known." *Id.* at *3. The court applied the immunity concluding that this practice is "well within a publisher's traditional editorial functions." *Id.* (quoting Shiamili v. Real Estate Grp. of N.Y., Inc. 952 N.E. 1011, 1019 (N.Y. 2011)).

145. No. FSTCV126012693S, 2012 WL 3641581 (Conn. Super. Ct. July 17, 2012).

146. *Id.* at *1, *4 ("Although NBCUniversal added an introduction leading readers to the defamatory statements, [it] did not materially create or develop any of the allegedly defamatory statements.").

147. *Id.* at *4. In this instance, commentators warned that linking to defamatory content and affirmatively adopting it may result in applying liability. *See* Sheri Wardwell, Note, *Communications Decency Act Provides No Safe Harbor Against Antifraud Liability for Hyperlinks to Third-Party Content Under the Securities Exchange Act*, 6 WASH. J.L. TECH. & ARTS 49 (2010); Kreimer, *supra* note 2, at 98.

148. *See* Jones v. Dirty World Entm't Recordings, LLC (*Jones I*), 840 F. Supp. 2d 1008 (E.D. Ky. 2012); Jones v. Dirty World Entm't Recordings, LLC (*Jones II*), 965 F. Supp. 2d 818 (E.D. Ky. 2013); Jones v. Dirty World Entm't Recordings, LLC (*Jones III*), 755 F.3d 398 (6th Cir. 2014); *see also* Elizabeth M. Jaffe, *Imposing a Duty in an Online World: Holding the Web Host Liable for Cyberbullying*, 35 HASTINGS COMM. & ENT. L.J. 277, 287 (2013) (discussing *Jones I*).

149. *See Jones I*, 840 F. Supp. 2d at 1009–10.

150. *See id.*

151. *See Jones I*, 840 F. Supp. 2d at 1012; *Jones II*, 965 F. Supp. 2d at 820.

152. *See Jones III* 755 F.3d at 415. Scholars have criticized this case as granting too much defense for bad faith moderation. *See* Grimmelmann, *Virtues*, *supra* note 6, at 105; Danielle Citron & Benjamin Wittes, *The Internet Will not Break Denying Bad Samaritans § 230 Immunity*, FORDHAM L. REV. 401 ,417 (2017) ("[T]o immunize it would turn the notion of the Good Samaritan on its head since its interests are aligned with the abusers.").

153. 3:11-cv-549, 2012 WL 3637394 (E.D. Tenn. Aug. 22, 2012).

compiled its user ratings into an annual ranking of the top 10 "dirtiest hotels."[154] The list was based on users' ratings, and included selective quotes. It ranked ten hotels; with the number "one" designated as the "dirtiest hotel" and was later disseminated to different media outlets.[155] TripAdvisor stated that the list was factual and trustworthy.[156]

The plaintiff, Grand Resort Hotel, was on the top of the list and featured as "the dirtiest hotel in America."[157] It sued TripAdvisor. The hotel claimed that by compiling a list of the "dirtiest hotels" with actual numerical rankings and comments, which suggested that the rankings were verifiable, TripAdvisor defamed the hotel.[158] In addition, the plaintiff argued that TripAdvisor used a "flawed methodology" because the percentage of negative reviews attributed to each of the ten hotels on the list did not correlate to the hotels' rank within the list.[159]

The district court focused on TripAdvisor's direct liability for compiling users' ratings into a list, characterizing the hotels as "the dirtiest" and presenting users' opinions as facts.[160] The court did not apply the immunity in § 230, but nonetheless exempted TripAdvisor from liability.[161] It explained that the list of "2011 dirtiest hotels" was not defamatory because the list employed hyperbolic language and did not communicate anything more than the opinions of TripAdvisor's users.[162] Furthermore, even if TripAdvisor employed a "flawed methodology" in creating the list, there was no cause for defamation because TripAdvisor's method was inherently subjective in nature and therefore protected.[163] The district court granted TripAdvisor's motion to dismiss.[164] On the appeal, the Sixth Circuit affirmed this judgment.[165]

In this case, the intermediary mixed its content with content generated by users. It redistributed the "level of dirt" ranking in a manner that did not directly reflect the relative level of negative ratings from the users.

---

154. *Id.* at *2.

155. *Id.*

156. *See id.*

157. *Id.*

158. *See id.* at *4.

159. *Id.* at *5 ("The Plaintiff alleges that the Defendant has 'a flawed methodology or arbitrary nature' that 'reskless[ly] [sic] or negligent[ly] . . . resulted in damages to the Plaintiff and his business.'").

160. *Id.* at *7.

161. *Id.* ("It does not appear to the Court that a reasonable person could believe that TripAdvisor's article reflected anything more than the opinions of TripAdvisor's millions of online users.").

162. *Id.* (internal emphasis omitted).

163. *See id.*

164. *See id.* at *1.

165. Seaton v. TripAdvisor, LLC, 728 F.3d 592 (6th. Cir. 2013).

One can challenge the court's decision that a reasonable person would understand TripAdvisor's list as an opinion.[166] Scholars argue that the court missed the point and the rankings can be viewed as a fact.[167] Moreover, "the court's reasoning could be misconstrued by allowing speakers to avoid defamation liability by hiding behind flawed algorithms."[168] Even Prof. Eric Goldman, one of the chief advocates of § 230's immunity, criticized the court's reasoning, which allows the characterization of clean hotels as dirty with impunity.[169]

2. Europe

The E-Commerce Directive dictates the framework for intermediaries' liability in Europe.[170] The directive does not impose a general duty of care on intermediaries to monitor content on their websites. The intermediaries are insulated from liability, provided that they remain passive facilitators and react upon knowledge of illegal content. This knowledge-based safe haven protects intermediaries whose role is "merely technical, automatic and passive,"[171] but does not shield intermediaries that play an active role. The directive is somewhat dated and its classification might no longer be comprehensive. Many intermediaries may not be considered "hosts" at all.[172] In such a case, the

166. *See, e.g.*, Demetriades v. Yelp, Inc., 228 Cal. Rptr. 3d 131 (Cal. Ct. App. 2014) (refusing to hold similar statements of an intermediary on trustworthiness of users' content as an opinion and remanding the case to the district court).

167. *See* RonNell Anderson Jones & Lyrissa Barnett Lidsky*, On Reasonable Readers and Unreasonable Speakers: Libel in a Networked World*, 23 VA. J. SOC. POL'Y & L. 155, 173 (2016).

168. *See id.*

169. *See* Eric Goldman, *TripAdvisor's "Dirtiest Hotels" List Isn't Defamatory-Seaton v. TripAdvisor*, TECH. & MARKETING. L. BLOG (Aug. 30, 2013), http://blog.ericgoldman.org/archives/2013/08/tripadvisors_di.htm [https://perma.cc/3RE5-2R2R] (agreeing with the result, but disapproving of the reasoning). Recently, in *Roca Labs, Inc. v. Consumer Opinion Corp*., the court exempted the intermediary "pissedconsumer.com" from liability even though it showed every post as a complaint regardless of whether a third party was "pissed" or "pleased." F. Supp. 3d 1311, 1323 (M.D. Fla. 2015). Thus, it legitimized flawed methodology and promoted distortions.

170. Directive 2000/31, 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, 2000 O.J. (L 178) I (EC); *see* Joris van Hoboken, *The Legal Space For Innovative Ordering: Update Selection Intermediary Liability in the EU*, 13 INT'L J. COMM. L. & POL'Y 49 (2009); Broder Kleinschmidt, *An International Comparison of ISP's Liabilities for Unlawful Third Party Content*, 18(4) INT'L J.L. & INFO. TECH. 332, 345–348 (2010).

171. *See* Joined Cases C-236/08 to C-238/08, Google France SARL, Google, Inc. v. Louis Vuitton Malletier SA et al., 2010 E.C.R. III-114. ("[I]n order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores.").

172. *See* Peggy Valcke & Marieke Lenaerts, *Who's Author, Editor and Publisher in UGC Content: Applying Traditional Media Concepts to UGC Providers*, 24 INT'L REV. L.

directive does not apply and an intermediary may not be considered "passive." As a result, the court may hold it responsible even for full dissemination of defamatory content.[173]

Accordingly, an intermediary that selects content for dissemination will not be considered as a passive transmitter in European courts. It controls the dissemination and is more likely to have knowledge of the content it disseminates. This knowledge increases the likelihood to bear liability for selective dissemination.

Judicial decisions regarding selective dissemination following users' signals are inconsistent. This is frequently discussed in the context of Google's liability for completing search queries by an "autocomplete" system.[174] Different courts in Europe have reached contradicting results regarding Google's liability for defamatory completion suggestions.[175]

As for linking, some countries offer specific liability exemptions to intermediaries for linking to defamatory content; others have out-

---

COMPUTERS & TECH. 119, 126 (2010). The scope of liability is unclear, leading to contradicting decisions. *Compare* Delfi AS v. Estonia, 2013 Eur. Ct. H.R. at 32 *and* Delfi AS v. Estonia, 2015 Eur. Ct. H.R. at 68 *with* Magyar Tartalomszolgáltatók Egyesülete Index.hu Zrt v. Hungary, 2016 Eur. Ct. H.R. at 22.

173. *See* Alastair Mullis & Andrew Scott, *Tilting at Windmills: the Defamation Act 2013,* 77 (1) MOD. L. REV. 87 (2014) (outlining the "notice-and-takedown regime of § 5 of the English Defamation Act of 2013). Accordingly, a website operator who fails to respond loses this defense. Yet, the defense applies when the operator shows that he did not post the statement on the website. Intermediaries' liability under this act is residual to the liability of the person who posted the statement. However, when the intermediary disseminates users' defamatory content, the victim may file an action against both the speaker and the intermediary. Ronen Perry & Tal Z. Zarsky*, Liability for Online Anonymous Speech: Comparative and Economic Analyses*, 5 J. EUR. TORT L. 205, 225 (2014). For an abridged, restricted version, see Ronen Perry & Tal Z. Zarsky, *Who Should Be Liable for Online Anonymous Defamation?*, 82 U. CHI. L. REV. DIALOGUE 162 (2015); COLLINS, *supra* note 10, at ¶ 2.104–2.114.

174. On "autocomplete," see *Search Using Autocomplete*, *supra* note 126 and accompanying text.

175. *See* Stavroula Karapapa & Maurizio Borghi, *Search Engine Liability for Autocomplete Suggestions: Personality, Privacy and the Power of the Algorithm*, 23 INT. J. L. INFO. TECH. 261, 261 n.1 (2015). *Compare* Bundesgerichtshof (BGH), (May 14, 2013), VI ZR 269/12, published in Versicherungsrecht (2013) 771, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=6376b91f5488494d9704d48a4b4ad29d&nr=64163&pos=2&anz=3 [https://perma.cc/V4JT-GCA7] (a German court held that Google is responsible for not filtering offensive completion suggestions, like when terms such as "Scientology" or "fraud" are adding to the plaintiff's name in the search tab), *and* Corinna Coors, *Reputations at Stake: The German Federal Court's Decision Concerning Google's Liability for Autocomplete Suggestions in the International Context*, 5 J. MEDIA L. 322 (2013), *and* David Mayer*, Google Loses Autocomplete Defamation Case in Italy*, ZDNET (Apr. 5, 2011) http://www.zdnet.com/article/google-loses-autocomplete-defamation-case-in-italy/ [https://perma.cc/C87J-FSRB], *with* Marco Bellezza & Frederica De Santis, *Google not Liable for Autocomplete and Related Searches Results, Italian Court Rules*, SES (Apr. 5, 2013) http://www.portolano.it/wp-content/uploads/2013/04/Google-not-liable-for-Autocomplete-and-Related-Searches-results-Italian-court-rules-Rapid-TV-News.pdf [https://perma.cc/82YM-2HAS].

lined a "notice-and-takedown" regime.[176] In spite of what may appear as a clear rule on the books for shielding intermediaries from liability for linking, in practice, judicial decisions remain inconsistent.[177] In a related example, the European Court of Justice ("ECJ") backed the "right to be forgotten"[178] in *Google Spain SL, Google, Inc. v. González.*[179] It ruled that search engines are responsible for search results linking to personal data, which appears on third parties' webpages.[180] The court reached this conclusion by broadly interpreting the term "controller" in Article 2 (b), (d) of the Data Protection directive. According to the decision, search engines should remove links to defamatory or irrelevant content after receiving a data removal request.[181] Yet, the court failed to reconcile this obligation with the safe haven principles of the E-Commerce Directive and the scope of intermediar-

176. *See* Thibault Verbiest et al., *Study on the Liability of Internet Intermediaries,* EUROPA (Nov. 12, 2007). http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf [https://perma.cc/QJ56-W8WM].

177. *See* Lorenzo Cotino Hueso, *The Problem of Liability for Illegal Content in the Web 2.0 and Some Proposals*, 3 PROC. FIRST WORKSHOP L. WEB 2.0. 73, 79 (2009). (comparing cases finding different ranges of liability for linking).

178. This right was represented as one of the "four pillars" of the new Regulation in the EU. *See, e.g.,* European Commission Memoranda MEMO/13/923, *LIBE Committee Vote Backs New EU Date Protection Rules* (Oct. 22, 2013); Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 162 (2012); Ignacio Cofone, *Google v. Spain: A Right to Be Forgotten*?, 15 CHI.-KENT J. INT'L & COMP. L. 1, 2 (2015); Cooper Mitchell-Rekurt, *Search Engine Liability Under the LIBE Data Regulation Proposal: Interpreting Third Party Responsibilities as Informed by Google Spain,* 45 GEO. J. INT'L L. 861 (2014); Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012).

179. *See* Case C-131/12, Google Spain SL, Google, Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=15206 [https://perma.cc/7PF2-W2DM] ("[T]he activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it, storing it and making it available to internet users . . . must be classified as 'processing of personal data' within the meaning of Article 2(b) [of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data] . . . and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing within the meaning of Article 2 (d)."); *see also* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 27 (2016); Cofone, *supra* note 178, at 23; Ioannis Iglezakis, *The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?*, SSRN (2014) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323 [https://perma.cc/423T-74H5]; Javier Aparicio Salom, *A Third Party to Whom Data Are Disclosed: A Third Group Among Those Processing Data,* 4 INT'L DATA PRIVACY L. 177, 183 n.20 (2014), http://idpl.oxfordjournals.org/content/early/2014/06/11/idpl.ipu011.full [https://perma.cc/48PC-QG4S].

180. *See* Case C-131/12.

181. *See* Anupan Chander & Uyen Pe Le*, Free Speech*, 100 IOWA L. REV. 501, 541 (2015) (complying with the ruling, "Google offered EU citizens the ability to file data removal requests. Within 24 hours the search engine received 'right to be forgotten' requests from at least 12,000 individuals."). *But see* Michael J. Kelly & David Satola, *The Right to be Forgotten*, 2017 ILL. L. REV. 1, 12 (2017) (revealing that Google rejects about 50% of the removal requests).

ies' liability remains unclear. Although a link to defamatory content might have been covered by the safe haven ensured in the E-Commerce Directive, the identification of search engines as 'controllers' might imply that they are not neutral and passive enough to be eligible for the safe harbors' protection.[182] This ruling may also affect the scope of websites' liability for linking.[183] In addition, it may affect their liability for autocomplete suggestions on private individuals.[184] Furthermore, when the General Data Protection Regulation (GDPR) comes into force in 2018,[185] data controllers will have to delete information on EU citizens from the internet under certain criteria This regulation may apply to online websites. [186]

European courts may hold intermediaries responsible for adopting defamation. Yet, in some cases, intermediaries may come under domestic law's defenses or privileges as speakers and may not bear liability.[187]

3. Canada

Canada does not have a legal framework like the EU Directive.[188] Therefore, content providers do not benefit from any safe haven. Liability is regulated by common law and the rules applying to distributors.[189] Accordingly, the "innocent dissemination" defense protects those who play a secondary role in the chain of distribution.[190] This

182. *See* Miquel Peguera, *The Shaky Ground of the Right to Be Delisted*, 18 VAND. J. ENT. & TECH. L. 507, 544 (2016).

183. *See* Ravi Antani*, The Resistance of Memory: Could the European Union's Right to be Forgotten Exist in the United States*? 30 BERKELEY TECH. L.J. 1173, 1176 (2015).

("[W]hile this ruling defined search engine operators . . . as data controllers because of their respective web search tools, it is possible that in the future other internet entities, like Facebook, could also fall into the category of 'data controllers' and be subject to similar rules.").

184. *See* Karapapa & Borghi, *supra* note 175, at 261, 263 ("[M]any requests for removal of suggestions including private individuals' information will be successful on the basis of EU data protection law . . . . However, no general obligation can be assumed for suggestions related to companies' or public persons' names . . . .").

185. *See* Peguera *supra* note 182, at 557.

186. *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 11 COM Art. 17 (Jan. 25, 2012). The last version was issued in April, 2016. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). 59 OFF. J. E.U. 1 (2016).

187. *See* COLLINS, *supra* note 10, at ¶ 1.41–1.47.

188. *See* POTTS, *supra* note 33, at 314.

189. *See* Corey Omer, Note, *Intermediary Liability for Harmful Speech: Lessons from Abroad*, 28 HARV. J.L. & TECH. 289, 305–06 (2014).

190. On the defense of "innocent dissemination" see POTTS, *supra* note 33, at ch. 18. *See also* Iris Fischer & Adam Lazier*, Crookes v. Newton: The Supreme Court of Canada Brings Libel Law into the Internet Age*, 50 ALTA. L. REV. 205, 212 (2012); Mitchell Drucker, Note, *Cana-*

defense absolves disseminators from liability provided they had no knowledge of the defamatory nature of the statement, and that their failure to detect the defamatory content was not due to negligence; furthermore, the burden of proof lies on the shoulders of the defendant.[191] The type of dissemination influences the intermediary's knowledge of defamation and has an important role in deciding its liability.

Courts are likely to avoid applying the innocent disseminator defense when an intermediary selectively disseminates specific defamatory content items or adopts defamation.[192] Selecting or adopting defamation may indicate prior knowledge of the intermediary, or at least lead to the conclusion that it should have known about the defamatory content. In contrast, courts are likely to conclude that the intermediary is an innocent disseminator when it follows users' signals, such as voting systems, or an autocomplete system that completes users' searches automatically.[193] In other words, it does not have knowledge of users' choices, and should not be aware of them.[194] This defense is likely to apply to full dissemination, in circumstances where the intermediary should not be aware of the content disseminated.[195]

Courts in Canada debated whether to impose liability on intermediaries for linking to defamation. In *Crookes v. Newton*,[196] the plaintiff sued an intermediary who posted shallow and deep links to other websites, which contained defamatory content about him. The plaintiff claimed that by using links, the intermediary published defamation.[197] The judge concluded that links are analogous to footnotes, which di-

---

*dian v. American Defamation Law: What Can We Learn from Hyperlinks*, 38 CAN.-U.S. L.J. 141, 157 (2013).

191. *See* POTTS, *supra* note 33, at ch. 18.

192. *See* Hemming v. Newton, 2006 B.C.S.C. No. 1748, para. 13 ("The defence of innocent dissemination is recognized in Canadian law, and has been applied in circumstances where the defendant was not the originator of the alleged defamation but simply someone who facilitated its public dissemination without being aware of the content . . ."). Selection of content for dissemination is likely to indicate the intermediary's knowledge of the content and preclude the application of the innocent dissemination defense, unless there are special circumstances such as automatic dissemination. *See id.*

193. On the related context of autocomplete, see Rolfe Winkler, *Should Google Have to Scrub Its 'Autocomplete' Suggestions?*, WALL ST. J. (Aug. 7, 2014), https://blogs.wsj.com/digits/2014/08/06/should-google-have-to-scrub-its-autocomplete-suggestions/ (last visited Dec. 20, 2017).

194. *See* Soc'y of Composers, Authors & Music Publishers of Can. v. Canadian Ass'n. of Internet Providers, 2004 SCC 45, [2004] 2 S.C.R. 427, 464 ¶ 89 (explaining the logic behind the innocent disseminator defense).

195. For example, where the intermediary tracks updates automatically by using RSS protocol.

196. Crookes v. Wikimedia Found., Inc. [2008] B.C.S.C. No. 1424 (Can.) (The full name of the case is Crookes v. Wikimedia Foundation, Inc. Anonymous #1, 2, 3 ,4, 5, & 6, Domains by Proxy, Inc. and Jon Newton).

197. *Id.,* at ¶ 6 ("The plaintiffs' case is that posting hyperlinks to websites containing defamatory material constitutes publication of the defamatory words in the latter websites.").

rect to another source without repeating it; thus, they are not considered a publication.[198] On appeal, the majority upheld the decision.[199] Yet, in both decisions, the courts left the possibility open for finding a defendant responsible as a publisher if he adopted the content of the link.[200]

The case reached the Supreme Court of Canada, who dismissed the appeal.[201] The decision of the majority, written by Justice Abella and joined by five other Justices, held that reference to an article containing defamation is not a publication. In order for a defendant to be liable, he must repeat the defamatory content from the linked website.[202] Justices McLachlin and Fish expressed reservations regarding the adoption or endorsement of defamation.[203] In their view, a link can be viewed as a publication if the text that includes the hyperlink adopts or endorses the content it links to.[204] Justice Deschamps preferred for "the Court to hold that in Canadian law, a reference to defamatory content can satisfy the requirements of the first component of publication if it makes the defamatory information *readily available*."[205] According to this view, a deep link that leads directly to the defamatory content is a publication.[206]

In *Niemela v. Malamas*,[207] the Supreme Court of British Columbia debated whether a search engine could be considered a publisher of defamation when it showed "snippets" in its search results.[208] After considering *Crookes v. Newton*, the court held that providing a hyperlink does not constitute publication.[209] As for a snippet that repeats words from the hyperlinked article, the court held that Google might come under the innocent dissemination defense.[210] Yet, the court did not decide the issue of whether Google is responsible as the publisher of snippets after having received notice that the content is defamatory.[211] In this case it was the method of dissemination which led the court to apply the innocent disseminator defense. Thus, due to the ab-

198. *See generally id.*
199. *See* Crookes v. Newton, [2009] B.C.C.A. 392 (Can.).
200. *See id.* at ¶¶ 89–90; Crookes v. Newton B.C.S.C. No. 1424 at ¶ 34.
201. *See* Crookes v. Newton, 2011 SCC 47, [2011] 3 S.C.R. 269 (Can.).
202. *See id.* at ¶ 42.
203. *See id.* at ¶ 46–52.
204. *See id.* at ¶ 50.
205. *Id.* at ¶ 59.
206. *Id.* at ¶ 99. In this case, Justice Deschamps concluded that Newton escaped liability because there was no proof anyone actually followed the link in question. *See* Fischer & Lazier, *supra* note 190, at 210.
207. [2015] B.C.S.C. 1024 No. 24 (Can. B.C.).
208. *Id.* A snippet repeats words from the hyperlinked article.
209. *See id.* at ¶ 92.
210. *See id.* at ¶ 94.
211. *See id.* at ¶ 108 ("I emphasize that I have not been asked in this case to consider whether Google could be a publisher of snippets and search results after notice of defamatory content").

sence of knowledge of the dissemination of defamation, the court did not impose liability but left the door open to do so in cases where the publisher was given notice.

To sum up: courts across the world are struggling to define the proper scope of liability. They are unsure when intermediaries should be liable for disseminating users' defamatory content and when they should not. Their decision should be viewed from a broader perspective of policy considerations, which this Article examines in the following sections.

### *E. Normative Considerations for Liability*

Liability of intermediaries rests at the junction of several branches of law. It balances constitutional rights and tort considerations. In addition, the technological context involves special considerations. Identifying the interests at stake and finding the right balance between them is a difficult judgment call, albeit a crucial one.

Different types of republication involve different actors and require nuanced examination. This Article will focus on two central situations: (1) Dissemination of users' content by the intermediary, and (2) Dissemination following users' requests or signals, as demonstrated in the flowchart below.

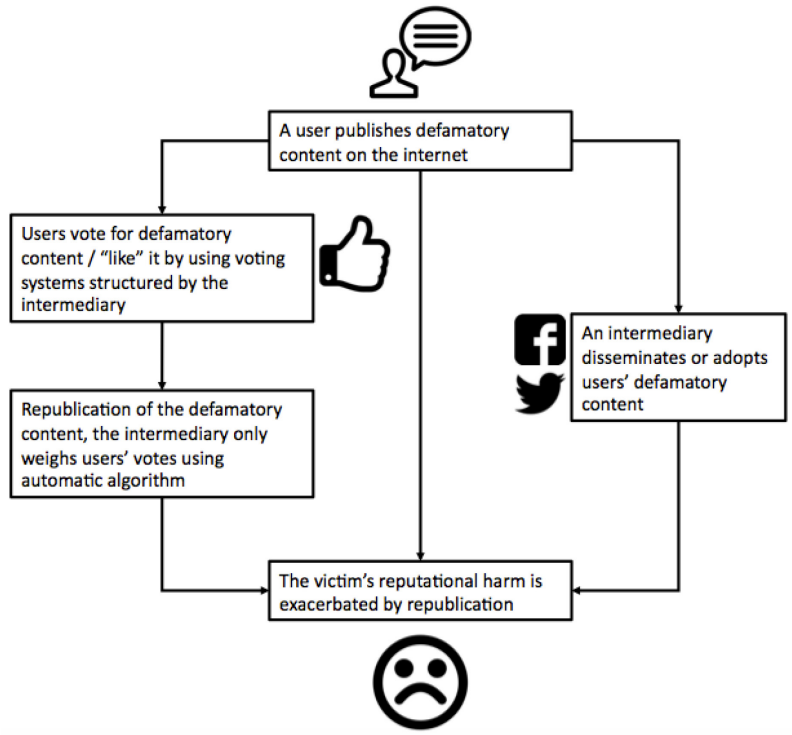


Figure 1: A Flowchart Describing How Content Posted by Site Users Can Lead to Defamation.

1. Constitutional Balance and the Base of Defamation Law

The civil rights at stake in defamation law are human dignity, reputation interests, and freedom of speech. The balance is between the reputation of victims and free speech. Liability for defamation protects the basic elements of a person's status, dignity, and reputation as a member of society.[212] The other consideration is the right to free speech. The purpose of this right is to shield against government censorship[213] and ensure the audience's right to receive information.[214] However, courts and scholars have developed numerous theories about

212. *See* Peter G. Danchin, *Defaming Muhammad: Dignity, Harm, and Incitement to Religious Hatred*, 2 DUKE F.L. & SOC. CHANGE 5, 17 (2010).

213. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 10 (2015) ("Courts have interpreted the First Amendment broadly to prevent the government from censoring our speech, pushing us directly for its content, or creating legal rules that allow us to be sued for speaking the truth.").

214. *See* Susan Nevelow Mart, *The Right to Receive Information*, 95 L. LIBR. J. 175, 175 (2003) ("The right to receive information has evolved from its early place as a necessary corollary to the right of free speech . . ."); *see also* Martin v. Struthers, 319 U.S. 141, 143 (1943).

why free speech should receive special protection.[215] The first rationale explains that it promotes individual autonomy and self-fulfillment. It enables the self-determination of an individual.[216] The second rationale for protecting free speech is the search for truth. Free speech assures that every expression enters the marketplace of ideas.[217] The third rationale is based on the understanding that free speech is crucial for maintaining a democracy. It is required to assure the effectiveness of the democratic process by informing the governed of the acts of government and guaranteeing that policy is presented to the public intelligently.[218] Contemporary theories on democracy focus on protecting and promoting a democratic participatory culture. Freedom of speech is required to assure an individual's ability to participate in the production and distribution of culture.[219] The right balance must be struck between the benefits of free expression and its potential harm to reputation.

In the digital age, intermediaries can easily disseminate users' defamatory content and increase its circulation. Thus, they can influence the attention, credibility, and magnitude given to it. Furthermore, dissemination of user-generated content may increase the likelihood that more users will spread the content.[220] Consequently, reputational harm is exacerbated. One may argue that the law should impose liability on intermediaries for disseminating user-generated content. Accordingly, liability can be the key for mitigating harm and protecting civil rights of victims.

Dissemination of content promotes freedom of expression and is based on constitutional rights.[221] It promotes individuals' autonomy. The disseminator who repeats others can find self-fulfillment and can also enhance the autonomy of the original speaker by supporting his way of life. It promotes a vibrant market of ideas, by increasing access

---

215. *See* RICHARDS, *supra* note 213, at 10 (reviewing influential theories which lay out justifications for the right to free speech).

216. *See* Joseph Raz, *Free Expression and Personal Identification,* 11 OXFORD J. LEGAL STUD. 303, 312–14 (1991).

217. *See* JOHN STUART MILL, ON LIBERTY 5–9 (1869); JOHN MILTON, AREOPAGITICA: A SPEECH FOR THE LIBERTY OF UNLICENSED PRINTING (1958); *see also* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting); RICHARDS, *supra* note 213, at 35; Michael D. Birnhack, *More or Better? Shaping the Public Domain, in* THE FUTURE OF THE PUBLIC DOMAIN 59, 68 (Lucy M.C.R. Guibault & P. Bernt Hugenholtz eds., 2006).

218. *See* ALEXANDER MEIKLEJOHN: FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1965); Birnhack, *supra* note 216, at 71.

219. *See* Jack Balkin, *Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 3 (2004); Birnhack, *supra* note 217, at 71–72.

220. *See generally* SUNSTEIN, CONSPIRACY, *supra* note 25.

221. *See* ERIK BRYNJOLFSSON & ANDREW MCAFEE: THE SECOND MACHINE AGE 126–130 (2014); Birnhack, *supra* note 217, at 71. *See* Rebecca Tushnet, *Copy this Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It,* 114 YALE L.J. 535, 565 (2004).

to content.[222] It also promotes democracy by advancing content to public awareness and enabling a dialogue on public issues.[223] In addition, by enhancing valuable dialogue on information from many sources, dissemination protects democratic participatory culture. The liability regime governing cyberspace affects free speech.[224] Imposing liability on intermediaries for dissemination of user-generated defamatory content may lead to a "chilling effect" and impair the open markets of information.[225] This chilling effect might not be as extensive as the potential effect of hosts' liability, because the intermediary decides whether and how to reproduce users' content; yet the concern remains.[226] Imposing liability for dissemination will curtail the availability and variety of content and hinder the benefits of free speech.

However, an in-depth examination reveals that not all types of dissemination promote free speech. In some cases, immunity may actually undermine free speech and thus not strike the right balance between fundamental rights.[227]

As for dissemination by an intermediary, we should differentiate between full dissemination and other types of reproduction. Full dissemination and regular linking to content enhance the availability of information and promote free speech. In such cases, immunity is necessary for preventing a disproportionate chilling effect. In contrast, when the intermediary selectively disseminates defamation or adopts it, the intermediary does not promote free speech, but rather undermines it. First, selective dissemination or adoption of defamation can impair the autonomy of the author who published the content because it changes the context in which the original content was created and it undermines the author's control over the content.[228] Second, by selecting to disseminate defamation, or adopting it, the intermediary exacerbates the potential harm. Due to the centrality of intermediaries, in comparison to the average user, the process that underlines the marketplace of ideas may work poorly and competition among ideas will

---

222. *See* Sanchez, *supra* note 63, at 314–16. ("The immense public dialogue opened by online [dissemination], which allows discussions at great speed and depth on the issues of the day, such dialogue allows the public to gain a better understanding of issues and ascertain the truth . . . .").

223. *See* Dan Laidman, Note, *When the Slander is the Story: The Neutral Reportage Privilege in Theory and Practice*, 17 UCLA ENT. L. REV. 74, 99–100 (2010) (noting that the democratic rationale supports repetition only when both "wise" and "unwise" ideas are able to be heard).

224. *See* Chander & Le, *supra* note 103, at 524.

225. *See* Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 304 (2011).

226. On host liability in comparison to disseminators' liability, see *id.*

227. *See* SUNSTEIN, RUMORS *supra* note 25, at 71.

228. Even in the case of adoption, the intermediary could mix his speech with the original expression in a manner that is not necessarily in line with the authors' intentions, distorting the expression and impairing the authors' autonomy.

not be effective. As the flow of falsehoods intensifies, many people might focus on falsehoods rather than on truths.[229] Third, selective dissemination or adoption of defamation can impair the democratic process because disseminated lies about state officials could hinder citizens from reaching informed decisions. It also impairs participatory culture by empowering specific speakers and indirectly infringing on the representation and participation of others.[230]

Selective dissemination and adoption of defamation may not promote free speech and may cause severe harm. Therefore, a degree of a chilling effect is necessary and may strike the right balance between fundamental rights. This conclusion applies particularly to intermediaries that select only defamatory speech for dissemination.[231] However, when the intermediary selects multiple items and only some of them are defamatory,[232] the dissemination may promote in-depth dialogue on important issues.

The right to free speech should be weighed against the right to human dignity and consequential effects on reputation. The severity of reputational harm depends largely on the type of dissemination. Full dissemination reproduces content; yet, the dissemination does not amplify the damage of the defamatory content item in particular. In this form of dissemination, the harm is low in comparison to other types of dissemination and the justification for liability weakens. In contrast, selective dissemination exacerbates the proportion of defamation and increases the attention and magnitude ascribed to it. This is even truer when the intermediary adopts defamation. Thus, intermediaries' liability for selective dissemination and adoption of defamation are justified in light of the right to dignity and preservation of reputation.

Disseminating content following users' requests or signals causes the same reputational harm as content dissemination by an intermediary. Yet, the users vote for defamatory content while the intermediary only facilitates the voting system. Imposing liability on intermediaries in this instance may cause a negative incentive for structuring systems that are based on updates and votes on content. Thus, it may cast too heavy a burden on the flow of information and may lead to a disproportionate chilling effect. Due to this reason, an exemption from liability is in order.

Balance must be struck between speakers and the freedom of speech of the victim. Exempting intermediaries from liability allows

---

229. *See* Cass R. Sunstein, *Believing False Rumors*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH AND REPUTATION 91, 92 (Levmore & Nusbaum eds. 2010).

230. *Cf.* Jack M. Balkin, *The First Amendment is an Information Policy*, 41 HOFSTRA L. REV. 1, 24–30 (2013); Jack M. Balkin, *Old School/New School Speech Regulation*, 127 HARV. L. REV. 2296 (2014).

231. *See, e.g.*, Seaton v. TripAdvisor, 728 F.3d 592, 594 (6th Cir. 2013).

232. *See, e.g.*, Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003).

them to disseminate defamation with impunity. It therefore infringes the victims' right to free speech and denies their ability to engage with others on the website that published the defamation. Due to the negativity bias and the weight ascribed to repeated content,[233] dissemination of defamation may lead to self-exclusion, which might suppress public debate.[234] Exempting intermediaries from liability impairs victims' autonomy, and the free market of ideas. Different types of dissemination lead to different degrees of harm to victims' free speech, and therefore standards of liability should not be uniform.[235]

The final balance must be between the rights of intermediaries to free speech and the right of users and third parties. One may argue that imposing liability on intermediaries undermines their free speech. However, it might also be argued that the intermediary is not speaking when it disseminates users' choices or signals.[236] Full dissemination and regular links are only functional and enhance the flow of information. They should not be considered the intermediary's speech. However, when the intermediary selectively disseminates defamation, the content should be considered the intermediary's speech. The same goes for adoption of defamation.[237]

The forms of dissemination that are considered speech of intermediaries focus on specific content. One may argue that intermediaries' liability for specific types of content is content-based regulation, which is subjected to strict scrutiny and may be disqualified by the courts.[238] However, intermediaries cannot have it both ways; they cannot claim to be active speakers when seeking First Amendment protection but also claim to be mere "tools" when facing tort liability.[239] By

---

233. *See generally* Baumeister, *supra* note 29. On the power of repeated hearsay, see DIFONZO & BORDIA *supra* note 24 at 225.

234. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 47–49 (Harvard University Press 2014); Danielle K. Citron, *Cyber Civil Rights,* 89 B.U. L. REV. 61, 97–105 (2009) (describing the potential of falsehoods to exclude individuals from public debate).

235. Full dissemination or regular links keep the defamatory expressions in context and do not particularly emphasize it. Thus, the harm to the victim's free speech is low in comparison to other types of dissemination. In contrast, selective distribution or adoption reinforce defamation and lead to severe harm.

236. *See* Robbins, *supra* note 47, at 130 (a "like" on Facebook is considered the user's expression).

237. On selection of content as speech, see Wu, *Machine Speech*, *supra* note 48, at 1521–1522; *see also* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 636 (1994).

238. *See Turner*, 512 U.S. at 636 (holding that content-based regulation is subject to strict scrutiny). It appears that regulating selective dissemination is content-based and will be subject to strict scrutiny. In contrast, full dissemination, which is content-neutral, is not subject to strict scrutiny.

239. However, some courts have allowed search engines to "have it both ways" by finding them to be speakers when sued over their search results, but mere conduits when sued under tort law. *See* Langdon v. Google, Inc., 474 F. Supp. 2d 622 (D. Del. 2007) (recognizing intermediaries' right of free speech for page-rank and rejecting their liability for optimization); Search King, Inc. v. Google Tech. Inc., No. Civ-02-1457-M, 2003 WL 21464568 (W.D. Okla. May 27, 2003). These rulings have been criticized in literature. *See* Frank Pasquale, *Reforming the Law*

enjoying the right to free speech, they undermine their immunity to civil liability.[240] If the court concludes that an intermediary is liable for defamatory speech, it should treat the intermediary as a speaker, with all the applied privileges.[241]

2. Theories of Tort Law

*a) Corrective Justice*

A central justification for imposing liability is corrective justice. Aristotelian philosophy defines corrective justice as a rectification of harm, wrongfully caused by one person to another, by means of a direct transfer of resources from the injurer to the victim.[242] Accordingly, every particular interaction embodies correlative rights and duties that are imposed on both parties. This deontological non-consequentialist concept focuses on bilateral interactions, which are not reliant on external values.

Corrective justice theorists offer different motives for the duty of rectification including concepts of faults and rights,[243] responsibility,[244] and nonreciprocal risks.[245] Most theorists explain that causation is not enough for imposing liability, but that fault (negligence or moral fault) must exist in order to justify compensation for the harm caused.[246] The reason that causing harm is insufficient for justifying liability can be explained by the theory of nonreciprocal risks. Liability exists when a respondent generates a disproportionately excessive risk of harm, relative to the victim's risk-creating activity. The enti-

---

*of Reputation*, 47 LOY. U. CHI. L.J. 515, 524 (2015); *see also* PASQUALE, THE BLACK BOX SOCIETY, *supra* note 6, at 165; Wu, *Machine Speech*, *supra* note 44, at 1527.

240. *See, e.g.*, James Grimmelmann, *Speech Engines*, 98 MINN. L REV. 868, 871–73 (2014); *see also* RICHARDS, INTELLECTUAL PRIVACY, *supra* note 213, at 87. The fact that specific content is speech does not mean that it is protected speech. Defamation, for instance, is an exception to the reservations regarding content-based restrictions.

241. On defenses and privileges, see *supra* Part III.A.

242. *See* ARISTOTLE, NICOMACHEAN ETHICS 109 (Ross trans., 1980).

243. *See* JULES L. COLEMAN, RISKS AND WRONGS 324–60 (1992).

244. *See* Ernest J. Weinrib, *Correlativity, Personality, and the Emerging Consensus on Corrective Justice,* 2 THEORETICAL INQUIRIES L. 107, 110 (2001) (pointing out that the tort doctrine constructs the relationship by treating the parties as doers and sufferers of the same injustice); *see also* Stephen R. Perry, *The Moral Foundations of Tort Law*, 77 IOWA L. REV. 449, 449 (1992); Stephen R. Perry, *The Impossibility of General Strict Liability*, 1 CAN. J. L. & JURIS. 147, 159–66 (1988).

245. *See generally* George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537, 537–64 (1972).

246. *But see* Richard Epstein, *A Theory of Strict Liability*, 2 J. LEG. STUD. 151, 157 (1973) (arguing that harm itself is sufficient to justify compensation). However, this theory of strict liability which focuses on factual causality has come under criticism. *See, e.g.,* Izhak Englard, *The System Builders: A Critical Appraisal of Modern American Tort Theory,* 9 J. LEGAL STUD. 27, 57–63 (1980).

tlement to recover a loss is handed to all injured parties to the extent the risks imposed on them were nonreciprocal. The goal is to distinguish between a risk that violates individual interests and background risks that must be borne by society. [247]

When an intermediary disseminates or adopts defamatory content, it enhances its availability. One may argue that the intermediary actually causes the harm and should bear liability. Yet, justifying liability under corrective justice theory depends on the type of dissemination. Full dissemination or regular links are merely background risks because these activities aim to facilitate the flow of information, and are an integral part of online platforms. Thus, such an intermediary does not impose nonreciprocal risks. Therefore, it should bear no responsibility for the harm.

When an intermediary selects a number of content items for dissemination and only few of them are defamatory, the normative answer to the question of whether it is a background risk or a nonreciprocal risk is unclear. Selective dissemination of defamatory content in particular and adoption of defamatory content are nonreciprocal risks. Unlike full dissemination, or even an operation of a listserv, selecting only defamatory content for dissemination is not an integral function of an operating platform. These activities aim to enhance the magnitude of defamatory content items in particular. The intermediary bears responsibility for causing the harm, thus it is fair and just to hold it accountable.

When content is disseminated following users' requests or signals, the intermediary only facilitates the voting systems and allows users to select popular or relevant content for dissemination. The users, rather than the intermediary, cause the dissemination. Nevertheless, one may argue that by allowing users to get updates or vote for users' content, the intermediary actually causes the dissemination. Updating and voting systems are an integral part of these operating platforms and therefore should be treated as background risks. These systems do not encourage the dissemination of defamation in particular. Thus, the intermediary should bear no liability for the harm caused by their users.

*b) Efficiency*

This perspective on the purpose of tort law focuses on the maximization of wealth and efficient allocation of risks. In general, it does not take into account deontological considerations.[248] According to

247. *See* Fletcher, *supra* note 245, at 543.

248. *See* Richard A. Posner, *The Ethical and Political Basis of the Efficiency Norm in Common Law Adjudication,* HOFSTRA L. REV. 487, 492 (1980).

this perspective, legal rules aim to incentivize efficient conduct *ex ante* and promote welfare maximization *ex post facto*.[249] This includes the benefits of the activity and the value that third parties gain when information is shared. In this regard, courts should not consider the harm to victims in isolation, but instead conduct all costs and benefits to society as a whole.

When intermediaries disseminate content, they operate independently of the users that published such content. To whom should liability be allocated? Who is the cheapest cost-avoider? The following subsections shall examine whether efficiency considerations support imposing liability on intermediaries for disseminating third party defamatory content,[250] or allowing victims to bear the costs instead. This part will refer to three types of traditional costs associated with efficiency: primary costs of deterrence, secondary costs of loss spreading,[251] and administrative litigation costs. In doing so, the analysis will weigh the cost of liability against its rewards and benefits.

One may argue that imposing liability on intermediaries who disseminate users' defamatory content is efficient. The intermediary is the cheapest cost-avoider because it controls the dissemination, or the implementation of systems that allow updating and voting.[252] Imposing liability on the intermediary could incentivize it to prefer forms of dissemination that do not lead to severe harm. Or, perhaps it would incentivize the intermediaries to develop new technologies and dissemination systems that would be in line with the law.

Waiving intermediaries' liability incentivizes them to disseminate users' content irresponsibly and externalize damage to others. In addition, intermediaries normally have deeper pockets than individual victims, and therefore are better suited to reduce secondary costs by bearing the loss themselves or spreading it among their users. An increase in litigation costs should be expected, but imposing liability on

---

249. *See generally* J. R. Hicks, *The Foundations of Welfare Economics*, 49 ECON. J. 696 (1939); Nicholas Kaldor, *Welfare Propositions of Economics and Interpersonal Comparisons of Utility*, 49 ECON. J. 549 (1939).

250. Spreading defamation about individuals injures their reputation. Thus, it may lead recipients of the defamatory information to mistakenly avoid efficient transactions and impair positive externalities. *See* RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 266–67 (8th ed. 2011).

251. Secondary costs are the costs associated with bearing primary costs. Significant losses borne by one person are more likely to result in secondary losses (arising from the initial damage) than allocating a series of small losses to many people, or large sum of losses to deep-pocketed entities. *See* GUIDO CALABRESI, THE COSTS OF ACCIDENTS 39 (1970).

252. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable,* 14 SUP. CT. ECON. REV. 221, 225 (2006); *see also* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 199–200 (6th ed. 2012); STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 192 (2004). Imposing liability can be efficient even if none of the parties is the cheapest cost-avoider at present, but one of them is likely to be the in the future. *See* Yuval Sinai & Benjamin Shmueli, *Calabresi's and Maimonides's Tort Law Theories*, 26 YALE J.L. & HUMAN. 67 (2014).

intermediaries may be better than the alternative of leaving the victim without a remedy and imposing on him a heavy secondary cost.

However, an in-depth examination reveals that imposing liability on intermediaries may lead to over-deterrence, producing a disproportional chilling effect on speech and hindering positive externalities generated by dissemination of user-generated content. It may also stifle innovation and development of efficient web tools that allow users to focus their attention on relevant content. Liability may also impair connectivity and distort access to digital markets.[253] The loss of dissemination may outweigh the benefits gained by mitigating harm caused by defamation.

Allocating liability to intermediaries may also increase secondary costs. Erroneous assessment of dissemination risks may lead intermediaries to increase their prices disproportionately. Not all intermediaries are born equal, and not all have deep pockets.[254] For example, it would be inefficient to impose liability on noncommercial intermediaries who may in turn quit the market or refrain from investing in online platforms in the first place. Consequently, only large commercial intermediaries would survive and this may impair the diversity of online content and services. As noted above, allocating liability to intermediaries would lead to an increase in legal action and administrative costs. The costs of complex litigation may lead intermediaries to limit their activities to suboptimal levels in order to reduce their exposure to liability.[255] Cost-benefit analysis leads to different conclusions regarding different types of dissemination.

We should differentiate between full dissemination and other types of reproduction regarding dissemination by the intermediary. Full dissemination does not frame defamatory content. This type of dissemination leads to positive externalities by allowing constant updates and improving the flow of information. Due to the ease of dissemination and the difficulty of filtering out defamatory content, the costs of preventing dissemination of defamatory content may outweigh the benefits. Thus, immunity from liability strikes the right balance.

Selective dissemination focuses the attention on user-generated defamatory content, frames it, and enhances its magnitude. Consequently, it is likely to cause severe harm to victims. The intermediary selects content for dissemination and controls the content it reproduc-

253. *See* Kreimer, *supra* note 2, at 17.

254. For example, the operator of the listserv in *Batzel v. Smith*, is not necessarily deep-pocketed. 333 F.3d 1018 (9th Cir. 2003).

255. *See* Sanchez, *supra* note 63, at 317–19 (concluding that some intermediaries will choose not to reproduce speech at all due to the cost of evaluating complex defamation law as well as meritless claims from plaintiffs aiming to suppress their speech rather than recover for a genuine harm).

es.[256] Thus, the prevention costs of disseminating defamation are low in comparison to full dissemination. The benefits of selective dissemination are not uniform. Selection of content that includes defamation can make it easier for recipients to get relevant information.[257] Although the intermediary controls the content it selects, the costs of preventing the dissemination of defamation may be particularly extensive. Thus, cost-benefit analysis does not produce a clear conclusion regarding the standard of liability. In contrast, when the intermediary selects *only* defamatory content items for dissemination,[258] the harm is extensive, the positive externalities of the dissemination are marginal, and the prevention costs are low in comparison to dissemination that is not focused on defamation.

As for adopting defamation, the intermediary controls the content it generates. Consequently, the cost of preventing harm is low. In addition, there are no extensive benefits in explicit adoption of specific defamatory content. In this context, imposing liability on intermediaries is efficient.

This result is different when the selective dissemination follows users' requests or signals. In this context, the intermediary can avoid embedding updating and voting systems on its platform. Yet, these systems allow users to focus on useful information, promote participation and enrich the market of ideas and democratic culture. The benefits of these systems far outweigh their cost; therefore, it is inefficient to allocate liability to intermediaries in these instances.

3. Technological Innovation

In the digital age, one cannot discuss the allocation of liability without referring to technological innovation. The liability regime taxes innovation and influences its course.[259] The expected liability outcome *ex post facto* influences investments in certain types of

256. Today the selection can be performed by automatic algorithms as demonstrated in the Facebook experiment. *See* Grimmelmann, *supra* note 41. However, the intermediary still controls the parameters at the base of the algorithms *ex ante*. On "policy neutral" vs. "policy directed" algorithms, see Omer Tene & Jules Polonetsky*, Taming the Golem: Challenges of Ethical Algorithmic Decision Making*, N.C. J.L. & TECH. (forthcoming 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2981466 [https://perma.cc/P4N2-VHH3].

257. For example, see the operator of the listserv in *Batzel*. 333 F.3d at 1022.

258. For example, see the selective dissemination of quotes from the reviews in Seaton v. TripAdvisor, LLC. 728 F.3d 592, 599 (6th Cir. 2013). *See also* Roca Labs, Inc. v. Consumer Opinion Corp., 140 F. Supp. 3d 1311, 1315 (M.D. Fla. 2015).

259. Evidence shows that under liberal liability regimes, innovation thrives. *See* Guy Pessach, *Deconstructing Disintermediation: A Skeptical Copyright Perspective*, 31 CARDOZO ARTS & ENT. L. REV. 833, 864 (2013); *see also* Gideon Parchomovsky & Alex Stein, *Torts and Innovation*, 107 MICH. L. REV. 285, 314 (2008); Tal Zarsky*, The Privacy–Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 126 (2015).

technologies and the adopted business models,[260] both of which play an important role in determining efficiency.

One may argue that an exemption of liability for dissemination will enable freedom and openness, thereby incentivizing entrepreneurs to invest in technological ventures and digital markets. They will develop innovative platforms and systems for disseminating information. Stricter liability, however, might stifle innovation. It might impede the significant technological progress witnessed in recent years, including productivity and personal satisfaction. Due to the ambiguity regarding the scope of liability, innovation will become too risky or expensive. Consequently, intermediaries will refrain from developing interactive systems for sharing content and will avoid disseminating user-generated content.[261]

Yet, liability probably would have limited effect on innovation as long as it remains neutral to specific technologies. Anyone who conducts business of any complexity must consult with a lawyer at some point regarding liability exposure. In some cases, despite formidable legal regulations, innovation continues to thrive.[262] The concern of impeding innovation might be overstated. Certainly, some innovators will shy away from legally murky areas. Nevertheless, promoting innovation alone cannot be a sufficient justification for exempting intermediaries from liability.[263] There is an even more fundamental reason why exemption from liability would be unwise. An overall immunity for all types of architecture designs will yield a generation of technologies that facilitates behavior that society seeks to prohibit. We should do what we can to guide the development of the internet in a direction that promotes compliance with the law.

Imposing liability for dissemination should not be ruled out. However, there are different types of dissemination. A one-size-fits-all approach to intermediaries' liability is inappropriate. When an intermediary disseminates indiscriminately or posts links to content, it does not add value to the content and therefore should not be responsible for defamation. In contrast, when it selects to disseminate defa-

---

260. *See* Dotan Oliar, *The Copyright–Innovation Tradeoff*, 64 STAN. L. REV. 951, 1000–01 (2012); Pessach, *supra* note 253, at 864 (noting that YouTube owes its survival to a notice-and-takedown copyright liability regime which allows YouTube to escape liability for copyrighted material posted on its site if it removes it upon notice by the copyright holder).

261. *See* ANUPAN CHANDER, THE ELECTRONIC SILK ROAD 57 (2013); JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET: AND HOW TO STOP IT 119 (2008); *see generally* Michael A. Carrier, *Copyright and Innovation*, WIS. L. REV. 891 (2012).

262. *See* Alex Kozinsky & Josh Goldfoot, *A Declaration of the Dependence of Cyberspace*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 169, 176 (Berin Szoka & Adam Marcus eds., 2010) (noting that the auto and pharmaceutical industries are heavily regulated, yet are able to innovate).

263. *See id.* ("[P]romoting innovation alone cannot be a sufficient justification for exempting innovators from the law.").

mation or adopts it, the intermediary adds its own value that extends beyond the design of the platform; the liability is not imposed on the act of dissemination, or on the creation of a new technological architecture, but rather on the value added to the technology. Therefore, there is less concern that liability will chill innovation.

As for selective dissemination following users' requests or signals, every user expresses his preferences by selecting or voting for specific content. The intermediary remains neutral and his involvement does not extend beyond the design of the platform.[264] Exempting intermediaries from liability will incentivize development of technological tools that expand on users' choices and improve their experience. In such cases, imposing liability on intermediaries will chill innovation; therefore, it is undesirable.

### *F. Rethinking Liability for Disseminating User-Generated Content*

Intermediaries are not mere conduits.[265] As demonstrated in Section III, intermediaries disseminate user-generated content and influence speech. Consequently, they increase the chance of causing extensive harm. How should the law respond to this harm? Should online intermediaries be liable for dissemination? What is the appropriate standard of liability? Current laws do not provide a clear and consistent answer to these questions. This extensive ambiguity results in uncertainty and confusion.

Intermediaries' liability has attracted a great deal of attention in judicial decisions and scholarly work. Some have suggested an overall immunity regime for all types of dissemination.[266] A different approach compares intermediaries' liability to traditional media gatekeepers and tends to hold them responsible for dissemination.[267] Other suggestions are too ambiguous regarding their application and the standard of liability remains equivocal. The following subsections, shall review these scholarly suggestions and their limitations.

---

264. Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 295–96 (2006).

265. *See generally* Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 1, 16 (2017) (describing the design of platforms to collect, analyze, and sort user data for their own commercial reasons and arguing that these functions belie any suggestion that online intermediaries are merely passive conduits of user information).

266. *See* Sanchez, *supra* note 63.

267. On the broad approach towards intermediaries' liability, see Delfi AS v. Estonia, No. 64569/09, HUDOC (Eur. Ct. H.R. Jun. 16, 2015), http://hudoc.echr.coe.int/eng?i=001-155105 [https://perma.cc/B4HE-L5LC]. This approach is overinclusive.

1. Protections for Neutral Reportage

There is a debate on whether courts have gone too far in shielding Internet disseminators from liability under § 230.[268] Though, as demonstrated above, some courts did not extend the immunity to dissemination and stripped intermediaries of their immunity.[269] In many jurisdictions, the fair report doctrine shields a publisher from liability for reporting on defamatory matters in a report of an official action or proceeding, or of a meeting open to the public that deals with a matter of public concern, if the report is accurate and complete or a fair abridgement of the occurrence reported.[270] A slightly expanded protection exists in some jurisdictions for the news media that report a neutral and accurate account of a newsworthy charge made by a responsible and prominent organization against a public figure. This privilege is called the "neutral reportage privilege."[271]

These doctrines come into action when a reproduction has value that outweighs the interests of the plaintiff in recovering for the alleged harm arising from the dissemination of defamation online.[272] Scholars have suggested applying the neutral reportage privilege to dissemination of defamation online.[273] Under this model, if courts strip online intermediaries of immunity, the neutral reportage privilege would limit the scope of liability and protect intermediaries that disseminate defamation without amplification. Consequently, online publishers "would have an incentive to engage in ethical journalistic behavior."[274]

This suggestion is a good policy, but it requires concretization in order to accommodate the types of dissemination online. This doctrine justifies avoiding liability for full dissemination and regular links

268. *See* Laidman, *supra* note 217, at 106.

269. *See, e.g.*, Diamond Ranch Acad., Inc. v. Filer, No. 2:14-CV-751-TC, 2016 WL 633351 (D. Utah Feb. 17, 2016); *supra* Part III.B.1.

270. *See* Laidman, *supra* note 223, at 79 (quoting RESTATEMENT (SECOND) OF TORTS § 611 (1977)); *see also* Groover Hyland, *supra* note 113, at 95.

271. *See* Edwards v. Nat'l Audubon Soc'y, Inc., 556 F.2d 113, 120 (2d Cir. 1977); Laidman, *supra* note 223, at 80; Sanchez, *supra* note 56, at 305–06; Justin H. Wertman, *Newsworthiness Requirement of the Privilege of Neutral Reportage is a Matter of Public Concern*, 65 FORDHAM L. REV. 789, 789 (1996). For a similar defense in England, see the public interest defense outlined in § 4(1) to the Defamation Act of 2013: "Publication on matter of public interest (1) It is a defense to an action for defamation for the defendant to show that — (a) the statement complained of was, or formed part of, a statement on a matter of public interest; and (b) the defendant reasonably believed that publishing the statement complained of was in the public interest." Defamation Act, 2013, c. 26 § 4(1) (U.K.).

272. *See* Sanchez, *supra* note 63, at 319.

273. *See* Laidman, *supra* note 223, at 105 ("[W]ider recognition of at least the core model of the neutral reportage privilege would benefit the law of republication of defamatory statements online.").

274. *Id.* at 106.

while not exempting intermediaries that adopt defamatory content. Yet, normative questions remain regarding selective dissemination.

2. Liability for Selective Dissemination

Scholarly literature proposes to impose liability on intermediaries that select content for dissemination and enhance its magnitude.[275] Not extending immunity to intermediaries that select particular defamatory posts for dissemination might be a good starting point, yet, it leaves some questions open regarding the scope of liability. Should the courts impose liability only on intermediaries that select defamatory content in particular? Or find the intermediaries responsible for defamation even if part of the content selected is nondefamatory? Should intermediaries bear liability for deep direct linking that directs users' attention to specific defamatory content, frame it, and thus enhance its magnitude?

3. Incentives of Speakers and Intermediation

Felix Wu defines collateral censorship as occurring "when a (private) intermediary suppresses the speech of others in order to avoid liability that otherwise might be imposed on it as a result of that speech."[276] Collateral censorship stems from a disconnection between the incentives of intermediaries and the original speaker. Intermediaries have different incentives to carry particular content than original speakers have to create it in the first place. Wu argues that "[t]hose incentives diverge both because original speakers obtain benefits from the speech not realized by intermediaries and because intermediaries face liability risks not borne by original speakers."[277] Applying the same law to intermediaries and original speakers alike, despite the divergence of incentives, would incentivize intermediaries "to suppress more speech than would be withheld by original speakers."[278] Intermediaries' immunity responds to the problem of collateral censorship.

Yet, immunity is not the appropriate response to situations in which collateral censorship is not the problem. An intermediary who obtains social benefits from speech and has the incentives of the original speaker does not need the incentives that immunity provides to facilitate speech. Whenever intermediaries function as speakers, the

275. By doing this, the intermediary takes an additional step beyond the traditional editorial function of publishers. *See* Fitt, *supra* note 86, at 1865–67.

276. Wu, *Collateral Censorship*, *supra* note 225, at 295–96 ("This is a problem because some of the suppressed speech might in fact be lawful, even socially desirable.").

277. *Id.* at 296–97.

278. *Id.* at 296.

rationale for immunity diminishes.[279] Courts should only apply the immunity to intermediaries that moderate the discussion, assist the speech of others, and have the incentives of intermediaries.

Differentiating between incentives of intermediaries and speakers is important. It excludes extreme cases from enjoying immunity. It should not extend to when the public can understand that the intermediary speaks for itself. Yet, this differentiation leaves a grey area, since the dividing line between intermediaries and speakers is often ambiguous and it is not always clear whether the intermediary speaks for itself or merely assists the speech of others. In addition, by focusing on the incentives to speak, one neglects to address the potential of dissemination to influence the audience. Intermediaries that assist speech may have far-reaching effects on users and can lead to severe harm. Extending immunity to these intermediaries may lead to irresponsible dissemination.[280]

#### 4. Differentiation Between Dissemination According to the Intermediary's Discretion and Dissemination that Depends on Users' Choices and Signals

In the related context of search engines, some literature argues that intermediaries are not mere conduits or editors, but advisors.[281] They help users achieve their diverse and individualized information goals. Thus, intermediaries that assist their users to achieve their goals should be exempt from liability.[282] This proposal justifies the exemption of selective dissemination that depends on users' choices or signals.

## IV. A NEW FRAMEWORK FOR IMPOSING LIABILITY ON INTERMEDIARIES

Dissemination of defamatory content exacerbates its circulation and influences the significance ascribed to it. An overall immunity is inadequate to respond to the challenges of intermediaries' liability for disseminating user-generated defamatory content. Suggestions in scholarly work for regulating intermediaries' liability are not optimal. Therefore, a more comprehensive framework is required. The following part re-conceptualizes dissemination of content and outlines a tailored guideline for imposing liability on intermediaries.

---

279. *See id.* at 331–33.

280. It remains unclear whether selective dissemination in a listserv is intermediation or speech. Furthermore, even if selective dissemination is not driven by the incentives of speakers, it can still exacerbate harm. *See* Hong Lee, *supra* note 120, at 490–91.

281. *See* Grimmelmann, *Speech Engines, supra* note 240 at 893.

282. *See id.* at 893–910.

### *A. Out of Context — A New Perspective on Liability*

Online speech does not occur in a void, but exists in many contexts. Each context facilitates distinctive kinds of expressions, interactions, and activities among users.[283] The source of the message, the context of the message, and the situation influence the flow of information and may be more important than the content itself.[284] Simple changes in the source of the message, the manner of presentation, and the nature of the recipients, influence the magnitude and credibility ascribed to the content.

Dissemination of content out of its original setting changes the context because it attracts a new audience that is characterized by different social structures.[285] Dissemination may influence the context of the message, its representation, and the way the audience perceives the source of the message. In other words, it takes content out of context.

The proposed framework views dissemination through the prism of context. This perspective leads to a new understanding of intermediaries' liability. A large body of scholarly work has already explored the importance of context in enhancing or infringing privacy.[286] In this related field — privacy law — policymakers even outlined suggestions for a context-dependent regulatory regime.[287] Judicial decisions on defamation also bind liability with context.[288] Some judges implicitly ascribe liability for defamatory content that was published out of context. In a dissenting opinion in *Batzel v. Smith*,[289] Justice Gould concluded that selecting particular information for distribution forms the

---

283. On the importance of context, see Lavi, *supra* note 18, at 894, 909.

284. *See id.* at 909–41; *supra* Part II.B.

285. Outside the original social network, content may be perceived differently because the audience of recipients may have different social norms.

286. These studies focused on the importance of context in enhancing or infringing privacy. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT, 50 (2010); James Grimmelmann, *Privacy as Product of Safety*, 19 WIDENER L.J. 793, 808–12 (2010).

287. *See* Helen Nissenbaum, *Respecting Context to Protect Privacy*, SCI. ENGINEERING ETHICS (July 12, 2015) (referring to the third principle of the Privacy Bill of Rights entitled "Respect for Context" endorsed by the White House in February 2012 that "companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."). In a similar manner, the context in which data is collected has an important role in Europe. *See* Regulation 2016/679, art. 6(4) (EU), General Data Protection Regulation, *supra* note 162 (referring to the compatibility of processing with the purpose for which personal data was initially collected). *But see* Tal Zarsky*, Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1008 (2017).

288. *See, e.g.*, Ollman v. Evans 750 F.2d 970, 979 (D.C. Cir. 1984). The *Ollman* test requires consideration of a statement's precision, verifiability, literary context, and social context when separating fact from opinion. *See also* Rodney W. Ott, *Fact and Opinion in Defamation: Recognizing the Formative Power of Context*, 58 FORDHAM L. REV. 761, 762 (1990); Robert C. Post, *The Constitutional Concept of Public Discourse*, 103 HARV. L. REV. 603, 640 (1990); COLLINS, *supra* note 10, at ¶¶ 8.43–8.55 (addressing the role of context in interpreting defenses).

289. 333 F.3d 1018, 1036 (9th Cir. 2003).

impression that it is worthy of dissemination and therefore the information is transformed.[290] In *Diamond Ranch Academy, Inc. v. Filer,* the court implied that the lack of quotation marks or another signal indicating a quotation from third parties' content may foil a defendant's immunity.[291] From these examples, it is clear that some courts consider context as a central factor for deciding intermediaries' liability.

Understanding the cognitive influence of context on the flow of information,[292] allows policymakers to apply a just and efficient legal policy for intermediaries' liability. Since the following analysis focuses on the context of dissemination and not on technology, it accommodates the dynamic online environment. In addition, we must also examine the causal link between the intermediary and how the content was taken out of context. This Article shall review these factors in the following sections.

1. The Degree of Taking Content Out of Context

Spreading defamation to a new audience of recipients takes it out of context. In some cases, the influence of dissemination is only noticed in increased circulation. Yet, it may influence the source of the message, and the importance ascribed to it.[293]

2. The Causal Link Between the Intermediary and Dissemination

This factor examines whether the defamatory content was disseminated by the intermediary's choice, or according to users' selection or signals. In the latter case, the dissemination reflects the "wisdom of crowds."[294] Consequently, the causal link between the intermediary and the harm weakens. In such cases, as long as the intermediary did not encourage users to vote in a specific way,[295] there are fewer justifications for imposing liability on the intermediary.

Using these axes allows us to analyze intermediaries' liability throughout the next sections. When taking these axes into mind, one

290. *See id.* at 1038–39 (Gould, J., dissenting).

291. *See* No. 2:14-CV-751-TC, 2016 WL 633351 at *20–21 (D. Utah Feb. 17, 2016).

292. For example, framing content exacerbates cognitive biases. *See generally,* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE (2008); OREN BAR-GILL, SEDUCTION BY CONTRACT (2012).

293. *See supra* Part II. Dissemination of content may encourage readers to spread it.

294. *See generally* JAMES SUROWIECKI, THE WISDOM OF CROWDS (2005).

295. When an intermediary influences users' choice to get updates on defamatory content or encourages them to vote for defamation, there is a causal link between the intermediary and the defamation. Under the proposed framework, the court may hold the intermediary responsible for the defamation.

can tailor the liability intermediaries should bear and outline differential standards for liability.

### *B. Out of Context — Particular Guidelines for Intermediaries' Liability*

The following sections will outline a nuanced guideline for intermediaries' liability, which is based on three forms of content dissemination: (1) Full Dissemination, (2) Selective Dissemination, (3) Adoption of Defamation.

#### 1. Full Dissemination

Spreading users' content without selecting specific items for dissemination[296] reproduces the content and enhances its circulation and availability. It also expands the audience of recipients. However, it does not frame defamation; it does not direct the public's attention to the defamatory comments in particular nor does it reinforce them. Although it enhances the quantity of defamatory content online, it does not increase in proportion, since positive comments are disseminated as well. In essence, the context and source of the messages remain the same. This type of dissemination takes content out of context in a mild degree and does not lead to a significant change in context. Thus, the likelihood for severe harm is lower in comparison to other types of dissemination.

The context hardly changes when the intermediary does not reproduce the content, but rather leads users to the original source by, for example, using regular links. In such cases, the intermediary exposes users to the full text and context of the social network in which the expression was originally published.

Full dissemination exacerbates defamation mildly. Imposing liability on an intermediary for full dissemination is undesirable. Liability is likely to disproportionately chill speech and hinder the benefits of public dialogue. This is even more true in light of technologies that make it difficult for intermediaries to control the content they disseminate in advance.[297]

The significant social cost of imposing liability, and the possibility of censorship mean that courts should apply § 230 and exempt intermediaries from liability in cases of full dissemination. Because the text is hardly taken out of context, judges should refrain from considering

296. On full dissemination, see *supra* Part II.B.1.

297. For example, intermediaries may use an RSS protocol (*see supra* note 9) and have no knowledge of the content disseminated by the protocol in advance. Imposing liability may reduce the usage of the protocol and may excessively reduce the dissemination of content.

this type of dissemination as creation or development of content. This is especially true when an intermediary exposes users to the full context of the source by linking to it.[298] Exemption from liability should also be applied to full dissemination that follows users' requests or signals since there is no significant causal link between the intermediary and the harm. Applying immunity to full dissemination strikes an optimal balance between free speech and reputation, and promotes corrective justice, efficiency, as well as innovation.

2. Selective Dissemination

Full dissemination is different from selecting content, which may include defamation, and disseminating it out of context,[299] or selecting to disseminate defamatory content in particular.[300] In the latter two cases, an intermediary selects some items for dissemination and rejects others. This selection is not a mere act of discrimination, but an act of self-expression.[301]

Selective dissemination enhances the magnitude of defamation. It affects the source of the message, and as a result, the public might get the impression that the intermediary's choice to disseminate that specific content is an indication regarding its importance. People might even reach the conclusion that the intermediary endorses the content. Selective dissemination influences the message by framing it. The dissemination also expands the number of recipients. Consequently, users are likely to pay more attention to the content. It is likely to become more credible as it spreads to others.[302] Selective dissemination may also lead the public to draw conclusions based on partial information. Consequently, people might reach the wrong conclusion regarding the victim of the defamation and as a result avoid efficient transactions with him.[303] Selective dissemination significantly takes content out of context in comparison to full dissemination**.** Thus, it exacerbates the gravity of defamation harm.

---

298. On links, see *In re* Philadelphia Newspapers, LLC, 69 F.3d 161, 174 (3rd Cir. 2012); Salyer v. Southern Poverty Law Center, Inc., 701 F. Supp. 2d 912, 916–18 (W.D. Ky. 2009); Life Designs Ranch, Inc. v. Sommer, 364 P.3d 129, 145 (Wash. App. Div. 3 2015).

299. *See, e.g.*, Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003).

300. *See, e.g.*, Seaton v. TripAdvisor, LLC, 728 F.3d 592, 598 (6th Cir. 2013).

301. *See* Tim Wu, *Is Filtering Censorship?*, *in* CONSTITUTION 3.0 83, 88–89 (Rosen & Wittes eds. 2011).

302. *See* DIFONZO & BORDIA, *supra* note 24; *Batzel*, 333 F.3d at 1038–39 (Gould, J., dissenting).

303. For example, an intermediary can disseminate only negative reviews from a rating service and omit the positive ones. It can also omit the comments of the subject of the review. Selecting to present only negative information exacerbates harm because it reduces the likelihood of correcting negative impression.

There are different types of selection and degrees to how content is taken out of context. An intermediary can select a few content items and disseminate them without focusing on defamation in particular. For example, an operator of a listserv can select to disseminate specific items (laudatory, neutral, and defamatory), which do not frame defamation in particular. This method of selection signals that the content is worthy of dissemination and allows users to focus their attention on relevant content.

An intermediary can select to disseminate defamatory content in particular. It can base the content of its homepage only on defamatory reviews, frame defamation and shape users' perception on the person or business reviewed. In such cases, the content is substantially taken out of context in comparison to the example of the listserv.

Both examples represent different models of dissemination.[304] However, there is no clear dichotomy between them; in fact, these models are on two ends of a spectrum. The intermediary can select any number of defamatory and neutral comments, playing with the number of each as it reproduces them. Different proportions enhance or reduce defamatory levels.[305] And it is not always clear whether an intermediary's incentives are identical to the incentives of the speaker. [306]

The proportion of defamation selected by the intermediary relative to the proportion of defamation in the source influences the degree to which the content was taken out of context. In addition, courts should examine the method of dissemination of the defamatory content. For example, deep linking can direct users to a defamatory expression.[307] Yet, in some cases, a simple action can expose users to the overall context of the expression and minimize harm.[308] When it takes more than just a simple action to expose users to the context of the expression, the degree in which it appears out of context becomes more significant.

Selective dissemination can inflict severe harm to reputation. Therefore, an overall immunity regime is over-inclusive and might create disincentives for those in the best position to minimize harm to do so. Such immunity can foster irresponsibility, increase harm to reputation, and fail to strike a proper balance between the normative considerations discussed above.[309]

---

304. In the first case, the intermediary selects a variety of content for dissemination and this selection is an act of moderation. The intermediary only advises users to consume relevant content. In contrast, the intermediary acts as a speaker when it only disseminates defamation.

305. For example, the intermediary can select three reviews from a rating service where two of them are defamatory and the third is neutral.

306. *See* Wu, *Machine Speech*, *supra* note 48, at 1521–22; Wu, *Filtering, supra* note 299, at 85.

307. On deep direct linking, see *supra* Part II.B.2.b.

308. For example, a simple scroll using the mouse exposes the user to the overall context.

309. On the values at the base of liability, see *supra* Part III.E.

When the intermediary selects content for dissemination, there is no defining line between intermediation and speech, and it is not always clear whether the incentives are directed towards a speaker or an intermediary.[310] Traditional publisher-style strict liability is not suitable, since it would cause over-deterrence, increase the cost of efficient conduct,[311] and lead to a severe chilling effect in comparison to other regimes.[312] Instead, the optimal liability regime in this context is distributor-style negligence liability. Accordingly, the court should subject the intermediary to liability only if it knows, or should have known of the defamatory nature of the content it selects to disseminate. This regime will lead to a differential liability system, which depends on how much text was taken out of context in proportion to the defamatory content in the source.

Judges should not hold an intermediary responsible for defamation when it selects a few content items for dissemination (neutral and defamatory) without framing the defamation, and especially when the rate of defamatory content in the overall selection is low. Instead, they should find that the intermediary does not have to know about the nature of every defamatory content item it selects to disseminate. Alternatively, judges can consider the dissemination as a neutral report on users' comments, especially when the intermediary does not frame the defamatory content. This interpretation inserts defamation into the normative standard of negligence, building upon a normative standard of duty of care. Such a regime would prevent a disproportionate chilling effect on the flow of information.[313]

When most or all of the content selected for dissemination is defamatory relative to the proportion of defamation in the source, the influence on the recipients is profound and the content is grossly taken out of context. In these cases, judges can hold an intermediary liable because it should have known of the defamatory nature of the content it selected.

The manner of distribution also influences the degree in which the content was taken out of context. When an intermediary directs users to defamatory content, by using deep direct linking or similar means, courts should not hold the intermediary responsible if the user, who clicks on the link, can be exposed to the context by a simple act, such as scrolling the screen. This conclusion also applies to intermediaries that automatically link to a post or a webpage and selectively repeat

---

310. Wu, *Collateral Censorship*, *supra* note 225, at 304–08.

311. On this standard of liability see *supra* Part III.C. *See also* POSNER, *supra* note 63 at 246–47.

312. For example, requiring a listserv operator to pre-screen the content it disseminates thoroughly may lead to inefficiency. *See* Batzel v. Smith, 333 F.3d 1018, 1034, 1039 (9th Cir. 2003).

313. On defamation law defenses, see *supra* Part III.A.

parts of the content stated in it on their users' newsfeeds and search results in order to make it easier for users to find relevant content. In such cases, selective dissemination is a regular practice. Thus, users know the snippet exposes them only to part of the content, and can click on the link and see the full context.[314]

Furthermore, even if a simple act does not expose the user to the full context, the scope of liability to deep direct linking should be narrower than the liability to actual dissemination. Thus, courts should hold the intermediary liable if it had actual knowledge of the defamation after receiving a complaint regarding the link. Liability to deep direct linking could be avoided by removing the link *ex post facto*. Thus, a disproportional chilling effect on connectivity can be mitigated.

As for selective dissemination following users' requests or signals, immunity under § 230 should apply, since the intermediary does not take the defamation out of context, and there is no direct causal link between its actions and the potential harm.

Differential liability for selective dissemination must depend on the degree to which the content was taken out of context. This regime allows for flexibility and enhances accountability. It also strikes an optimal balance between free speech and reputation, promotes corrective justice, efficiency, and innovation.[315]

3. Adoption of Defamation

Adoption of defamatory content places the intermediary in the role of a speaker.[316] When an intermediary mixes its own content with users' posts and adopts their content, the intermediary frames the content, enhances the magnitude ascribed to the content, and influences the context of the message. The intermediary functions as a social actor and users may perceive it as the source of the message. Due to the centrality of the intermediary, users are likely to ascribe importance to the message it disseminates, since it originates from an influential par-

314. The law in the United States exempts intermediaries from liability for snippets due to CDA immunity, *see* O'Kroley v. Fastcase, Inc., 831 F.3d 352, 353–55 (6th Cir. 2016), while the law in Canada exempts intermediaries from liability for automated snippets due to the lack of knowledge as to the defamatory content they contain, *see* Niemela v. Malamas, No. S146067 2015 B.C.S.C. 1024 ¶ 84 (June 16, 2015) (Can.). The proposed solution supplies a defense because in snippet cases, the degree of contextual breach is relatively low.

315. Distributor-style liability based on negligence will strike the proper balance between freedom of expression and reputation. This regime is fault-based and in line with corrective justice. Liability for selective dissemination also leads to efficient deterrence. The chilling effect on innovation is expected to be proportional because liability is based on the degree to which the message was taken out of context and not on the technological systems that are employed.

316. The incentives of intermediaries that adopt content are like those of speakers. On incentives of intermediaries and speakers, see Wu, *Collateral Censorship*, *supra* note 225, at 13–17.

ticipant.[317] By mixing its own content with users' content, it also increases the likelihood that users will spread the content. Adoption of a defamatory statement takes it out of context at the highest level of the three categories reviewed, and exacerbates the gravity of harm.

Additions or remarks to users' content are not uniform. Different additions or endorsements can lead to different degrees of taking messages out of context. First, the content that an intermediary adds to users' posts influences the context of the mixed content. The intermediary can draw the attention of the public to specific content, can support the defamatory content, and enhance its magnitude. Courts should examine the message the intermediary conveys and its possible influences on the perception of defamation by the recipients.[318] Second, the manner of adoption influences the degree of taking the message out of context. For example, the intermediary can adopt content that users publish on its platform, or link to content published elsewhere and adopt it. In the latter case, it is less likely that users perceive the intermediary as the source of the overall content. Thus, the degree into which the content is out of context is lower.

Due to the different degrees in breach of context, liability should be differential. Adoption of defamatory content is considered a publication, and may result in a new cause of action.[319] When an intermediary positively adopts defamation**,** or adds titles that are defamatory in nature, it participates in the process of developing information.[320] Courts may attribute the mixed content to the intermediary and hold it responsible as a speaker.[321] Accordingly, an intermediary's adoption of defamation can be actionable under defamation law. Yet, the intermediary can enjoy the defenses or privileges of defamation laws[322] and first amendment protections. For example, the intermediary can claim that the adoption is a protected opinion. However, this defense should

317. On "influentials," see *supra* note 16. On adoption of defamation in particular, see *supra* Part II.B.3.

318. *See* Lidsky & Jones, *supra* note 168, at 165 (describing the hashtag symbol on Twitter (#) and arguing that hashtags contextualize speech on social media, and could help lend important context to a statement that might or might not be actionable defamation. Thus, "attaching '#justkidding' to a tweet ought to mitigate or completely remove its defamatory sting while attaching '#totallyserious' might magnify it.").

319. On repetition as a new publication, see KEETON *supra* note 63.

320. For example, adding defamatory titles to users' defamatory reviews such as "fraud" or "rip-off." *See* GW Equity, LLC v. Xcentric Ventures, LLC, No. 3:07-CV-976-O, 2009 WL 62173, at *3–4, *6 (N.D. Tex. Jan. 9, 2009).

321. *See* Morley, *supra* note 55; *see also, e.g.*, Seaton v. TripAdvisor, LLC, 728 F.3d 592, 594–95 (6th Cir. 2013); Diamond Ranch Academy, Inc. v. Filer, No. 2:14-CV-751-TC, 2016 WL 633351, at *21 (D. Utah Feb. 17, 2016); MCW, Inc. v. Badbusinessbureau.com, LLC, No. Civ.A.3:02–CV–2727–G, 2004 WL 833595, at *10, *18 (N.D. Tex. Apr. 19, 2004).

322. On the privileges of defamation laws in general, see *supra* Part III.A.

be interpreted narrowly to matters of public interest and should not be extended to a flawed ranking methodology.[323]

The manner of adoption should affect the defenses that the intermediary can enjoy. When an intermediary links to a particular source and adopts the content included in the link, it distinguishes between its own opinions and the opinions of the author. Thus, it is more likely to enjoy a defense because the context is apparent.[324] In contrast, a court may not apply the defense when the intermediary does not distinguish between the user's content and its own opinion.

In one hypothetical, an intermediary adopts content after following a user's request or signals and users vote for the most appropriate title that it is added automatically to the content. In this case, § 230's immunity should apply since there is no causal link between the adoption and the intermediary. In this case, users are responsible for the breach in context.[325] Liability under defamation laws is in line with the normative considerations reviewed in Part IV.E.[326]

Table 2: Summary of the Guidelines for Intermediaries' Liability

| Context | Full Dissemination | Selective Dissemination | Adoption of Defamation |
|---|---|---|---|
| Actual Dissemination | • § 230's immunity | • Distributor-style negligence | • Liability to defamation |

323. A narrow interpretation of the defenses is justified particularly due to the intermediaries' extensive influence on the flow of information. Accordingly, the intermediary in the case of *TripAdvisor* should have been held responsible for adoption, since the flawed rating methodology and the intermediaries' additions to users' ratings left the impression that they viewed the assertions as facts.

324. Supporting statements with links may allow for a broader application of defenses. *See* Adelson v. Harris, 973 F. Supp. 2d 467, 471 (S.D.N.Y. 2013) (finding a publication not responsible for defaming the plaintiff because the publication linked to the content upon which its statements were based); *see also* Adelson v. Harris, 402 P.3d 665 (Nev. 2017) (holding that a hyperlink to source material concerning judicial proceedings qualifies under fair report privilege).

325. *See* Whitney Info. Network, Inc. v. Xcentric Ventures, LLC, No. 2:04-cv-47-FtM-34SPC, 2008 WL 450095, at *5, *8 (M.D. Fla. Feb. 15, 2008) (applying CDA immunity because the intermediary merely provided disparaging categories (*e.g.*, "con artists," "corrupt companies") from which a user must make a selection); *see also* Morley, *supra* note 55.

326. Adoption of users' defamatory content significantly takes it out of context. Liability under defamation laws will strike the right balance between freedom of expression and reputation. This regime is *not* fault-based; yet the defenses narrow the gap between defamation and fault-based regimes. Thus, in most cases it is in line with corrective justice. Liability for adoption leads to efficient deterrence. The chilling effect on innovation is expected to be marginal, because the liability is based on the degree of contextual breach and not on technology.

| | | | |
|---|---|---|---|
| | applies. | liability.<br>• The conclusion of liability/ exemption depends on the level of contextual breach. | as a speaker.<br>•The intermediary can enjoy the defenses, or privileges of defamation laws. |
| Dissemination Exposes Users to Complete Context (*E.g.*, linking to the original source) | • § 230's immunity applies. | • Liability for deep direct linking depending on the level of contextual breach.<br>• When the degree of contextual breach is significant and the user cannot be easily exposed to the context of text, the intermediary may be responsible if it did not remove the link upon knowledge. | • An intermediary that positively adopts the source to which it links might be responsible for defamation.<br>•The intermediary might enjoy defenses and First Amendment protections. |
| Dissemination/ Adoption Following a User's Request or Signal | • § 230's immunity applies. | • § 230's immunity applies. | • § 230's immunity applies. |

### *C. The Guidelines and the Law: Bridging the Gaps*

The current law provides an extensive shield to protect intermediaries from civil liability. Intermediaries are not treated as publishers for material they did not publish or develop.[327] Courts usually interpret the immunity broadly and extend it to selective dissemination. In some

327. *See* 47 U.S.C. § 230 (2012); *supra* Part III.B.

cases, they even extend the immunity to adoption of defamation.[328] However, the overall immunity scheme was constructed when the web was in its infancy. As technologies advance and the web becomes more prevalent, defamation can easily get out of context, spread, and lead to substantial harm. Therefore, it is time to challenge the immunity regime and refine it. Scholarly work suggests amending § 230 can narrow down the immunity.[329]

Yet courts can rediscover the proper boundaries of immunity without legislative changes.[330] Using the proposed guidelines would allow the courts flexibility when adjudicating online defamatory cases without hindering the dynamic environment online. According to a proper reading of § 230, intermediaries that selectively disseminate, or adopt defamation are responsible at least in part for creating or developing defamatory content.[331] Thus, in such situations, courts should not grant intermediaries immunity and should allow lawsuits to proceed after the preliminary stages.[332]

### *D. The Guidelines and the Challenge of Voting Systems in the Algorithmic Governance Age*

This Article proposes to exempt intermediaries from liability if they disseminate or adopt content after following users' requests or signals. In these cases, intermediaries do not cause harm; instead, there is a direct causal link between the users and the harm. However, in the digital age, voting systems weigh users' choices by using automatic algorithms.[333] Intermediaries and other stakeholders can manipulate algorithms and thereby influence the disseminated content. Thus, disseminated content, that might appear as if users selected it, reflects the choices of the intermediaries and stakeholders. An overall exemption in this instance is therefore under-inclusive. This Part aspires to meet the challenges algorithms impose on automated voting systems.

The first challenge is to determine whether the dissemination truly reflects the choice of the users. Although it may appear as if the sys-

---

328. *See supra* Part III.B.; s*ee, e.g.*, Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398 (6th Cir. 2014).

329. *See* Browne-Barbour, *supra* note 67, at 1554.

330. On narrowing the scope of § 230 through interpretation by the courts, without amending the law, see Sylvain, *supra* note 266, at 75 ("[C]ourts ought to rethink the scope of the immunity under Section 230 . . . ."). The interpretative route is also preferred by Citron & Wittes. *See* Citron & Wittes, *supra* note 152 at 418.

331. *See* 47 U.S.C. § 230 (c), (f)(3).

332. For an application of this argument to revenge porn victims, see Franklin, *supra* note 107, at 1334.

333. *See generally* Tal Zarsky, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making,* SCI., TECH. & HUM. VALUES 118 (2015) (discussing the problems of opacity and the automatic nature of algorithmic decisions).

tem operates without human intervention, the intermediary facilitates it and the operation of the algorithm depends on the discretion of its programmers. Internet users are not made aware of the scope of the intermediary's intervention.[334] The intermediary can program the algorithm to manipulate the result of a voting system and promote its goals. For example, it can favor negative content on competitors of advertisers on its platform. If that is indeed the case, there is a causal link between the intermediary and the harm, and the rationales for exempting it from liability disappear. Scoring systems are shrouded in secrecy; it is difficult to contest them and evaluate the neutrality of the intermediary.[335]

One way to accommodate this problem is to encourage research and public review to reveal manipulative algorithmic practices. Regulators can call upon or even fund independent researchers specifically to analyze digital practices and attempt to uncover biased algorithms and manipulative practices of platforms.[336] Policy makers can also encourage active engagement of the public in challenging non-transparent and possibly biased systems of algorithmic governance by using a proactive methodology of "black box tinkering."[337] These solutions have the potential to mitigate the problem. Nevertheless, independent research and tinkering would reveal only part of the cases of biased algorithms and manipulation to public awareness. Consequently, the public would be left with insufficient knowledge on the utiliza-

---

334. *See generally* Tene & Polonetsky, *supra* note 256 (differentiating between policy-neutral algorithms that can, in some cases reflect existing entrenched societal biases and historic inequalities, and in contrast, policy-directed algorithms that are purposefully designed to advance a predefined policy agenda). For criticism on the lack of transparency in algorithmic decision-making, see Tarleton Gillespie, *The Relevance of Algorithms*, *in* MEDIA TECHNOLOGIES 167 (Gillespie et al. eds. 2014); Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 156 (2010). This leaves algorithms open to criticism that their criteria can skew results to the provider's commercial or political benefit.

335. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 7–11 (2014); *see also* TUFEKCI, TWITTER AND TEAR GAS, *supra* note 5, at 156 (explaining that Facebook's algorithm uses an opaque, proprietary formula that changes every week and can cause "huge shifts in news traffic."); CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA, 3–6 (2017) (explaining that Facebook uses its algorithm to prioritize posts of our friends and family on our newsfeeds, direct our attention to these posts, and influence the discourse without neutrality).

336. *See* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power,* 117 COLUM. L. REV. 1623, 1684 (2017) (focusing on non-transparent manipulative practices in a related context of sharing economy platforms and suggesting that third parties' independent research can reveal some of these manipulative practices. This solution has the potential for mitigating the problem of non-transparent biased practices of platforms).

337. Researchers argue that public engagement in checking the practices of automatic enforcement systems can mitigate the problem and enhance the awareness to biased algorithms. *See generally* Niva Elkin-Koren & Maayan Perel, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLA. L. REV. 181 (2017) (focusing on a related context of algorithmic enforcement of copyright infringement).

tion of biased algorithms and the manipulative influences of the platform.

Another way to accommodate this problem is to impose transparency obligations on intermediaries to disclose the parameters of the voting systems. For example, the courts or regulations may require them to articulate the number of voters and their names, or pseudonyms.[338] This will enable the court to find out whether the intermediary or the users are responsible for the dissemination.

Scholars propose to impose transparency obligations in similar issues, such as in search engines and credit score algorithms.[339] Yet, transparency appears to be insufficient to guarantee an acceptable public policy,[340] and it is doubtful if broad obligations of transparency are normatively desirable. Transparency obligations will allow commercial stakeholders to abuse public algorithms since they could use the information to optimize and manipulate results. In addition, algorithms are often changed, rendering simplified disclosures useless.[341] Thus, transparency is not the optimal path to enhance fairness and efficiency.[342] Furthermore, disclosure has limited benefits, since users might not understand it or be overwhelmed by overload of information.[343]

However, algorithms of voting systems tend to be simple in contrast to ones used in search engines. Moreover, the purpose of transparency obligations is to verify the site's operation and ascertain that dissemination comes from votes cast by users. Therefore, transparency

---

338. For example, Facebook allows users to see who liked or shared users' content. *See generally* FACEBOOK'S DATA POLICY, https://www.facebook.com/about/privacy [https:// perma.cc/ELA7-JU9J].

339. *See* PASQUALE, THE BLACK BOX SOCIETY, *supra* note 6, at 140; Frank Pasquale, *Dominant Search Engines: An Essential Cultural & Political Facility*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 401, 416 (Szoka & Marcus eds. 2011); Frank Pasquale, *Restoring Transparency to Automated Authority,* 9 J. TELECOMM. & HIGH TECH. L. 235, 254 (2011); Frank Pasquale, *Beyond Innovation*, *supra* note 334, at 172; Andrew Tutt, *The New Speech*, 41 HASTINGS CONST. L.Q. 235, 293–94 (2014).

340. *Cf.* Elkin-Koren & Perel, *Black Box Tinkering*, *supra* note 337, at 198 ("[A]lgorithmic enforcement by private entities raises serious challenges to the notion of transparency as the principal guardian of decision makers' accountability.").

341. *See* James Grimmelmann, *Some Skepticism About Search Neutrality*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 435, 455 (Szoka & Marcus eds. 2011).

342. On the shortcomings of transparency in the related context of credit scores, see generally Zarsky, *Algorithmic Decisions*, *supra* note 333.

343. On the limits of transparency and disclosure, see Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 31 (2014); Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 721 (2011); Elkin-Koren & Perel, *supra* note 309, at 185 ("Without proper tools to analyze massive amounts of data, these overwhelming disclosures are mostly pointless."); Florencia Marotta-Wurgler, *Even More Than You Wanted to Know About the Failures of Disclosure*, 11 JERUSALEM REV. LEGAL STUD. 63, 70 (2015); *see generally* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW 55–118 (2014). On the failure of disclosure in a related context of hidden sponsorship, see Zahr Said, *Mandated Disclosure in Literary Hybrid Speech,* 88 WASH. L. REV. 419, 457 (2013).

is not likely to disrupt the operation of the platform or impair the efficiency of the system. Despite the limitations of transparency, this method will allow victims to examine the intermediary's responsibility *ex post facto*.[344] Thus, although transparency obligations are not optimal, the benefits of disclosing the parameters at the base of voting systems exceed their cost.

One must bear in mind, however, that algorithms are guarded trade secrets; therefore, there are legal difficulties to imposing disclosure obligations upon them. To meet this problem, some scholars propose limited disclosure.[345] Some suggest allowing the Federal Trade Commission ("FTC") or an agency like the Food and Drug Administration ("FDA") to review scoring systems and thus protect against unfairness.[346] Applying this idea to potentially defamatory voting systems, the intermediary would be shielded by § 230's immunity only if the federal authority finds that the system is truly driven by users' selection. The review by federal authority may deter intermediaries from manipulating the system in the first place and promote efficiency. This solution is not optimal and involves administrative costs. Yet, despite criticism,[347] the rise of algorithm-based systems and their decisive influences on the flow of information make clear that now is the time to adopt this proposal.[348]

Another solution to the problem of voting systems' opacity is voluntary adoption of a transparency regime by the intermediaries. Fiduciary intermediaries can grant a trust mark to intermediaries that allows them to review their systems.[349] This self-regulating free mar-

---

344. After the fact, the victim could use experts to prove his claims. The information on the operation of the algorithm may also facilitate the flow of information about intermediaries' bad influences on voting systems. Thus, more users could be informed about the nature of the system. This dynamic may influence intermediaries' behavior *ex ante*. For this argument in a related context, see Shmuel I. Becher & Tal Z. Zarsky, *Online Consumer Contracts: No One Reads, but Does Anyone Care?*, 12 JERUSALEM REV. LEGAL STUD. 105, 119–20 (2015).

345. *See* PASQUALE, THE BLACK BOX SOCIETY, *supra* note 6 at 142–43; *see also* Citron & Pasquale, *supra* note 335, at 21; Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1540 (2013). Recently, scholars expressed their opinion that an operator of an algorithm should be precluded from relying on the model's predictive accuracy in defining its conduct, unless it is willing to disclose details of its model. *See* James Grimmelmann & Daniel Westreich, *Incomprehensible Discrimination*, 7 CALIF. L. REV. ONLINE 164, 174 (2017).

346. *See* Citron & Pasquale, *supra* note 335, at 23–27; Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 115–16 (2017).

347. *See* Adam Thierer et al., *Artificial Intelligence and Public Policy*, MERCATUS RES., MERCATUS CTR. GEO. MASON U., (2017) (arguing that this solution might hinder innovation and that the creation of a new regulatory body to audit algorithms, datasets, and techniques advances a "transparency paradox" of their own).

348. On the extensive influences of algorithm-based systems, see generally Citron & Pasquale, *supra* note 335, at 7; PASQUALE: THE BLACK BOX SOCIETY, *supra* note 6.

349. "Trust marks have been defined as: Electronic labels or visual representations indicating that an e-merchant has demonstrated its conformity to standards regarding, e.g., security, privacy, and business practice." THE EUROPEAN CONSUMER CENTRES' NETWORK, *Trust Marks Report 2013 "Can I Trust the Trust Mark?"* 7 (2013) (internal quotations omitted),

ket approach ascertains that voting systems reflect users' choices and selections. Over time, internet users might ascribe more credibility to content of websites that have trust marks and prefer them over others. This may incentivize online intermediaries to pursue a trust mark, and avoid manipulating the system. Yet, this solution is only partial because not all intermediaries are expected to adopt it.

The second challenge facing voting systems is manipulation by stakeholders, who are interested in promoting specific content. For example, a disappointed customer may vote for a negative review more than once (by using multiple user names). Thus, such a customer on Yelp could, using inflated votes, drive their review to become "The Review of the Day" and be disseminated to central websites. This dissemination does not reflect overall users' satisfaction, but rather the disgruntled view of one specific customer.

Stakeholders may manipulate voting systems by using automated software programs, known as bots.[350] These bots may be programmed to crawl the web, click a "like" button, or vote for specific types of content and enhance its dissemination.[351] Thus, disseminated content will not reflect the wisdom of the crowd but rather the choice of the stakeholder who employed the bots. In light of this result, one may argue that § 230's immunity should not apply to voting systems. However, intermediaries have incentives to prevent manipulation by stakeholders and preserve the credibility of their voting system. To do so, intermediaries can and do forbid such practices in their terms of service, block users that manipulate voting systems and use technologies for mitigating the harm of manipulations.[352] Thus, market forces can mitigate stakeholders' manipulation.

Private ordering is superior to legal regulation. In this context, mandates are far from ideal and may disproportionately chill voting

---

http://ec.europa.eu/dgs/health_food-safety/information_sources/docs/trust_mark_report_ 2013_ en.pdf [https://perma.cc/P6CB-LG47].

350. *See, e.g.*, Lucille M. Ponte, *Mad Men Posing as Ordinary Consumers: The Essential Role of Self-Regulation and Industry Ethics on Decreasing Deceptive Online Consumer Ratings and Reviews*, 12 J. MARSHALL REV. INTELL. PROP. L. 462, 481–82 (2013).

351. *See id.*; SILVERMAN, *supra* note 6, at 85 (explaining that "likes" and votes can be bought).

352. For example, the intermediary can use CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) and prevent the participation of nonhuman software. Furthermore, some technologies allow detecting and removing "likes" generated by "automated software programs, malware, and hacked accounts." Ponte, *supra* note 321, at 504. In a related context of extremist content, Facebook is improving its methods to combat harmful content by using artificial intelligence (AI) and machine learning. As technology develops, platforms are expected to find better ways to combat fake votes. *See* Julia Fioretti, *Pressured in Europe, Facebook Details Removal of Terrorism Content*, REUTERS (June 15, 2017) http://www.reuters.com/article/us-facebook-counterterrorism-idUSKBN1962F8 [https://perma.cc/Q3TQ-8SV9?type=image]; Julia Fioretti, *Web Giants to Cooperate on Removal of Extremist Content*, REUTERS (Dec. 5, 2016) http://www.reuters.com/article/us-internet-extremism-database-idUSKBN13U2W8 [https://perma.cc/3V48-KSSC].

systems, which promote democratic participation. Hence, exempting intermediaries from liability is the best alternative.

### *E. Dissemination and Compensation*

After liability is determined, the scope of compensation also influences fairness and efficiency. Liability to defamation can be determined without proving actual harm.[353] Deciding the scope of compensation involves additional factors that go beyond the level of the contextual breach. First, courts should consider the severity of the expression disseminated. The more obvious the defamation, the greater the compensation.

Second, the extent of dissemination is another important factor in the calculation of damage. Thus, judges should consider whether a broad or narrow audience was exposed to the expression and whether it can be located via search engines' queries. Disseminating defamation to a closed group on Facebook or to a few email recipients is a consideration for reducing damages.[354] In contrast, a large audience exacerbates the injury to reputation and should increase the amount of compensation.

Third, courts should consider the plaintiff and the defendants' conduct after the dissemination.[355] These considerations are central in traditional defamation claims and should also be considered in cases revolving around intermediaries' liability.

Fourth, the level of contextual breach influences the gravity of the harm. Therefore, courts should impose a nuanced compensation scheme that is sensitive to the degree of contextual breach. When an intermediary explicitly adopts users' defamation, and adds his own defamatory titles, the level of contextual breach is significant. In such cases, courts may conclude that the intermediary acted maliciously and may award the victim with higher compensation, or even punitive damages.[356]

Fifth, the sum of compensation should also depend on the reputation of the specific intermediary, and the magnitude ascribed to speech in the relevant platform category. Thus, judges should impose higher compensation on well-known intermediaries, and credible platforms

---

353. *See* PROSSER & KEETON, *supra* note 56, at § 116A; DAVID ELDER, DEFAMATION: A LAWYER'S GUIDE § 9.2, Westlaw (database updated Aug. 2017) (explaining that courts can reasonably compensate plaintiffs for any general damages resulting from libel or slander).

354. *See* COLLINS, *supra* note 10, at ¶ 21.18; Robert Danay, *The Medium Is Not the Message: Reconciling Reputation and Free Expression in Cases of Internet Defamation*, 56 MCGILL L.J. 1, 30 (2010).

355. *See* PROSSER & KEETON, *supra* note 63, at § 116A; *see also* COLLINS, *supra* note 10, at ¶ 21.25 (addressing possibility that claimant's conduct at trial may mitigate damages).

356. On punitive damages, see PROSSER & KEETON, *supra* note 63, at § 116A.

that disseminate defamatory comments. Less known or credible intermediaries should not be held to the same standard.

### *F. Potential Objections to the Proposed Framework*

The framework applies differential liability on intermediaries for disseminating user-generated defamation. It outlines separate standards of liability for different types of dissemination (full, selective and adoptive) in light of the degree of the breach of context and the causal link between the intermediary and defamatory content. The proposed framework structures judicial discretion and assists the courts with a just and efficient policy. Yet, several objections to the framework can be anticipated. The following section addresses these challenges and responds to them.

The first possible objection is that the proposed framework leads to over-deterrence relative to the overall immunity regime. Furthermore, this framework does not provide precise guidelines as to what qualifies as proscribed conduct. It requires an investigation on how content was taken out of context, leaving a degree of ambiguity and uncertainty. Due to the various nuances of selection, the standard of liability for selective dissemination is inconclusive. Furthermore, the extent of the defenses of defamation law under this framework is unclear. Consequently, intermediaries may act defensively and avoid selective dissemination or adoption of any content. This might stifle the flow of information and the innovation of online services.[357]

Indeed, the guidelines reduce the level of certainty that exists with the current regime of overall immunity. However, a cost-benefit analysis leads to the conclusion that relative ambiguity is a price worth paying, so that a balance will be maintained between a right to dignity and freedom of speech. In addition, the alternative of overall immunity is over-inclusive and leads to inaccuracy. A differential liability regime has more benefits than shortcomings. The framework outlines separate standards, which allow proportionate disincentives for different degrees of contextual breach, allowing for flexibility and adjustments to ever-changing situations and technologies. This regulation attempts to promote efficiency more than other proposals reviewed in scholarly work.[358] In addition, the proposed framework should not be expected to reduce certainty, since today, more than a third of internet defamation and libel claims already survive a § 230 defense.[359] By structuring

357. For example, intermediaries that are concerned with legal liability may act defensively and avoid operating important services such as a listserv.

358. *See supra* Part III.F.

359. On this inconsistency, see *supra* Part III.B. More than a third of these claims survive a § 230 defense. *See* Ardia, *supra* note 101 at 493. On the erosion of the immunity in § 230, see Eric Goldman, *Ten Worst Section 230 Rulings of 2016 (Plus the Five Best),* TECH. &

judicial discretion, judges are likely to reach more consistent, just and efficient outcomes relative to the inconsistency reflected in case law today. Certainty and consistency will grow over time as precedents accumulate.

One may argue that even if the scope of liability were to become clear over time, the disincentives may lead to over-deterrence. Consequently, intermediaries may avoid selective dissemination and adoption. This possibility however, is less realistic because most intermediaries are guided by economic considerations such as the profits garnered by advertisements on their sites.[360] Dissemination of user-generated content enhances interactive participation and boosts the intermediaries' profits from content they did not generate. In order to attract more users and profits, cost-benefit analyses may bring them to consult with lawyers regarding liability risks who may propose exposure to some level of liability. Thus, they are likely to continue disseminating users' content but avoid significant contextual breach. Some degree of a chilling effect is unavoidable, but this proposal attempts to strike the right balance between the benefits of free expression and its potential harm.[361] This conclusion also applies to non-commercial intermediaries that are normally driven by ideology since they can control their exposure to liability and avoid irresponsible dissemination.

The second objection may be directed at the immunity for disseminating defamatory content according to users' votes. One may argue that this exemption would incentivize intermediaries to develop systems that depend on users' choices. Consequently, the victims of defamation will always have to bear the cost of their damage because it would be impractical for victims to file an action against every one of the decentralized users that voted for defamatory content.[362] This results in diffusion of responsibility,[363] which leaves the innocent victim without a tenable legal recourse.

---

MARKETING L. BLOG (Jan. 4, 2017), http://blog.ericgoldman.org/archives/2017/01/ten-worst-section-230-rulings-of-2016-plus-the-five-best.htm [https://perma.cc/MFQ8-ZD7Y]; Kosseff, *supra* note 142.

360. *See* JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH, 100–02 (2011); *see generally* NICHOLAS CARR, THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE, 57–154 (2008).

361. *See* SUNSTEIN, RUMORS, *supra* note 24, at 71–72.

362. Many voters cannot be identified. Furthermore, imposing liability on voters as tortfeasors in concert, that are jointly and severally liable, is undesirable. There are significant policy considerations that support exempting users from liability for voting on content (an act carried out without thought, by automatically clicking on a button). Imposing liability on users may impede participation and burden the efficient flow of information.

363. Diffusion of responsibility is a socio-psychological phenomenon whereby many individuals are present and nobody takes responsibility for an action. *See generally,* John M. Darley & Bibb Latané, *Bystander Intervention in Emergencies: Diffusion of Responsibility*, 8 J.

Exempting the liability of intermediaries for this type of dissemination is an under-inclusive policy. Yet, despite possible negative effects of immunity, this regime is superior to other possibilities. Voting systems are neutral to defamatory content and do not enhance dissemination of defamation in particular. In many cases, these systems lead to dissemination of relevant content, advance dialogue on issues of public importance, and promote freedom of expression. Imposing liability on intermediaries for voting systems may lead intermediaries to avoid implementing these beneficial systems. By balancing the overall cost and benefits, the conclusion is that a policy which would make the victim bear the voting systems' harm is a worthwhile price.

The third objection is drawn from the development of search engines and new ways of sharing and disseminating content. It appears as if taking content out of context has become a social norm.[364] For example, in some cases, operators of public pages selectively repeat specific some users' posts or statuses in order to focus other users' attention on the most relevant or popular content.[365] Similarly, search engines regularly take short snippets out of the context of the original website and selectively reflect them in their search results in order to facilitate search. Therefore, one may argue that imposing liability on contextual breach is an unbearable burden on intermediaries. [366]

The response to this objection is that the proposed guidelines strive to improve policy regarding dissemination of defamation. Thus, it does not refer to taking content out of context in general. In cases of disseminating defamation, significant degrees of contextual breach may inflict severe harm and justify liability. When powerful intermediaries take defamatory comments out of context and inflict severe harm to third parties; the law should be a key force in regulation.[367] Due to the prevalence of contextual breach in the digital age, it is even more important to incentivize intermediaries that disseminate users' defamatory content to stick to the original context.

---

PERSONALITY & SOC. PSYCHOL. 377 (1968). In the context of user-based defamation, many individuals are responsible for defamation but no one affirmatively bears liability.

364. *See* BOYD, *supra* note 3, at 31 (explaining that electronic media "easily collapse seemingly disconnected contexts . . . . A context collapse occurs when people are forced to grapple simultaneously with otherwise unrelated social contexts that are rooted in different norms and seemingly demand different social responses.").

365. For example, a public Facebook page that repeats popular users' content with neutrality to defamation, in order to focus users' attention on relevant content, increase their attraction to the page, and earn more revenues from advertisements. This practice is part of the attention economy, and is central for platforms business models.

366. *See, e.g.*, O'Kroley v. Fastcase, Inc., 831 F.3d 352, 353–55 (6th Cir. 2016); Niemela v. Malamas, No. S146067 2015 B.C.S.C. 1024 ¶ 84 (June 16, 2015) (Can.).

367. Lessig identified "technology," "law," "markets," and "social norms" as key factors that shape and regulate the online environment. LAWRENCE LESSIG, CODE VERSION 2.0 121–23 (2006); *see generally* Tal Zarsky, *Social Justice, Social Norms and the Governance of Social Media*, 35 PACE L. REV. 154 (2015).

Search engines, which reflect specific expressions in their search results and take them out of their context lead to only mild degrees of contextual breach. First, search engines take expressions out of context only on the first layer of the search results. This layer includes snippets in the results page.[368] But, when an individual has an interest in a specific search result, he would not be satisfied with a partial quotation and he would most likely click on the link. This would expose him to the full context of the expression. By linking to the original platform, search engines preserve context. Second, Google's page rank is based on previous searches of users and the amount of links ("votes") to specific content. The search results are a result of users' signals and are not the intermediaries' exclusive choice. Thus, the proposed framework, which considers the causal link between the intermediary and the dissemination can actually justify the immunity given to search engines.[369]

One may argue that there should be complementary regulations, which would allow individuals a right of revisability if they are not public figures.[370] This discussion is beyond the scope of this paper. Regardless, the ECJ outlined the right to delist from search results in the EU.[371] Delisting from search results does not delete the source of information. Thus, the information is still kept on the original website and can be found directly. In addition, delisting is limited to searches made by the name of individuals and the information can be found by other searches that are not based on the subject's name. Thus, delisting from the search engine only obscures information and causes reduced chilling effect in comparison to removal of the speech from the internet altogether.[372] Therefore, the right to delist does not stand in direct contradiction with the proposed framework.

Americans seem to support the establishment of some form of a "right to be forgotten."[373] If the law recognizes a right for an American citizen's to be delisted, this right should be limited. It should not allow individuals to delist themselves from search results as they see fit. Instead, the law should set forth guidelines for determining when content

368. *See O'Kroley*, 831 F.3d at 355 (exempting Google for "snippets" that selectively repeated content from a linked website).

369. Note that there is a difference between users' signals and positive votes. Yet, this argument is not the main argument and only supports the previous argument regarding the mild degree of contextual breach.

370. *See generally* Andrew Tutt*, The Revisability Principle*, 66 HASTINGS L.J. 1113 (2015).

371. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [https://perma.cc/7PF2-W2DM].

372. *See* Pasquale, *Reforming the Law of Reputation*, *supra* note 239, at 517; Peguera*, supra* note 182, at 554–55.

373. *See* Kelly & Satola, *supra* note 181, at 50 (explaining that "61% of Americans favored some form of a right to be forgotten, 39% wanted a broad European-style right, and 47% believed that irrelevant search results can harm reputations.").

is inadequate or is no longer relevant and apply it in narrow contexts. This rule shall mitigate a disproportional chilling effect on speech and protect the public's right to receive information.[374]

## V. CONCLUSION

This Article is part of a series that advances a context-based theory of liability.[375] It aspires to take the first step in addressing the liability of online intermediaries for disseminating user-generated defamatory content.

This Article demonstrated the influences of dissemination on context and on the importance ascribed to content. It further mapped central types of dissemination that intermediaries use to spread users' content. Intermediaries can substantially exacerbate the harm of defamatory users' content that they publish. Therefore, an overall immunity should not apply to all types of dissemination. Following this analysis, this Article applied multidisciplinary insights to legal policy and molded a framework that proposes to observe intermediary liability through the prism of context. Following this line of thought, this Article outlined guidelines for deciding the sort of liability that intermediaries should bear. The guidelines could structure judicial discretion and assist courts to apply open-ended standards. This framework could promote consistency and lead to just and efficient outcomes, in contrast to the inconsistency reflected in case law today. The framework attempts to strike a proper balance between normative values and considerations.[376]

The proposed framework changes intermediaries' incentives for disseminating users' defamatory content. Yet the framework could apply beyond the scope of this article and may have broader potential in promoting freedom of expression in general. Online intermediaries are private entities. As such, they are not subjected to the First Amendment's public forum doctrine and can discriminate speech.[377] Furthermore, intermediaries are not required to provide coverage on

---

374. *See* Antani, *supra* note 183, at 1210 (concluding that the right should "manifest in narrow contexts where the right is deemed appropriate. For example, a right to be forgotten could be justified where analogs already exist in the law (credit reporting), private entities already engage in the practice (Google removing cyberbullying content), or important conversations surround a problematic issue (revenge porn))." Narrowly tailored rules may not violate the First Amendment. *See* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 164 (2016). ("Even in the U.S., there are ways to make the Digital Age a forgiving era, but the ways must be within the bounds of what makes Americans the most free.").

375. The first Article in the series focuses on secondary liability. *See* Lavi, *supra* note 18.

376. *See supra* Part III.E.

377. On the public forum doctrine, see DAWN NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 42–48 (2009); SUNSTEIN, #REPUBLIC, *supra* note 335, at 34–36.

issues of public importance or enhance public deliberation and debate.[378]

Whether the law should impose First Amendment obligations on intermediaries involves a complex balancing act. On the one hand, in the absence of such obligations, intermediaries may abuse their power, influence the flow of information to promote their goals, and impair the public interest. On the other hand, such general obligations may impede speech, stifle innovation and raise prices of online services.[379] This question is not within the scope of this article and is open for future debates.

Outlining specific procedures, which apply only to the dissemination of defamation, may be complex. An intermediary who aims to manage risk efficiently and reduce its exposure to liability may be incentivized to use types of dissemination that do not lead to a significant degree of contextual breach. In light of this behavior, the proposed framework has a potential for promoting fairer practices of dissemination and enhancing speech in general.

This Article is not the last word on the topic. There are further avenues of analytic inquiry and more to discuss regarding intermediaries' liability in related contexts. It leaves open questions regarding intermediaries' liability for selective dissemination of specific types of content for promoting services or products.[380] Should the law regulate commercial dissemination of content online? [381] Should these practices lead to liability for misrepresentation or deception? What about selective nontransparent dissemination of information on political candidates that influence election results?[382] What lessons should be learned

---

378. The Federal Communications Commission abolished the "Fairness Doctrine," which imposed public interest obligations on traditional intermediaries. This doctrine applied to broadcasters, and online intermediaries were never subjected to it. *See* NUNZIATO, *supra* note 35, at 41–42; William H. Read & Ronald Alan Weiner, *FCC Reform: Governing Requires a New Standard*, 49 FED. COMM. L.J. 289, 295 (1997).

379. *See* Adam Thierer, *The Perils of Classifying Social Media Platforms as Public Utilities*, 21 COMMLAW CONSPECTUS 249, 278–82 (2013).

380. *See, e.g.*, James Grimmelmann*, The Law and Ethics of Experiments on Social Media Users,* 13 COLO. TECH. L.J. 219 (2015) (describing ethical issues related to social media experiments wherein intermediaries selectively disseminate users' content in a non-transparent way).

381. On dissemination of commercial content by users for a benefit, see Robert Sprague & Mary Ellen Wells, *Regulating Online Buzz Marketing: Untangling a Web of Deceit*, 47 AM. BUS. L.J. 415 (2010). *See also* Shannon Byrne, *The Age of the Human Billboard: Endorsement Disclosures in New Millennia Media Marketing,* 10 J. BUS. & TECH. L. 392 (2015).

382. For a discussion on these practices, see ZEYNEP TUFEKCI*,* TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST 264–65 (2017) (discussing "disinformation campaigns" that exploited social media algorithms to influence the U.S. presidential election); Zeynep Tufekci, *Mark Zuckerberg Is in Denial*, N.Y. TIMES (Nov. 15, 2016) https://www.nytimes.com/2016/11/15/opinion/mark-zuckerberg-is-in-denial.html (last visited Dec. 20, 2017) (discussing possible stifling of "real journalism" during the 2016 presidential election season); *see generally* Zittrain*, Engineering Elections*, *supra* note 8 (raising concerns over "digital gerrymandering");

for the age of the internet of things that merges online and offline networks, erodes the line between online and the real world, allows personalized selective dissemination of information, and more extensive influences on context?[383] Another challenge concerns the liability of users for taking content out of context by spreading third parties' defamatory content. Should the court hold them responsible for exacerbating harm? Can the proposed guidelines regulate users' liability for dissemination? Or should the courts exempt individual disseminators from liability?[384] These challenges and others are projects for another day.

383. For a discussion on these effects, see generally MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW 42 (2015) (referring to the elimination of the dichotomy between online and offline as the "onli*f*e [sic] world"); Michal S. Gal & Niva Elkin-Koren*, Algorithmic Consumers,* 30 HARV. J.L. & TECH. 309 (2017); SILVERMAN*, supra* note 6, at 298–310; JOSEPH TUROW*,* THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER (2017).

384. In many cases users share content with the click of a button, without thinking of the consequences in contrast to an intermediary which calculates the benefits and risks of dissemination. *Cf.* NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US 83–85 (2014) (discussing phenomenon where technology hinders a user's deep thinking). Furthermore, individual disseminators are influenced by information and reputation cascades. Thus, many times they spread content because others do so. On cascades, see SUNSTEIN, RUMORS, *supra* note 24, at 21–38.