Harvard Journal of Law & Technology
Volume 28, Number 1 Fall 2014

INTERMEDIARY LIABILITY FOR HARMFUL SPEECH: LESSONS FROM ABROAD

*Corey Omer**

TABLE OF CONTENTS

I. INTRODUCTION

Nearly twenty-three years ago, the question of intermediary liability for defamatory content posted online by a third party arose in *Cubby, Inc. v. CompuServe Inc.*,[1] the first documented U.S. cybertort case.[2] The case was brought before the courts when the World Wide

* Harvard Law School, LL.M. and Frank Knox Fellow, 2014; McGill University, Faculty of Law, B.C.L., LL.B., 2011. Thanks to Professor Urs Gasser for supervising the paper that led to this Note, the faculty at the Berkman Center for Internet & Society for fostering my interest in cyberlaw, and Harry Khanna and Steve Omer for their insightful comments. A special thanks to Article Editor Brianna Beswick for her dedication, patience, and keen editorial pen. Finally, thanks to the staff of the *Harvard Journal of Law and Technology* for their hard work in bringing this Note to print.

1. 776 F. Supp. 135 (S.D.N.Y. 1991).

2. Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 364 (2005) ("The first cybertort case was decided in 1991, when CompuServe, Inc. was held not liable for a third party's publication of defamatory statements on its services."). This case, Cubby, Inc. v. CompuServe Inc., was decided only a year after a federal

Web was still in its infancy.[3] Over the intervening years, much has changed with respect to both Internet technology and law, but the debate regarding the proper contours of intermediary liability for user-generated content has persisted relatively unabated.[4] This debate continues to vex courts, legislators, academics, Internet intermediaries, and Internet users.

Adopting a comparative methodology, this Note proposes that the United States rethink aspects of its approach to intermediary liability for user-generated content by learning from the experiences of and challenges faced by other Western legal jurisdictions with which it regularly interacts. While accounting for the unique policy goals and obstacles faced by the United States, the proposed approach would bring the American legal regime closer in line with those of Canada, the European Union, and the United Kingdom. The scheme proffered is directed at online service providers that host socially unacceptable or harmful user-generated content. The scheme would not require intermediaries to assess the legality of content themselves — intermediary *judgment* — but rather, would hinge intermediary liability on failure to act on knowledge of content judged illegal or defamatory by an external authority. Ultimately, the proposal strives to grant victims of defamatory speech greater ability to have illegal or defamatory content removed.

Given the breadth of this area of law and the myriad issues it encompasses, the in-depth treatment of one legal question by this Note precludes exploration of others. This Note deals with intermediaries that host user-generated content online. It does not deal with intermediaries that provide only technical and physical infrastructure for the transmission of information, e.g., data processing, content delivery,

---

court mentioned the term "Internet" for the first time, dealing with a conviction for the creation of an Internet worm. *Id.* (discussing United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991)).

3. *See World Wide Web Timeline*, PEW RESEARCH INTERNET GROUP (Mar. 11, 2014), http://www.pewinternet.org/2014/03/11/world-wide-web-timeline.

4. For examples of this trend from 1994 to present, see I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1000–06, 1041–48 (1994); Lai Leng Fong et al., *Internet Defamation: Liability of Intermediaries and Alternative Dispute Resolution*, 19 SING. L. REV. 202 (1998); Rosa Julià-Barceló & Kamiel J. Koelman, *Intermediary Liability in the E-Commerce Directive: So Far So Good, but It's Not Enough*, 16 COMPUTER L. & SECURITY REV. 231 (2000); Tomas A. Lipinski, Elizabeth A. Buchanan & Johannes J. Britz, *Sticks and Stones and Words that Harm: Liability vs. Responsibility, Section 230 and Defamatory Speech in Cyberspace*, 4 ETHICS & INFO. TECH. 143 (2002); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239 (2005); Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237 (2007); Jeff Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, 15 J. TECH. L. & POL'Y 123 (2010); 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 (2010); Margo Kaminski, *Positive Proposals for Treatment of Online Intermediaries*, 28 AM. U. INT'L L. REV. 203 (2012).

payment processing, and Internet access services to users ("ISPs").[5] Search engines also raise unique challenges not expressly addressed herein.[6] The scope of this Note is limited to user-generated content considered to be harmful speech. The Note focuses on defamatory and libelous speech, but also touches upon criminal speech, such as child pornography and hate speech. Infringements of intellectual property rights such as copyright and trademark raise fascinating legal questions and cross-border challenges, but are not covered by this Note.[7] Nor does this Note address "cyber-bullying" and its equally distasteful variant "slut-shaming." While repugnant, the speech involved in such conduct may constitute constitutionally protected opinion.[8] Many proposals have been put forward on how to best address cyber-bullying,[9] but to the extent that such speech does not constitute defamation, it falls beyond the scope of the proposal advanced herein.

This Note is divided into three further parts. Part II discusses the relevance of three cyber-trends: (1) the ever-growing role of online

---

5. Examples of such intermediaries include Verizon ("[p]rovid[ing] access to the Internet to households, businesses, and government"), Register.com ("[t]ransform[ing] data, prepar[ing] data for dissemination, or stor[ing] data or content on the Internet for others"), and Visa ("[p]rocess[ing] Internet payments"). Organization for Economic Co-operation and Development [OECD], *The Economic and Social Role of Internet Intermediaries*, DSTI/ICCP(2009)9/FINAL 9 (Apr. 2010), *available at* http://www.oecd.org/sti/ieconomy/44949023.pdf.

6. *See, e.g.*, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, [2014] E.C.R.I. (delivered May 13, 2014); Michael A. Carrier, *Google and Antitrust: Five Approaches to an Evolving Issue*, HARV. J.L. & TECH. (OCCASIONAL PAPER SERIES) 1 (July 2013), *available at* http://jolt.law.harvard.edu/antitrust/articles/Carrier.pdf; Urs Gasser, *Regulating Search Engines: Taking Stock and Looking Ahead*, 8 YALE J.L. & TECH. 201 (2006).

7. For articles related to intermediary liability for the infringement of intellectual property rights, see for example Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009); Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101 (2007) (comparing intermediary liability in the U.S. for illegal speech, copyright, and trademark); Christopher M. Swartout, *Toward a Regulatory Model of Internet Intermediary Liability: File-Sharing and Copyright Enforcement*, 31 NW. J. INT'L L. & BUS. 499 (2011); Ignacio Garrote Fernández-Díez, *Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringements of Copyright and Related Rights*, WORLD INTELL. PROP. ORG., http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf; Daniel Seng, *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*, WORLD INTELL. PROP. ORG., http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf.

8. *See* Lee Goldman, *Student Speech and the First Amendment: A Comprehensive Approach*, 63 FLA. L. REV. 395, 413 (2011).

9. *See, e.g.*, Alison Virginia King, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845 (2010); Karly Zande, *When the School Bully Attacks in the Living Room: Using* Tinker *To Regulate Off-Campus Student Cyberbullying*, 13 BARRY L. REV. 103 (2009); Emily Poole, Note, *Hey Girls, Did You Know? Slut-Shaming on the Internet Needs to Stop*, 48 U.S.F. L. REV. 221 (2013); Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41 (Sept. 9, 2007), http://www.yalelawjournal.org/forum/regulating-cyberbullies-through-notice-based-liability.

intermediaries, (2) the unprecedented rate at which user-generated content is produced and distributed, and (3) the concurrent assertion of personal jurisdiction over online actors by courts in multiple jurisdictions. Part III compares the law on intermediary liability in four jurisdictions: the United States, Canada, the European Union, and the United Kingdom. Each has adopted a different approach to the issue, giving rise to various benefits and challenges. This survey does not provide an exhaustive review of the law in each of the jurisdictions. Instead, it seeks to describe in broad strokes the treatment of online intermediaries in each jurisdiction and identify significant legislative and jurisprudential developments as well as areas of continued controversy. Part IV sets out the proposed changes to U.S. law governing intermediary liability.

Part IV is divided into three subparts, based on the nature of the content at issue: (1) content declared to be illegal or defamatory, (2) content not yet judged illegal where the poster of the content is known, and (3) content not yet judged illegal where the poster of the content is unknown. Part IV contends that where content is declared illegal or defamatory by a competent authority, regardless of whether the poster is known or unknown, removal orders should be enforceable against online intermediaries. Contrary to the current state of U.S. law, an intermediary who refuses to remove content after receiving notice of a duly issued removal order should not be able to rely on the safe harbor from liability for user-generated content typically granted to intermediaries by section 230(c) of the Communications Decency Act of 1996 ("CDA").[10] In such circumstances, the intermediary should be held liable as the content's publisher. On the other hand, where content has not yet been judged illegal or defamatory and the identity of the poster is *known*, Part IV submits that the American approach operates exactly as it should, directing the claimant to pursue the poster rather than the intermediary and guaranteeing the latter full immunity.[11] Finally, where content has not yet been judged illegal or defamatory and the identity of the poster is *unknown*, a claimant is often left without an efficient or meaningful remedy under U.S. law.[12] Part IV proposes a streamlined procedure by which a claimant can seek to establish that content published by an unknown poster is *prima facie* illegal or defamatory. If that *prima facie* showing is made, Part IV argues that the impugned content should — like content actually declared illegal or defamatory — be excluded from the scope of section 230 CDA's safe harbor. The *prima facie* determination would, however, have no immediate effect on the liability of the intermediary. It would merely open the way to, not determine the outcome of,

10. Communications Decency Act of 1996, Pub. L. No. 104-104 § 230(c) (1996).
11. *See infra* Part IV.B.
12. *See infra* Part IV.C.

an action against the intermediary as publisher of the impugned content.

II. RELEVANT CYBER-TRENDS

The discussion of the legal role of intermediaries in regulating socially unacceptable or harmful forms of speech online must be framed and informed by three interrelated cyber-trends: (1) the dominance of intermediaries, (2) the explosion of user-generated content, and (3) the concurrent assertion of personal jurisdiction over online actors by courts in multiple jurisdictions.

A. Dominance of Online Intermediaries

In the mid-to-late 1990s, the Internet was heralded as the harbinger of "disintermediation,"[13] the technological gateway into an era of "friction-free capitalism."[14] Academics predicted that the role of traditional intermediaries — brick-and-mortar stores, publishing houses, newspaper editors, financial brokers, even national governments[15] — would rapidly shrink, and with it the constraints imposed by such gatekeepers upon an individual's access to commerce, culture, and information.[16] Users would interact and deal with each other directly in a gloriously unmediated and unbound digital universe "in which market information will be plentiful and transaction costs low."[17]

The sounding of the death knell for intermediaries proved premature. They did not disappear. Rather, "[w]e simply swapped one set of middlemen for another."[18] The Internet became a newfangled "intermediated information exchange,"[19] and while many of the traditional intermediaries did falter,[20] a new guard quickly positioned itself at the

13. Andrew L. Shapiro, *Digital Middlemen and the Architecture of Electronic Commerce*, 24 OHIO N.U. L. REV. 795, 795 (1998).

14. BILL GATES, THE ROAD AHEAD 180 (2d ed. 1996).

15. *See, e.g.*, John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

16. *See* Derek E. Bambauer, *Middlemen*, 65 FLA. L. REV. FORUM 1 (2013), http://www.floridalawreview.com/wp-content/uploads/Bambauer_Forum.pdf; Shapiro, *supra* note 13, at 795–97.

17. GATES, *supra* note 14, at 181. *But see* Shapiro, *supra* note 13, at 800–05 ("[T]he new architecture of commerce may not, or at least need not, be as free of middlemen as some cyber-romantics would have us believe. As will become clear in a moment, I think this is almost certainly a good thing.").

18. Bambauer, *supra* note 16, at 1.

19. Jacqueline D. Lipton, *Law of the Intermediated Information Exchange*, 64 FLA. L. REV. 1337, 1337 (2012).

20. *See, e.g.*, Paul Farhi, *For Tower Records, End of Disc*, WASH. POST (Dec. 11, 2006), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/10/AR2006121001003.html (bemoaning the end of the record store culture); Terry Pristin, *Struggling Newspapers Sell Off Old Headquarters*, N.Y. TIMES, Oct. 22, 2013, at B8 (discussing struggling newspaper industry); Julie Bosman, *After 244 Years, Encyclopaedia*

chokepoints of cyberspace. Arguably today, "[n]othing can happen online that does not involve one or more of these actors."[21] Indeed, some of these intermediaries have become household names and the functions they serve have become iconic representations of Web 2.0[22]: Google and searches, Facebook and social media, LinkedIn and professional networking, YouTube and streaming video content, Wikipedia and general knowledge, Twitter and microblogging, and Amazon and e-commerce, among others.[23]

The centrality of online intermediaries means that the rules governing liability for user-generated content will necessarily have powerful and broad effects. Carefully crafted regulations could suppress undesirable content while protecting freedom of expression on online platforms. An inadequate or untailored approach could lead to the over- or under-regulation of a vast quantity of online speech.

B. Explosion of User-Generated Content

As the clout of online intermediaries has grown, so too has the pervasiveness of the Internet and the sheer quantity of new user-generated content. Today, 87% of U.S. adults use the Internet, including 97% of those aged 18–29, 97% of those with college degrees, and 99% of those living in households earning $75,000 or more.[24] Every minute YouTube users upload 100 hours of new video,[25] Instagram users share over 41,000 new photos,[26] Twitter users tweet over 347,000 times,[27] and Facebook users update 293,000 statuses.[28] Ten

---

Britannica Stops the Presses, N.Y. TIMES MEDIA DECODER, (Mar. 13, 2012), http://mediadecoder.blogs.nytimes.com/2012/03/13/after-244-years-encyclopaedia-britannica-stops-the-presses/.

21. Lipton, *supra* note 19, at 1338; *see also* Ardia, *supra* note 4, at 377.

22. Defined as "a second generation in the development of the World Wide Web, conceived as a combination of concepts, trends, and technologies that focus on user collaboration, sharing of user-generated content, and social networking." *Web 2.0 Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/web+2.0 (last visited Dec. 18, 2014).

23. All of the listed websites rank among the twelve most visited websites on the Internet. *The Top 500 Sites on the Web*, ALEXA, http://www.alexa.com/topsites (last visited Dec. 18, 2014).

24. *The Web at 25 in the U.S.*, PEW RESEARCH INTERNET PROJECT (Feb. 27, 2014), http://www.pewinternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf. As of December 31, 2013, there were over 2.8 billion Internet users worldwide. *Internet Users in the World*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited Dec. 18, 2014).

25. *Statistics*, YOUTUBE, http://www.youtube.com/yt/press/statistics.html (last visited Dec. 18, 2014).

26. *Press Page*, INSTAGRAM, http://instagram.com/press/ (last visited Dec. 18, 2014) (sixty million average photos per day).

27. *About*, TWITTER, https://about.twitter.com/company (last visited Dec. 18, 2014).

28. *The Top 20 Valuable Facebook Statistics — Updated October 2014*, ZEPHORIA, http://zephoria.com/social-media/top-15-valuable-facebook-statistics/ (last visited Dec. 18,

years ago, only the last of these platforms even existed, and it was still in its nascent stage.[29]

The unprecedented rate and magnitude at which users generate and distribute content suggest that any liability scheme relying on intermediary monitoring, knowledge, or assessment of particular items of user-generated content is impractical. Such a scheme would incentivize either the suppression of protected speech or the absence of self-regulation. If liability of online intermediaries for illegal or defamatory user content is triggered by notice of the fact that the impugned content exists or is contingent on the content's removal or "takedown," intermediaries will be strongly incentivized to overcompensate and trade-off the possibility of censoring their users' legitimate expression for the certainty of avoiding legal liability.[30] By contrast, if self-regulation and monitoring triggers intermediary liability, intermediaries will be inclined to turn a blind eye to users' problematic content entirely.[31]

C. Concurrent Assertion of Personal Jurisdiction over Online Actors

Finally, due to the global reach of the Internet, an increasing number of online actors and intermediaries are finding themselves subject to the personal jurisdiction of multiple national and international courts.[32] Perhaps the most well known of these cases is *Yahoo!*,

---

2014); *see also* Tamiz v. Google, [2013] EWCA (Civ) 68, [16], [2013] 1 W.L.R. 2162 (Eng.) (250,000 new words are added every minute to blogs hosted by Google).

29. *Company Info*, FACEBOOK, https://newsroom.fb.com/company-info/ (last visited Dec. 18, 2014).

30. *See* CTR. FOR DEMOCRACY & TECH., INTERMEDIARY LIABILITY: PROTECTING INTERNET PLATFORMS FOR EXPRESSION AND INNOVATION 4 (Apr. 2010), https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf (observing that notice and takedown intermediary liability "chills expression online and transforms technological intermediaries into content gatekeepers"); Rebecca Ong, *Internet Intermediaries: The Liability for Defamatory Postings in China and Hong Kong*, 29 COMPUTER L. & SEC. REV. 274, 281 (2013) ("[T]he concern remains that to avoid liability, Internet intermediaries will promptly seek to remove the offending material without first verifying the 'truth' of the material, effectively making them, [sic] the judge and the jury over any complained postings or materials."); Daithí Mac Síthigh, *The Fragmentation of Intermediary Liability in the UK*, 8 J. INTELL. PROP. L. & PRAC. 521, 525–26 (2013); Emily Barabas, *Internet Defamation Double Whammy in the UK: New Court Decision Plus New Legislation Threaten Online Free Expression*, CTR. FOR DEMOCRACY & TECH. (Feb. 27, 2013), https://cdt.org/internet-defamation-double-whammy-in-the-uk-new-court-decision-plus-new-legislation-threaten-online-free-expression/ ("In an attempt to reduce risk, companies will likely err on the side of removal, taking down questionable but lawful content to the detriment of free expression.").

31. *See infra* notes 63–72 and accompanying text.

32. Jurisdiction has been described as "a word of many, too many, meanings." United States v. Vanness, 85 F.3d 661, 663 n.2 (D.C. Cir. 1996). Herein, personal jurisdiction refers to "a court's power to bring a person into its adjudicative process." Personal Jurisdiction Definition, BLACK'S LAW DICTIONARY (9th ed. 2009); *see also* Niloufer Selvadurai, *The Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving Towards Unification?*, 13 J. TECH. L. & POL'Y 124, 128 (2013) ("A

Inc. v. La Ligue Contre Le Raisme et L'Antisemitisme.[33] Yahoo! had allowed French users to participate in global auctions of Nazi memorabilia, the display and sale of which is illegal under French law.[34] Despite the auction platform being in English, hosted in California, and primarily targeted at American users, the French Tribunal de grande instance de Paris asserted jurisdiction over Yahoo!. The French court's broad jurisdictional finding was based on the ability of individuals in France to view the illegal content and the existence of technological measures that Yahoo! could employ to minimize or eliminate such access.[35] Among other things, the court ordered Yahoo! to "take all measures to dissuade and render impossible"[36] access of French users to the illegal content.

Courts have adopted varied tests to determine whether they can assert jurisdiction over non-resident actors in cases involving online content. The standard applied in the Yahoo! France case is relatively in line with the approach of other European Union member states,[37]

State is found to have personal jurisdiction over a foreign defendant when it has authority to require a defendant to appear before its courts and defend a claim.").

33. UEJF & LICRA v. Yahoo!, Inc. & Yahoo France, Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, N. 00/05308 (finding Yahoo! liable for its violation of French Penal Code R. 645-1). Though Yahoo! had a French subsidiary, Yahoo! France, the court asserted jurisdiction over the American-based site and company. *Id*.

34. CODE PÉNAL [C. PÉN.] art. R645-1 (Fr.).

35. UEJF & LICRA v. Yahoo!, Inc. & Yahoo France, Tribunal de grande instance (May 2000); LICRA & UEJF v. Yahoo!, Inc. & Yahoo France, Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, N. 00/05308 (affirming the *Yahoo France, May* decision and holding that after consulting the experts Vinton Cerf, Ben Laurie, and Francois Wallon, the court was of the view that it was feasible for Yahoo! to comply with the order restricting the access of French users using IP filtering technology).

36. UEJF & LICRA v. Yahoo!, Inc. & Yahoo France, Tribunal de grande instance (May 2000), *translated by* author (original text states "prendre toutes les mesures de nature à dissuader et à rendre impossible").

37. *See* Council Regulation 44/2001, 2000 O.J. (L 12), arts. 2(1), 5(3) (EC) (EU member state domiciliary may be sued in matters "relating to tort, *delict* or *quasi-delict*" either in the courts of the defendant's state of residence or in the member state where the harm was suffered); Csongor István Nagy, *The Word is a Dangerous Weapon: Jurisdiction, Applicable Law and Personality Rights in EU Law — Missed and New Opportunities*, 8 J. PRIVATE INT'L L. 251, 253–64 (2012); Richard Freer, *American and European Approaches to Personal Jurisdiction Based upon Internet Activity*, (Emory Univ. Sch. Of L. Pub. L. & Legal Theory Research Paper No. 07-15, 2007), http://ssrn.com/abstract=1004887. *But see* Case C-68/93, Shevill v. Presse Alliance SA, 1995 E.C.R. I-450 (tempering the harm-suffered jurisdiction by holding that a plaintiff could sue only for the harm occasioned in that member state, not for all harm occasioned by the publication worldwide); Joined Cases C-509/09 & C-161/10, eDate Advertising GmbH v. X; Martinez v. MGN Ltd., [2011] E.C.R. I-10269 (extending *Shevill* to online communication delicts by holding that "distribution" of the publication means "accessibility" online, but adding that a person injured by such a delict may also bring the entire claim for damages before the court of his or her "centre of interests," which is generally the victim's country of principle residence or professional activity). In the now infamous "Vividown case," the Milan Court of Appeals also held that it had jurisdiction over Google for user-uploaded content on its U.S. servers based on the harm suffered in Italy. *See* Federica De Santis & Laura Liguori, *The Italian 'Google Vividown' Case: ISPs' Liability for User-Generated Content*, LAW FEED (Apr. 3, 2013),

subject to the caveat that an electronic commerce service provider domiciled in the European Union cannot generally be "made subject to stricter requirements than those provided for by the substantive law in force in the Member State in which that service provider is established."[38]

In the United States, a non-resident defendant can be haled into court if there are "continuous and systematic" activities by the defendant in the forum state[39] or if "(1) the defendant [has] sufficient 'minimum contacts' with the forum state, (2) the claim asserted . . . arise[s] out of those contacts, and (3) the exercise of jurisdiction [is] reasonable"[40] according to "'traditional notions of fair play and substantial justice.'"[41] The minimum contacts requirement is the "constitutional touchstone"[42] of the test and generally requires a non-resident to have "purposefully avail[ed] itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws."[43]

In Canada, the applicable test — the presence of a "real and substantial connection" between the defendant and the forum — has proven to be a very low bar to the assumption of jurisdiction in defamation cases.[44]

---

http://www.portolano.it/2013/04/the-italian-google-vividown-case/. German courts have held that under section 32 of the *Zivilprozessordnung* (Code of Civil Procedure) they have jurisdiction over non-European defendants if the tortious act took place in Germany or if the relevant protected interest was harmed in Germany. Holger P. Hestermeyer, *Personal Jurisdiction for Internet Torts: Towards an International Solution?*, 26 NW. J. INT'L L. & BUS. 267, 280–86 (2006). This generally boils down to a mere accessibility test in non-competition cases. *See id.*

38. eDate Advertising GmbH, [2011] E.C.R. I-10269, para. 68 (holding pursuant to E-Commerce Directive, pmbl. Recital 22, art. 3). For a more detailed discussion of why this does not conflict with Council Regulation 44/2001, see LORNA A. GILLIES, ELECTRONIC COMMERCE AND INTERNATIONAL PRIVATE LAW, 66–68 (2008).

39. *See* Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414–16 (1984).

40. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1122–23 (W.D. Pa. 1997).

41. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940).

42. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474 (1985).

43. Hanson v. Denckla, 357 U.S. 235, 253 (1958). Various tests have been developed to assess purposeful availment with respect to online actors. The first leading approach is the *Zippo* "sliding scale approach" which looks at the "nature and quality of [the website's] commercial activity." 952 F. Supp. at 1123–24. The second leading approach is the *Calder v. Jones* "effects and targeting test," which looks at the intention of the website to target the forum state and where foreseeable harm was suffered. 465 U.S. 783, 789–90 (1984); *see also* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 243 F. Supp. 2d 1073, 1089 (C.D. Cal. 2003); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001).

44. *See* Club Resorts Ltd. v. Van Breda, [2012] 1 S.C.R. 572 (Can.). In cases of defamation, an allegation of publication in the state (that is, commission of the tort) is recognized as a presumptive connecting factor that *prima facie* entitles the court to assume jurisdiction under the *lex loci delicti* (the place of the tort) principle. "[T]he tort of defamation occurs upon publication to a third party — that is, when the allegedly defamatory material is read

Similarly, prior to the passage of the Defamation Act of 2013,[45] the United Kingdom was viewed as an attractive pick for plaintiff forum shoppers due to its flexible jurisdictional requirements and generous libel law.[46] Many foreign defendants — some with at best tenuous connections to the United Kingdom[47] — found themselves before the jurisdiction's courts. As one commentator quipped, a "quick glance at previous [libel] case law is a Forbes List of the foreign rich and famous . . . ."[48] The 2013 Defamation Act has, however, circumscribed the jurisdiction of U.K. courts over non-European resident defendants in libel actions.[49]

Under the aforementioned tests, several states may be able to assert jurisdiction over a single online intermediary for a particular piece of user-generated content. All the legal systems surveyed provide some standard by which a court can exercise long-arm jurisdiction over non-resident defendants; most of these standards are relatively non-onerous. Such jurisdictional overlap lends itself to forum shopping, or "libel tourism."[50] In its recent decision in *Éditions Écosociété Inc.*, the Supreme Court of Canada expressly noted that

---

or downloaded by someone other than the plaintiff or the publisher." Éditions Écosociété Inc. v. Banro Corp., [2012] S.C.R. 636, para. 57 (Can.). Republication can also trigger the liability of the original author in some instances. Breeden v. Black, [2012] S.C.R. 666, para. 20 (Can.). A second approach that has gained some currency in Canada is looking for the location of "the most substantial harm to reputation." *See Éditions Écosociété Inc.*, 2012 SCC 18, [2012] 1 S.C.R. 636 at para. 62. Quebec courts have recently followed this approach, relying primarily on the domicile of the person attacked and the location where the injury was suffered. *See, e.g.*, Gravel v. Lifesitenews.com, 2013 QCCS 36 (Can.); Cohen v. Desert Eagle Res. Ltd., 2012 QCCS 5654 (Can.). Finally, a small minority of Canadian courts have in the past applied the *Zippo* approach. *See* Braintech, Inc. v. Kostiuk (1999) 171 D.L.R. 4th 46, para. 60 (Can. B.C. C.A.). For a comparison between the Canadian and American approaches to personal jurisdiction, see Frank Chirino, Note, *Business Without Borders: Tailoring American and Canadian Personal Jurisdiction Principles To Provide Greater Certainty for Online Businesses*, 12 SW. J. L. & TRADE AM. 97 (2005).

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

46. *See* Lili Levi, *Addressing "Libel Tourism," in* TRANSNATIONAL CULTURE IN THE INTERNET AGE 55, 56–60 (Sean A. Pager & Adam Candeub eds., 2012); Geoffrey Wheatcroft, *The Worst Case Scenario*, GUARDIAN (Feb. 28, 2008), http://www.theguardian.com/commentisfree/2008/feb/28/pressandpublishing.law.

47. *See, e.g.*, Mafhouz v. Ehrenfeld, [2005] EWHC (QB) 1156 (Eng.), [22], [65] (holding that the English courts had jurisdiction on the basis that twenty-three copies of the allegedly defamatory book, which was never published in the United Kingdom, had been ordered from Amazon for distribution in England).

48. Sally Martin, *United Kingdom: The Defamation Act 2013: The Emperor's New Clothes?*, MONDAQ (Dec. 20, 2013), http://www.mondaq.com/x/282472/Libel+Defamation/The+Defamation+Act+2013+The+Emperors+New+Clothes.

49. *See* Defamation Act, 2013, c. 26, § 9; Martin, *supra* note 48 (Under the 2013 Act, "a court cannot hear the case of a defendant who is not domiciled in the UK or another EU or Lugano Convention State unless it is satisfied that of all the places publication has taken place, England and Wales is clearly the most appropriate.").

50. *See, e.g.*, Ehrenfeld v. Mahfouz, 881 N.E.2d 830, 834 (N.Y. 2007) (acknowledging the "pernicious" effect of "libel tourism," "the use of libel judgments procured in jurisdictions with claimant-friendly libel laws — and little or no connection to the author or purported libelous material — to chill free speech in the United States").

defendants may be liable for defamation in more than one jurisdiction and acknowledged the associated challenge of libel tourism:

> The defendants in this action have expressed the concern that an overly flexible application of the real and substantial connection test would render them liable in defamation in more than one jurisdiction. Indeed, given the elements of the tort of defamation, if an allegedly libellous book is distributed in more than one jurisdiction, then an inference may be drawn that the libellous material has been published in all these jurisdictions. If publication is sufficient to connect the plaintiff's claim to a given jurisdiction, then the courts of more than one jurisdiction could potentially assume jurisdiction over the same tort.
>
> The elements of a tort such as defamation potentially vary from one jurisdiction to another, thus making it easier or more difficult to sue depending on one's choice of jurisdiction. That being the case, a plaintiff might make a strategic choice and sue in the jurisdiction in which he or she enjoys the greatest juridical advantage. This is the well-known problem of "forum shopping" or "libel tourism."[51]

These concerns are amplified in the online context, where "communications dissect[] and transcend[] national boundaries. Material published on the internet can be uploaded in one state, downloaded in another, and viewed in a large number of other states. Damage is typically simultaneously suffered in multiple states . . . ."[52]

Overlapping personal jurisdiction over intermediaries coupled with the disparity in their substantive legal treatment across the jurisdictions surveyed has several undesirable consequences. As already mentioned, litigants are encouraged to forum shop. Moreover, intermediaries lack a unifying international standard with which to align their conduct, the free functioning of markets is hampered,[53] and the

---

51. 2012 SCC 18, [2012] 1 S.C.R. 636, at paras. 35–36 (Can.).

52. Selvadurai, *supra* note 32, at 1; *see also* Reno v. ACLU, 521 U.S. 844, 851 (1997) (Cyberspace is "located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."); Barrick Gold Corp. v. Lopehandia, (2005) 71 O.R. 3d 416, at para. 62 (Can. Ont. C.A.) (noting that the Internet provides the opportunity for "virtually limitless international defamation"); Bryan G. Baynham & Daniel J. Reid, *The Modern-Day Soapbox: Defamation in the Age of the Internet*, CLEBC Defamation Law Paper No. 3.1 (2010), https://www.cle.bc.ca/PracticePoints/LIT/11-ModernSoapbox.pdf.

53. *See* Council Directive 2000/31/EC, 2000 O.J. (L 178), pmbl. Recital 40 [hereinafter E-Commerce Directive] ("Both existing and emerging disparities in Member States' legisla-

legal and policy balances struck by individual legislatures risk being undermined by the law of more restrictive jurisdictions — the "slowest ship in the convoy"[54] problem.[55]

Many solutions — both legal[56] and code-based or al[57] — have been proposed to address the challenge of concurrent jurisdiction over online actors. Proposals include reining in the reach of long-arm jurisdiction through legislative solutions,[58] harmonizing international Internet jurisdiction rules,[59] relying on geolocation technologies such as IP filtering,[60] limiting the enforceability of foreign judgments,[61] and employing the *forum non conveniens* doctrine.[62] While these measures minimize or avert the problem to varying degrees, the challenge posed by concurrent jurisdiction remains.

---

tion and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition . . . .").

54. Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, *in* WHO RULES THE NET? 13, 19–20 (Adam Thierer & Clyde Wayne Crews Jr. eds. 2003).

55. *See* Thomas Schultz, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 799, 812–14 (2008).

56. *See infra* notes 57–58, 60–61.

57. *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 (1998).

58. This approach is exemplified by the U.K.'s Defamation Act, 2013, c. 26, § 9.

59. *See* Hestermeyer, *supra* note 37, at 286–88; Selvadurai, *supra* note 32.

60. This approach was the solution suggested by the French Tribunal de grande instance de Paris in the Yahoo! France case. *See* Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, 00/05308. *See generally* Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61 (2011); Dan Jerker B. Svantesson, *Geo-location Technologies and Other Means of Placing Borders on the 'Borderless' Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101 (2004).

61. *See* Schultz, *supra* note 55, at 813 (Limited enforcement jurisdiction "acts as a limiting factor, reducing the overlapping of directly effective regulations to the various states where Internet actors have a presence or assets . . . ."). Perhaps the clearest example of enforcement jurisdiction as a limiting factor is the United States' Securing the Protection of Our Enduring and Established Constitutional Heritage Act (SPEECH Act), 28 U.S.C. § 4101 (2010), signed into law on August 10, 2010, which is a "libel tourism" law that prohibits domestic U.S. courts from recognizing or enforcing foreign defamation judgments unless "the defamation law applied . . . provided at least as much protection for freedom of speech and press in that case as would be provided by the first amendment to the Constitution of the United States and by the constitution and law of the State in which the domestic court is located . . . ." *Id.* § 4102(a)(1)(A). Alternatively, enforcement is recognized if, "even if the defamation law applied . . . did not provide as much protection . . ., the party opposing recognition or enforcement of that foreign judgment would have been found liable for defamation by a domestic court applying the first amendment to the Constitution" and State law. *Id.* § 4102(a)(1)(B).

62. *See* Éditions Écosociété Inc. v. Banro Corp., 2012 SCC 18, [2012] 1 S.C.R. 636, para. 36 (Can.) (LeBel, J., writing for a unanimous Supreme Court of Canada, proposing to address the problems of forum shopping and libel tourism "at the *forum non conveniens* stage of the analysis").

III. APPROACHES TO INTERMEDIARY LIABILITY

This Part surveys the legal framework for intermediary liability in the United States, Canada, the European Union, and the United Kingdom, explaining the law of each jurisdiction in broad strokes. The goal is not to provide an exhaustive review of the minutiae of black letter intermediary liability law, but to identify the building blocks for harmonization: how the liability of online intermediaries is generally treated in each jurisdiction, significant legislative and jurisprudential developments, and areas of continued controversy.

A. United States

In the early years of the Internet, the application of traditional law to the online environment raised a slew of difficult issues for courts to consider. As already mentioned, one of the earliest questions, raised in *Cubby Inc.*, was whether courts should hold online intermediaries liable as "publishers" or "distributors" of defamatory content posted on their platforms by third parties.[63] In that case, the U.S. District Court for the Southern District of New York held that an online intermediary that exercised no editorial control over third-party content was a mere distributor, akin to "a public library, book store, or newsstand,"[64] and therefore liable for defamation only if "it knew or had reason to know of the allegedly defamatory . . . statements."[65] In *Stratton Oakmont, Inc. v. Prodigy Services Co.*, however, the New York Supreme Court (trial court level in New York) found that if an intermediary had "held itself out to the public and its members as controlling the content of its computer bulletin boards" and had exercised editorial control by screening content, it would be considered the "publisher" of the defamatory content and directly liable for the speech of its users.[66]

The adoption of section 230(c) of the Communications Decency Act[67] was prompted by the perverse incentives created for intermediaries by the *Stratton Oakmont* decision, as well as by rising concern

63. *See* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104 § 230(c) (1996).

64. *Cubby, Inc.*, 776 F. Supp. at 140.

65. *Id.* at 141.

66. *Stratton Oakmont, Inc.*, 1995 N.Y. Misc. LEXIS 229 at *10.

67. Communication Decency Act, 47 U.S.C. § 230(c) (1996). The CDA was passed as Title V of the Telecommunications Act of 1996 and amended 47 U.S.C. §§ 223 and 230. The amendments to § 223 were struck down as unconstitutional in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

over Internet pornography.[68] Under *Stratton Oakmont* and *Cubby Inc.*, an intermediary could be held to the lower "distributor" standard only if it did not screen its users' content.[69] If the intermediary chose to exercise editorial control — by removing offensive, obscene, or defamatory posts, for instance — it risked being subjected to the higher "publisher" standard.[70] Representatives Cox and Wyden, who put forward section 230 in an amendment in the House, believed *Stratton Oakmont* "punished legitimate efforts to provide a 'family-oriented' computer service."[71] They hoped the new provision would "promote the continued development of the Internet" and encourage self-regulation by users and intermediaries.[72]

Section 230(c)(1) CDA states 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."[73] Shortly after its adoption, section 230(c)(1) was interpreted by the Fourth Circuit in *Zeran v. AOL, Inc.* as affording nearly complete immunity to online intermediaries for their users' content.[74] Since then, the provision has continued to be read as a broad safe harbor for intermediaries,[75] with the exception of cases where the intermediary played a significant role in the creation or development of the allegedly harmful content.[76]

---

68. *See* H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.) *reprinted in* 1996 U.S.C.C.A.N. 10 ("One of the specific purposes of [§ 230] is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."); Medenica & Wahab, *supra* note 4, at 249.

69. Medenica & Wahab, *supra* note 4, at 248.

70. *Id.* at 249.

71. *Id.*

72. *See* CDA, § 230(b)(1)–(4); Zeran v. AOL, Inc., 129 F.3d 327, 331, 335 (4th Cir. 1997).

73. CDA, § 230(c)(1).

74. *Zeran*, 129 F.3d at 332. The court reached this conclusion despite the provision not mentioning distributor liability. It collapsed the distinction between distributors and publishers for purpose of defamation law and held that in passing § 230, "Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages." *Id.* at 331–32. *But see* CDA, § 230(e) (providing no liability exemptions for intermediaries under federal criminal law, intellectual property laws, or communications privacy laws).

75. *See* Rustad & Koenig, *supra* note 2, at 370–71; *see, e.g.*, Johnson v. Arden, 614 F.3d 785, 792 (8th Cir. 2010); Nemet Chevrolet, Ltd v. ConsumerAffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009); Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008); Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); *About Us: Want To Sue Ripoff Report?*, RIPOFF REPORT, http://www.ripoffreport.com/ConsumersSayThankYou/WantToSueRipoffReport.aspx#3 (last modified Jan. 19, 2011) ("Based on the protection extended by the CDA, Ripoff Report has successfully defended more than 20 lawsuits in both state and federal courts.").

76. *See, e.g.*, CDA, § 230(f)(3); Fed. Trade Comm'n v. Accusearch Inc., 570 F.3d 1187, 1196 (10th Cir. 2009); Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1166 (9th Cir. 2008) (The court held that by requiring users to answer questions it asked through dropdown menus, Roommates.com was affirmatively soliciting

Section 230(c)(2) CDA further clarifies that intermediaries cannot be held liable for self-policing, restricting access to, or providing others the technical means to restrict access to material considered to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected . . . ."[77]

The broad reading of section 230(c) CDA has contributed to the growth and vibrancy of speech on the Internet.[78] Moreover, most major intermediaries — from Facebook and CNN.com to Craigslist and Wikipedia — have taken up the mantle of self-regulation.[79]

Such a broad reading has, however, also had some more perverse effects. The broad understanding of intermediary immunity adopted in *Zeran* "paved the way," in some instances, for intermediaries, "relying upon § 230 as a panacea, to ignore and even facilitate a variety of defamatory and sometimes egregious behaviors."[80] Two examples include failure to remove content judged defamatory and failure to remove content held illegal under state criminal law.

---

discriminatory content and thus acting as an information content provider within the meaning of the CDA: "By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information." Section 230 does not apply: "[S]ection 230 provides immunity only if the interactive computer series does not 'creat[e] or develop[]' the information 'in whole or in part.'" (citation omitted)); Jones v. Dirty World Entm't Recordings, LLC, 965 F. Supp. 2d 818, 823 (E.D. Ky. 2013) (holding that the operator "played a significant role in 'developing' the offensive content such that he has no immunity under the CDA"); Alvi Armani Med., Inc. v. Hennessey, 629 F. Supp. 2d 1302, 1306–07 (S.D. Fla. 2008); Capital Corp. Merch. Banking, Inc. v. Corporate Colocation, Inc., No. 6:07-cv-1626-Orl-19KRS, 2008 U.S. Dist. LEXIS 68154, at *10 (M.D. Fla. Aug. 26, 2008) (holding that § 230 "provides immunity for the removal of content, not the creation of the content"); Woodhull v. Meinel, 202 P.3d 126, 133 (N.M. Ct. App. 2008) (denying § 230 immunity where defendant solicited potentially defamatory material). *But compare Jones*, 965 F. Supp. 2d 818, *with* S.C. v. Dirty World, LLC, No. 11-CV-00392, 2012 WL 3335284, at *3–4 (W.D. Mo. Mar. 12, 2011), *and* Hare v. Richie, No. ELH-11-3488, 2012 WL 3773116, at *17 (D. Md. Aug. 29, 2012), in which all three reach different results on the same operator's role in development. Note as well that in *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1107 (9th Cir. 2009), the Ninth Circuit found that a promissory estoppel claim is not barred by § 230 CDA and that plaintiff may have such a claim against Yahoo! for failing to remove defamatory content despite promising to do so.

77. *See* CDA, § 230(c)(2).

78. *See* Matt Zimmerman, *State AGs Ask Congress To Gut Critical CDA 230 Online Speech Protections*, ELEC. FRONTIER FOUND. (July 24, 2013), https://www.eff.org/deeplinks/2013/07/state-ags-threaten-gut-cda-230-speech-protections.

79. *See* Ardia, *supra* note 4, at 489–92; Kosseff, *supra* note 4, at 153–57; Kathleen M. Walsh & Sarah Oh, *Self-Regulation: How Wikipedia Leverages User-Generated Quality Control Under Section 230* (Feb. 23, 2010), http://ssrn.com/abstract=1579054; *see also Domestic Minor Sex Trafficking: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 111th Cong. 168 (2010) (statement of William "Clint" Powell, Director, Customer Service and Law Enforcement Relations, Craigslist, Inc.), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58250/html/CHRG-111hhrg58250.htm.

80. Medenica & Wahab, *supra* note 4, at 254.

In most instances, once user-generated content is judged defamatory or unlawful, intermediaries will remove such content voluntarily.[81] However, this is not always the case. In *Blockowicz v. Williams*, the operators of RipoffReport.com refused to delete postings about the Blockowicz family that the district court found defamatory.[82] The Seventh Circuit ruled that a court order enjoining the removal of defamatory content cannot be enforced against an online intermediary under the Federal Rules of Civil Procedure.[83] Surely Congress did not intend this result. Section 230 was not meant to grant defamatory content perpetual online existence, nor should it preclude the application of defamation law to cyberspace writ large.

Similarly, there has recently been significant controversy surrounding a request to Congress made by forty-seven states' Attorneys General to amend section 230 to carve out all state criminal statutes.[84] The Attorneys General claim that the amendment is necessary in order to grant authorities the power to fight online child sex trafficking.[85] The response from the tech community was swift, unwavering, and unequivocal: empowering states' Attorneys General to pursue online intermediaries for user conduct ranging from criminal libel to the publication of gun permit information or the sharing of Netflix passwords would fracture and threaten the Internet as we know it.[86] It would be impermissibly onerous to require intermediaries to simultaneously enforce the divergent criminal laws of fifty states. Through their crim-

---

81. Erica Johnstone, *Removing Offending Web Posts*, CAL. LAWYER (June 2011), http://callawyer.com/Clstory.cfm?eid=916163&wteid=916163_Removing_Offending_Web_Posts.

82. *See* Blockowicz v. Williams, 675 F. Supp. 2d 912, 913 (N.D. Ill. 2009).

83. *See* Blockowicz v. Williams, 630 F.3d 563, 569 (7th Cir. 2010); *see also* FED. R. CIV. P. 65(d)(2)(C).

84. Letter from Nat. Ass'n of Att'y Gen., to S. Comm. on Com. Sci. & Transp. and the H. Comm. on Energy & Com. (July 23, 2013), https://www.eff.org/sites/default/files/cda-ag-letter.pdf.

85. The request also formed part of a long-running crusade against Craigslist's now defunct "erotic services" section and Backpage.com's "adult services" section, notwithstanding both websites' extraordinary willingness to cooperate and assist law enforcement in apprehending users involved in human trafficking or prostitution rings. *See, e.g.*, M.A. v. Village Voice Media Holdings, LLC, 809 F. Supp. 2d 1041, 1043 (E.D. Mo. 2011); Dart v. Craigslist, 665 F. Supp. 2d 961, 961 (N.D. Ill. 2009); Zimmerman, *supra* note 78; *see also* JJ Hensley, *Adult Services Ads Are Targeted*, THE ARIZ. REPUBLIC (May 19, 2012), http://www.azcentral.com/arizonarepublic/local/articles/2012/05/16/20120516backpage-adult-ads-targeted.html.

86. *See* Zimmerman, *supra* note 78; Eric Goldman, *Why the State Attorneys General's Assault on Internet Immunity Is a Terrible Idea*, FORBES (June 27, 2013), http://www.forbes.com/sites/ericgoldman/2013/06/27/why-the-state-attorneys-generals-assault-on-internet-immunity-is-a-terrible-idea/; Grant Gross, *Groups Oppose Proposed Change to Internet Content 'Safe Harbor,'* PCWORLD (July 31, 2013), http://www.pcworld.com/article/2045653/groups-oppose-proposed-change-to-internet-content-safe-harbor.html; Lee Rowland & Gabe Rottman, *New Proposal Could Singlehandedly Cripple Free Speech Online*, ACLU (Aug. 1, 2013), https://www.aclu.org/blog/free-speech-national-security-technology-and-liberty/new-proposal-could-singlehandedly-cripple.

inal laws, states would have the power to control immense quantities of extra-jurisdictional online speech, and the specter of criminal liability would have a chilling effect on entrepreneurship and innovation.[87]

And yet, while the proposal of the Attorneys General certainly goes too far, it raises an interesting question: Should state law enforcement have some ability to demand the suppression of content that is illegal throughout the fifty states?[88] This Note cautiously answers in the affirmative.

B. Canada

The state of the law with respect to intermediary liability for user-generated content is significantly less developed in common law Canada[89] than in the United States.[90] Importantly, there is no statutory provision comparable to section 230 CDA.[91] There is also a dearth of case law dealing directly with online intermediary liability. Much of the applicable law was, therefore, developed in the non-digital context.

Intermediaries benefit from the defenses generally available to allegations of defamation including "'innocent dissemination,'" which protects "'those who play a secondary role in the distribution system, such as news agents, booksellers, and libraries' . . . ."[92] To escape liability, an intermediary would have to show that it "ha[d] no actual

87. Goldman, *supra* note 86.

88. I say this without endorsing the wisdom of the request of the Attorneys' General to shut down Backpage.com's "adult services" section. When Craigslist gave in to the demands of the Attorneys General and shut down its "erotic services" section, the ads simply migrated to other websites, including Backpage.com. There is no reason to think the same would not occur if Backpage.com shut down its adult section. Arguably, keeping the ads on a cooperative U.S.-operated website benefits law enforcement efforts. *See* Hensley, *supra* note 85.

89. This Note does not address the legal situation in the civil law province of Quebec. For an excellent summary of Internet defamation law throughout Canada, see Antonin I. Pribetic, *Internet Defamation: A Canadian Perspective*, ONT.-N.Y. LEGAL SUMMIT (Mar. 28, 2014), http://ssrn.com/abstract=2425120.

90. *See generally* Mark A.B. Donald, *Liability for Third-Party Cyberlibel: A Basic Legal Primer for Editors, Moderators and Bloggers in the Online Sphere*, ONT. B. ASS'N 5 (Jan. 2014), http://www.oba.org/Sections/Entertainment-Media-and-Communications-Law/Articles?keywords=liability&author=mark+a.b.+donald.

91. *Id.* at 4.

92. Crookes v. Newton, 2011 SCC 47, [2011] 3 S.C.R. 269, para. 20 (Can.) (quoting ALLEN M. LINDEN & BRUCE FELDTHUSEN, CANADIAN TORT LAW 783–84 (8th ed. 2006)); *see also* Hemming v. Newton, 2006 BCSC 1748, para. 13 ("The defence of innocent dissemination . . . applie[s] 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 . . . ."); Robert W. Grant, et al., *Canadian Law and Procedure*, *in* ENTERTAINMENT LITIGATION 875, 919 (Charles J. Harder ed., 2011) (noting that ISPs and webpage owners "who merely provide a passive vehicle for the posting of content by others" are not liable by "extension of the innocent dissemination rule, . . . historically . . . applied to [those] who passively disseminate publications without reviewing or monitoring their content.").

knowledge of an alleged libel, [was] aware of no circumstances to put [it] on notice to suspect a libel, and committed no negligence in failing to find out about the libel . . . ."[93] This defense is roughly analogous to the common law defense open to "distributors" under U.S. law.[94] Most recently, in *Demenuk v. Dhadwal*, the British Columbia Supreme Court (trial court level in British Columbia) explained that "'some element of fault is required' before liability will attach to an intermediary . . . ."[95] Such fault may include a failure "to exercise reasonable care to ensure that third-party defamatory comments are promptly taken down from areas that the intermediary directly controls."[96] Therefore, under Canadian law an intermediary can become liable for user content if it receives notice of the allegedly defamatory content, has control over it, and fails to remove it in a timely manner.[97]

Despite the low standard for liability, there are statutory restrictions in nearly all Canadian common law provinces on how and when notice must be provided to a defendant where an action is instituted for libel in a newspaper or in a radio or television broadcast.[98] In Ontario, notice must be in writing (for which email will suffice)[99] and delivered within six weeks of the alleged defamation coming to the plaintiff's attention.[100] The notice requirement is clearly applicable to online newspapers, but it is unclear whether it would apply to other websites.[101] When it is required, failure to provide proper notice acts as a complete bar to legal action.[102]

Some scholars have suggested that intermediaries may claim that their conduct does not constitute "publication" and therefore cannot trigger liability under Canadian law, irrespective of their

93. Soc. of Composers, Authors & Music Publishers of Can. v. Canadian Ass'n. of Internet Providers, 2004 SCC 45, [2004] 2 S.C.R. 427, para. 89.

94. *See* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); *see also supra* notes 64–65.

95. Donald, *supra* note 90, at 5 (citing Demenuk v. Dhadwal, 2013 BCSC 2111, 2013 CarswellBC 3544 at paras. 107–11 (Can.)).

96. *Id.*

97. *See id.* at 9.

98. *See generally Cyber Libel and Canadian Courts: Notice of Intended Action*, MCCONCHIE LAW, http://www.libelandprivacy.com/cyberlibel_home.html#b (*cases published to* Aug. 11, 2014).

99. In a recent case, the British Columbia Supreme Court authorized the plaintiff to serve his statement of claim on the John Doe defendants via private notification on their message board accounts. Burke v. John Doe, 2013 BCSC 964, [2013] B.C.W.L.D. 6248, para. 22 (Can.).

100. Libel and Slander Act (Ontario), R.S.O. 1990, c. L-12, § 5(1) (Can.).

101. *See* Weiss v. Sawyer, 2002 CarswellOnt 3003, [2002] O.J. No. 3570, para. 24; MCCONCHIE LAW, *supra* note 98.

102. *See* Grossman v. CFTO-TV Ltd., 1982 CarswellOnt 1361, [1982] O.J. No. 3538, para. 29.

knowledge.[103] The best indication of the state of the law on this question is the Supreme Court of Canada's recent decision in *Crookes v. Newton* holding that mere hyperlinking does not constitute publication. Justice Abella, writing for a majority of the Court, found that:

> Making reference to the existence and/or location of content by hyperlink or otherwise, without more, is not publication of that content. Only when a hyperlinker presents content from the hyperlinked material in a way that actually repeats the defamatory content, should that content be considered to be "published" by the hyperlinker. Such an approach promotes expression and respects the realities of the Internet, while creating little or no limitations to a plaintiff's ability to vindicate his or her reputation. While a mere reference to another source should not fall under the wide breadth of the traditional publication rule, the rule itself . . . may deserve further scrutiny in the future.[104]

One commentator argues that this decision is generally relevant to intermediary liability law:

> While a hyperlinker is not an intermediary, she shares essential characteristics with most intermediaries, in that both play primarily facilitative roles. The intermediary provides access to content created by others, while the hyperlinker merely draws reader's attention to that content. Crookes squarely raises the question of the extent to which we should be making individuals liable for what others have done.[105]

In this light, *Crookes* suggests that some measure of immunity exists (or may in the future exist) under Canadian law for passive online intermediaries, irrespective of whether they have knowledge of the illegal or defamatory nature of the content they host.

---

103. *See* Crookes v. Newton, 2011 SCC 47, [2011] 3 S.C.R. 269, para. 21 ("[I]n order to hold someone liable as a publisher, '[i]t is not enough that a person merely plays a passive instrumental role in the process'; there must be 'knowing involvement in the process of publication of *the relevant words*'" (citing Bunt v. Tilley, [2006] EWHC 407, [2006] 3 All E.R. 336, para. 23 (Q.B.)).

104. Crookes, 2011 SCC 47, para. 42.

105. Tamir Israel, *Crookes v. Newton: Speculations on Intermediary Liability . . . .*, SLAW (Nov. 2, 2011), http://www.slaw.ca/2011/11/02/crookes-v-newton-speculations-on-intermediary-liability/.

It is highly unlikely, in the absence of intent or knowledge, that Canadian courts would find an intermediary criminally liable for the hate speech of its users[106] or for failing to identify child pornography hosted on its servers.[107] An online intermediary could, however, probably be found civilly liable for the hateful or discriminatory speech of its users under provincial human rights statutes.[108] Though there are no cases directly on point, the language in the provincial statutes tends to be very broad and can reasonably be read to capture online intermediaries.[109]

Overall, when proper notice is given, Canadian courts are significantly more plaintiff-friendly than their American counterparts in civil lawsuits against online intermediaries.

C. United Kingdom

Before the 2013 Defamation Act was passed, the United Kingdom's intermediary liability laws were very similar to those of Canada. Unless an intermediary "knew or ought by the exercise of reasonable care to have known that the publication was likely to be defamatory"[110] or exercised editorial control over the publication,[111]

106. This improbability is due to the *mens rea* requirements of both the offence of "public incitement of hatred" and of aiding and abetting. *See* Criminal Code, R.S.C. 1985, c. C-46, §§ 21(2), 319(1); R. v. Briscoe, 2010 SCC 13, [2010] 1 S.C.R. 411, para. 15; R. v. Greyeyes, [1997] 2 S.C.R. 825, para. 37.

107. Under Canadian law, there is no affirmative duty or permission to seek out child pornography. *See* An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4, § 6. However, once the intermediary has reasonable grounds to believe that child pornography is being transmitted through its system, either through notices from users or from its own knowledge, it has an obligation to notify the police. *Id.* at § 3. It is also obliged to preserve the evidence for a 21-day period. *Id.* at § 4. A judge may issue a warrant authorizing seizure of the content. Criminal Code, R.S.C. 1985, c. C-46, § 164.1(1). There would also be no criminal liability for possession of child pornography because under Canadian criminal law "possession" requires a subjective knowledge of the nature of the object possessed. *See* Criminal Code, R.S.C. 1985, c. C-46, § 163.1(4); Beaver v. R., [1957] S.C.R. 531, para. 3.

108. *See, e.g.*, Human Rights Act, R.S.P.E.I. 1988, c. H-12, § 12(1) (P.E.I.); Saskatchewan Human Rights Code, R.S.S. 1979, c. S-24.1, § 14, *as limited by* Saskatchewan (Human Rights Comm'n) v. Whatcott, 2013 SCC 11, [2013] 1 S.C.R. 467; Alberta Human Rights Act, R.S.A. 2000, c. A-25.5, § 3; Human Rights Act, R.S.N.W.T. 2002, c. 18, § 13 (N.W.T.). Note that the hate speech provision of the Federal Canadian Human Rights Act, R.S.C. 1985, c. H-6, § 13 was repealed in 2013 by An Act to amend the Canadian Human Rights Act (protecting freedom), S.C. 2013, c. 37, despite the provision being found to be a constitutionally acceptable limitation on freedom of expression by the Supreme Court of Canada. Canadian Human Rights Comm'n v. Taylor and Western Guard Party, [1990] 3 S.C.R. 892.

109. *See, e.g.*, Saskatchewan Human Rights Code, § 14 (Making it an offense for any person to "publish or display, or cause or *permit to be* published or displayed . . . in a newspaper, through a television or radio broadcasting station or *any other broadcasting device*, or in any printed matter or publication *or by means of any other medium that the person owns, controls, distributes or sells*, any" prohibited speech. (emphasis added)).

110. Tamiz v. Google Inc, [2013] EWCA (Civ) 68, [26], [2013] 1 W.L.R. 2162 (Eng.).

the intermediary was not treated as a publisher or distributor of the content and was not liable for its defamatory nature.[112] Similarly, under the Electronic Commerce (EC Directive) Regulations of 2002, which implemented the European Union's 2000 E-Commerce Directive,[113] a hosting intermediary would not be liable for unlawful content if it did "not have actual knowledge of unlawful activity or information[,] . . . [was] not aware of facts or circumstances from which it would have been apparent . . . that the activity or information was unlawful[,] or upon obtaining such knowledge or awareness, acted expeditiously to remove or disable access to the information."[114] The 2002 Regulations and the E-Commerce Directive apply to most illegal content hosted by an intermediary, including hate speech, child pornography, and defamatory content.[115]

While keeping the above defenses and limitations on liability intact, the 2013 Defamation Act clarified and made several significant changes to the law on intermediary liability for defamatory content in the U.K.[116]

---

111. *See* Kaschke v. Gray, [2010] EWHC (QB) 690, [25], [2011] 1 W.L.R. 461 (Eng.) (citing § 1 of the 1996 Defamation Act in explaining editorial control).

112. Defamation Act, 1996, c. 31, § 1 (U.K.); Paul Dacam, *UK: Defamation (Operators of Websites) Regulations 2013*, LEXOLOGY (Nov. 5, 2013), http://www.lexology.com/library/detail.aspx?g=e194fb66-8c23-4908-866d-5923038f37fa. Note that in Godfrey v. Demon Internet Ltd, [2001] Q.B. 201 at 205–06 (Eng.), the court held that the intermediary had lost § 1 immunity because it had kept defamatory posts up for two weeks after notification.

113. Council Directive 2000/31/EC, Directive on Electronic Commerce, art. 14, 2000 O.J. (L 178) 1, 13.

114. Electronic Commerce (EC Directive) Regulations, 2002, S.I. 2002/2013, art. 19, ¶¶ 19(a)(i)–(ii) (U.K.). One factor to consider in determining whether an intermediary had actual knowledge is whether they have received notice. *Id*. art. 22, ¶ 22(a). But the test remains whether the intermediary was actually "aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality . . . ." Case C-324/09, L'Oréal SA vs. eBay International AG, ¶¶ 120, 122 (July 12, 2011), http://curia.europa.eu/juris/liste.jsf?num=C-324/09. *But see* Daithí Mac Síthigh, *Notice and No-Takedown*, LEX FERENDA (Mar. 6, 2012), http://www.lexferenda.com/06032012/notice-and-no-takedown/ (suggesting that the earlier High Court decision in Tamiz v. Google Inc, ([2012] EWHC (QB) 449 (Eng.)) confirms that under the E-Commerce Directive, a notice alleging defamation does not suffice to strip the statutory protection). The Court of Appeal found it unnecessary to decide this use. Tamiz, [2013] EWCA (Civ) 68, [52].

115. *See First Report on the Application of Directive 2000/31/EC*, at 12, COM (2003) 702 final (Nov. 21, 2003), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF ("The limitations on liability provided for by the Directive are established in a horizontal manner, meaning that they cover liability, both civil and criminal, for all types of illegal activities initiated by third parties."). Note that under U.K. law, an intermediary will not be liable for hosting child pornography absent knowledge of its content. *See* Criminal Justice Act, 1988, c. 33, § 160(2) (U.K.) ("[I]t shall be a defence [to a charge of possession of child pornography] for [a person] to prove . . . that he had not himself seen the photograph . . . and did not know, nor had any cause to suspect, it to be indecent . . . .").

116. *See generally* Síthigh, *supra* note 30, at 527–28; Dacam, *supra* note 112; Martin, *supra* note 48.

First, a court lacks jurisdiction to hear an action against a non-publisher intermediary where it is reasonably practicable to bring an action against the author, editor, or publisher of the defamatory post.[117] Even if the intermediary does meet the test for publication,[118] if the claimant has sufficient information to identify and bring proceedings against the person who posted the defamatory content,[119] "[i]t is a defence for the [intermediary] to show that it [did not] post[] the statement on the website"[120] as long as it had not acted "with malice in relation to the posting of the statement concerned."[121]

Second, if the claimant cannot identify the person who posted the defamatory content (i.e., the post was anonymous or pseudonymous), the claimant must send a detailed notice of complaint to the intermediary.[122] To benefit from immunity, the intermediary must within forty-eight hours attempt to forward a copy of the notice of complaint to the poster.[123] The poster then has five days to respond and either (1) consent to the allegedly defamatory material being removed from the website or (2) provide his or her full name and postal address.[124] If the intermediary cannot contact the poster, if the poster fails to respond within five days of contact, or if the poster consents to the material being removed, the intermediary must remove the material within forty-eight hours of the five-day deadline.[125] If the poster duly responds and refuses to consent to the removal of the material, the intermediary must inform the claimant, again within forty-eight hours.[126] It is up to the poster whether the intermediary can disclose the poster's contact information to the complainant in the absence of a court order.[127] In the case of repeat removals involving the same poster, content, and website, the above procedure no longer applies.[128]

---

117. *See* Defamation Act, 2013, c. 26, § 10 (U.K.); Defamation Act, 1996, c. 31 § 1 (U.K.).

118. For instance, because the intermediary moderates posts made on its website. *See* Defamation Act, 2013, § 5(12) ("The defence under this section is not defeated by reason only of the fact that the operator of the website moderates the statements posted on it by others.").

119. *See id.* § 5(3)(a), 5(4).

120. *Id.* § 5(2).

121. *Id.* § 5(11).

122. *See id.* § 5(3)(b). The notice of complaint must include, *inter alia*, the aspects of the statement the complainant believes are factually inaccurate or opinions not supported by facts, the meaning which the complainant attributes to the statement, and a confirmation that the complainant does not have sufficient information about the poster to bring legal proceedings directly against that person. The Defamation (Operators of Websites) Regulations, 2013, S.I. 2013/3028, art. 2, ¶¶ 2(b)–(d).

123. *See* The Defamation (Operators of Websites) Regulations, 2013, S.I. 2013/3028, Schedule.

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

Instead, the intermediary must remove the content within forty-eight hours of receiving the notice of complaint.[129]

Finally, where a court gives judgment for the claimant in an action for defamation, the court may order an intermediary to remove the defamatory statement from its website.[130] The court can also order any person who was not the author, editor, or publisher of the defamatory statement to stop distributing, selling, or exhibiting material containing the statement.[131]

If involved parties follow the above procedure, then the intermediary benefits from immunity.[132] The intermediary's "involvement in the action will cease, subject to a possible court order being sought by the claimant to obtain the poster's details, if consent to provide them was refused."[133] The intermediary is therefore shielded from legal liability, while the victim of the allegedly defamatory speech obtains removal of the content, learns the identity of the poster, or at the very least is guaranteed that a successful petition to the court to unmask the poster's identity will prove fruitful.

D. European Union

The European Union E-Commerce Directive governs intermediary liability in all EU member states in the same manner as in the United Kingdom. As mentioned above, it protects intermediaries whose role is "merely technical, automatic and passive" from liability, but does not shield intermediaries that play "an active role of such a kind as to give [them] knowledge of, or control over, the data stored."[134] The Directive has multiple enforcing bodies: Both courts and administrative authorities can order non-monetary relief by instructing an intermediary "to prevent or stop infringement of any rights."[135] Thus, regulators in countries like France and Germany can and do order intermediaries to remove or block access to illegal content such as child pornography or Nazi memorabilia.[136] Moreover,

---

129. *Id.*

130. Defamation Act, 2013, § 13.

131. *Id.*

132. Dacam, *supra* note 112.

133. *Id.*

134. Delfi AS v. Estonia, Eur. Ct. H.R. App. No. 64569/09, ¶ 43 (2013), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635; Case C-236/08, Google France SARL v. Louis Vuitton Malletier SA, ¶¶ 113–14, 121 (Mar. 23, 2010), http://curia.europa.eu/juris/liste.jsf?num=C-236/08.

135. Electronic Commerce (EC Directive) Regulations, 2002, S.I. 2002/2013, art. 20, ¶¶ 20(1)(b)–(2) (U.K.).

136. *See* LICRA & UEJF v. Yahoo!, Inc. & Yahoo France, Tribunal de grande instance [TGI][ordinary court of original jurisdiction] Paris, Nov. 20, 2000, N. 00/05308; Katalin Parti & Luisa Marin, *Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content*, 9 J. CONTEMP. EUR. RES. 138, 148–49 (2013).

since the Directive has been enacted by national legislation — such as the U.K.'s 2002 Regulations — in each EU member state, there is some divergence in treatment among states and less harmonization than expected.[137]

Discussions regarding intermediary liability for user-generated content in Europe have recently centered on the European Court of Human Rights' 2013 opinion in *Delfi AS v. Estonia*.[138] In that case, the Court held that the Estonian courts did not violate Delfi's freedom of expression right (guaranteed by article 10 of the European Convention on Human Rights)[139] when they imposed liability on the major news portal for defamatory comments posted under one of its news stories by anonymous users.[140] The Estonian Supreme Court had previously held that Delfi was not a host within the meaning of the Information Society Services Act (the Estonian legislation enacting the E-Commerce Directive) and ordered Delfi to pay damages to the defamed party.[141] The European Court of Human Rights ruled that Estonia had not violated article 10 of the Convention because Estonia's

137. *Compare* Vjatšeslav Leedo v. Delfi (2009; 3-2-1-43-09) (Est. Sup. Ct.), https://www.riigiteataja.ee/akt/13192224.pdf, *cited in* Delfi AS v. Estonia, Eur. Ct. H.R. App. No. 64569/09, ¶ 65 (2013), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635 (holding that a news portal did not qualify for immunity because it did not permit commenters to change or delete their comments after posting, "play[ed] . . . an active role" by deleting and modifying comments, and had previously monitored comments and taken measures to minimize insulting comments), *with* Tamiz v. Google Inc, [2013] EWCA (Civ) 68, [50], [2013] 1 W.L.R. 2170 (Eng.) (holding that Google would not have been liable prior to receiving notice of the defamatory content). *See also* Kaschke v. Gray, [2010] EWHC (QB) 690, [89–90], [2011] 1 W.L.R. 480 (Eng.) (stating that the relevant target for the analysis is whether the post alleged to be defamatory was edited, monitored, or went beyond mere storage); Gavin Sutter, *Rethinking Online Intermediary Liability: In Search of the 'Baby Bear' Approach*, 7 INDIAN J.L. & TECH. 33, 78–80 (2011) (discussing diverging national results in Germany, England, and France with respect to eBay trademark cases under articles 14 and 15 of the E-Commerce Directive dealing with immunity for hosts and there being no general obligation to monitor the information stored). The U.K. case has since been referred to and decided by the European Court of Justice. Case C-324/09, L'Oréal SA vs. eBay International AG (July 12, 2011), http://curia.europa.eu/juris/liste.jsf?num=C-324/09.).

138. Eur. Ct. H.R. App. No. 64569/09 (2013), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635.

139. The Convention for the Protection of Human Rights and Fundamental Freedoms. art. 10, Nov. 4, 1950, http://www.echr.coe.int/Documents/Convention_ENG.pdf.

140. The facts of the case can be briefly summarized. In January 2006, Delfi published an article about how a popular ferry company's decision to change its routes resulted in a delay in the opening of alternative and cheaper means of transportation to certain islands. Below the news story, users could post anonymous comments to the website and access the comments of others. A series of highly offensive and threatening comments were posted about the ferry company and its owner. In April 2006, the owner sued Delfi for defamation. In June 2008, the first instance court found Delfi responsible for the defamatory comments and awarded the ferry company owner 5000 kroons (roughly $426 USD) in damages. Estonia's Supreme Court affirmed the decision in June 2009. *See* Delfi AS v. Estonia, Eur. Ct. H.R. App. No. 64569/09, ¶ 65 (2013), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635.

141. Vjatšeslav Leedo v. Delfi (2009; 3-2-1-43-09) (Est. Sup. Ct.), https://www.riigiteataja.ee/akt/13192224.pdf.

courts restricted Delfi's freedom of expression in order to protect another person's reputation.[142] The restriction was also only to a degree proportionate to the circumstances.[143] In particular, the Court noted that Delfi (1) should have expected the offensive posts in light of the nature of the article and should have been prepared,[144] (2) failed to take any proactive steps — beyond an automated word-filtering system and a user take-down notification system — to remove defamatory and offensive comments,[145] (3) permitted users to post anonymously, thereby making it very difficult to hold them personally liable,[146] and (4) benefited commercially from the comments being made due to increased web traffic.[147] Delfi's explicit notice to users that they would be liable for their content and the site's prohibition on threatening or insulting comments were held to be insufficient to avoid liability.

Although the European Court of Human Rights did not decide whether the Estonian courts had properly interpreted and applied the Information Society Services Act or article 14 of the E-Commerce Directive in denying Delfi host immunity,[148] and despite the fact that each European country has its own E-Commerce Directive enacting legislation for national courts to interpret,[149] the judgment raises some serious questions about intermediary liability in Europe. The decision has been heavily criticized, with detractors arguing that the Court "fail[ed] to grasp the EU framework governing intermediary liability . . . ."[150] Indeed, the ruling bears some of the hallmarks of the oft-criticized and now superseded U.S. *Stratton Oakmont* decision and highlights the continuing barriers to true harmonization of European intermediary liability law.[151] Many commentators consider the ruling's suggestions — (1) takedown upon notice is insufficient to avoid liability,[152] (2) there may be some affirmative duty to monitor user-generated content,[153] and (3) permitting anonymous posting should

142. Delfi AS, Eur. Ct. H.R. App. No. 64569/09, ¶ 94.

143. *Id.*

144. *Id.* ¶ 86.

145. *Id.* ¶¶ 87–88. Though Delfi removed the offensive comments the *same day* it received a takedown notice from the complainant. *Id.* ¶ 15.

146. *Id.* ¶¶ 91–92.

147. *Id.* ¶¶ 86, 89, 94.

148. *Id.* ¶ 74. (noting that "[i]t is primarily for the national authorities, notably the courts, to resolve problems of interpretation of domestic legislation").

149. *See supra* note 137.

150. *See, e.g.*, Gabrielle Guillemin, *Case Law, Strasbourg: Delfi AS v Estonia: Court Strikes Serious Blow to Free Speech Online*, INFORRM'S BLOG (Oct. 15, 2013), http://inforrm.wordpress.com/2013/10/15/case-law-strasbourg-delfi-as-v-estonia-court-strikes-serious-blow-to-free-speech-online-gabrielle-guillemin/.

151. *See supra* note 137 and accompanying text.

152. *See supra* note 150.

153. *Id.*

count against an intermediary's immunity[154] — deeply troubling from an online freedom of expression perspective.[155] On February 17, 2014, the Grand Chamber of the European Court of Human Rights accepted the referral of the *Delfi* case — a rather rare occurrence — and a hearing took place on July 9, 2014.[156] A decision has yet to be rendered.

IV. RETHINKING THE U.S. APPROACH TO INTERMEDIARY LIABILITY

The following proposal seeks to leverage the legal developments in host intermediary liability in Canada, the European Union, and the United Kingdom in order to improve the United States' approach to the issue. The proposal remains committed to the unique policy decisions underlying the U.S. system, tackles challenges currently confronting the U.S. approach, and accounts for the broader cyber-trends that favor international harmonization and reduced reliance on intermediary knowledge, assessment, and monitoring.

Greater harmonization of substantive intermediary liability laws across jurisdictions will have many benefits. It will lead to greater predictability and lower costs for intermediaries,[157] minimize the incentives for forum shopping,[158] and ensure that intermediaries implement in practice the policy balances struck by legislation, rather than simply complying with the laws of the most restrictive jurisdiction to which they are subject.[159] As noted in the World Intellectual Property Organization report comparing various jurisdictions' approaches to

---

154. *Id.*

155. *See, e.g.*, David Banks, *Online Comments: Why Websites Should Be Worried by Court Ruling*, GUARDIAN (Oct. 11, 2013), http://www.theguardian.com/media/media-blog/2013/oct/11/online-comments-websites-court-ruling-estonian; Liat Clark, *European Ruling on Anonymous Comment Liability Shouldn't Be Universally Damaging*, WIRED (Oct. 14, 2013), http://www.wired.co.uk/news/archive/2013-10/14/european-courts-privacy-ruling; Tim Worstall, *Every Website that Accepts Comments Now Has a European Problem*, FORBES (Oct. 11, 2013), http://www.forbes.com/sites/timworstall/2013/10/11/every-website-that-accepts-comments-now-has-a-european-problem/.

156. Registrar of the Court, *Grand Chamber Panel's Decisions*, EUR. CT. H.R. (Feb. 18, 2014), http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-4674833-5667824; Registrar of the Court, *Grand Chamber Hearing on Internet Portal's Liability for Offensive Comments Posted by Its Readers*, EUR. CT. H.R. (July 9, 2014), http://hudoc.echr.coe.int/webservices/content/pdf/003-4816452-5873028.

157. *See* Kaminski, *supra* note 4, at 211 ("The potential benefits of standardization [of intermediary liability rules] are many: lower transaction costs, in the form of compliance checks, and greater willingness to expand into markets that share the standardized rules, among others.").

158. *See, e.g.*, *Ehrenfeld*, 881 N.E.2d at 834; *Éditions Écosociété Inc.*, [2012] 1 S.C.R. 636, at para. 36 (Can.); Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law for Europe and America*, 5 J. HIGH TECH. L. 13, 34–38 (2005) (providing various examples of individuals taking advantage of differences in national defamation laws to forum shop in Internet defamation cases).

159. *See* Zittrain, *supra* note 54; Schultz, *supra* note 55.

intermediary liability for infringements of intellectual property rights, "[d]ifferences in national approaches to the complex issue of indirect intermediary liability and the safe harbor immunities just do not make much sense in an interconnected and transnational digital environment."[160] This Note advocates for the United States to move towards a semi-harmonized approach to intermediary liability. The proffered approach leaves a measure of flexibility for sovereign policy choices and national experimentation with respect to the most contentious issues, such as the protection of anonymous speech. However, it also tightly aligns with other jurisdictions' substantive laws where possible.

The U.S. approach to intermediary regulation encapsulated in section 230 CDA was intended to promote self-regulation and ensure the continued development of a vibrant Internet.[161] The United States chose not to adopt a "least cost avoider" approach to regulation that could have incentivized intermediaries to over-police content for fear of litigation.[162] This policy decision means that mere intermediary knowledge or monitoring should be irrelevant to the imposition of liability.[163] More importantly, however, the broader policy decision to favor online free speech means that intermediaries should not need to assess or judge the legality of content they host. The core arguments against intermediary liability today do not turn on a belief that all content should be permitted online, but merely that governments cannot encumber intermediaries with the task of judging which content is permissible and which is not.[164] Thus, the virtue of the U.S. approach is that it absolves intermediaries from an adjudicative role and ensuing costs.

This Note, however, contends that adherence to the values underlying the U.S. approach need not make intermediaries impervious to regulation with respect to illegal online content. Well-crafted legislation could maintain the benefits of protecting intermediaries from adjudicative functions while still providing a mechanism to encourage the removal of illegal online content. The proposal below has three parts based upon type of content: (1) content already determined to be illegal, (2) content not yet judged illegal where the poster is known, and (3) content not yet judged illegal where the poster is unknown.

---

160. Seng, *supra* note 7, at 6.

161. Mann & Belzley, *supra* note 4, at 246 ("Controlling [detrimental behavior] without restraining the Internet's potential is surely a worthy goal.").

162. *See supra* Section III.A. *See generally* Mann & Belzley, *supra* note 4, at 249 (discussing the theory that intermediaries might be the least cost avoiders of some Internet-related misconduct).

163. *See supra* Section II.B.

164. *See, e.g.*, *Infographic: Why CDA 230 Is So Important*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230/infographic (last visited Dec. 18, 2014). This argument against encumbering intermediaries, however, has developed over time and has not always existed. *See* Barlow, *supra* note 15.

A. Content Declared To Be Illegal

An important element absent from the present section 230 CDA, but accounted for by the United Kingdom and the European Union, is due consideration of the decisions of institutions with comparably greater competence to determine the legality of user content.[165] Regardless of whether the poster is known or unknown, when content is declared illegal by a competent authority, the balance tips heavily in favor of removal, subject to considerations of administrability and harmonization. Illegal speech should not benefit from the law's protection.[166]

Court orders for removal of content pronounced defamatory should be made enforceable against intermediaries such that intermediaries who refuse to remove the content would become liable as its publishers. Decisions like *Blockowicz* — in which an order requiring the removal of defamatory content could not be enforced against the intermediary, RipoffReport.com[167] — are unsupported by any policy rationale underlying section 230 CDA. Requiring removal of content deemed defamatory by a competent court would not impose any excessive burden on intermediaries or stunt the development of the Internet, particularly given both the paucity of cases in which intermediaries refuse to voluntarily remove defamatory content[168] and the significant time and effort required of plaintiffs to obtain a judgment in defamation.[169] Permitting immunity to intermediaries hosting defamatory content should not equate to perpetuity for the content.

With respect to content illegal under states' criminal laws, a balance must be struck. The proposal advocated by the Attorneys General is unworkable in that intermediaries would have to monitor user content *ab initio* to determine whether the content accords with the laws of every state. Beyond being effectively impossible to implement, the proposal would undermine the goal of harmonizing intermediary liability law by fracturing the United States into fifty

---

165. *See* Defamation Act, 2013, c. 26, § 13; Electronic Commerce (EC Directive) Regulations, 2002, S.I. 2002/2013, art. 20, ¶¶ 20(1)(b)–(2); E-Commerce Directive, *supra* note 53, § 14(3).

166. Three examples of this principle acting upon U.S. case law are rulings regarding child pornography, hate speech that poses an imminent danger of unlawful action, and libelous speech. *See* New York v. Ferber, 458 U.S. 747, 761–62 (1982) (child pornography); Gertz v. Robert Welch, Inc., 418 U.S. 323, 345–47 (1974) (private figure defamation); Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (hate speech posing an imminent danger of unlawful action); New York Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) (public figure defamation).

167. Blockowicz v. Williams, 630 F.3d 563, 568–70 (7th Cir. 2010).

168. *See supra* notes 79 and 81 and accompanying text.

169. David S. Ardia, *Freedom of Speech, Defamation, and Injunctions*, 55 WM. & MARY L. REV. 9, 16 (2013).

jurisdictions, each with its own unique demands on intermediaries.[170] This proposal would only further reinforce the "slowest ship in the convoy" problem by forcing intermediaries to comply with the most restrictive state's laws. Accordingly, the proposal of the Attorneys General could trigger a race to the bottom in terms of fostering free online speech.

Nevertheless, the argument against complying with states' laws should not be overstated. One need only glance across the Atlantic to be reassured that requiring intermediaries to remove or block *specific* illegal content will not topple the entire Internet, as long as intermediaries are regulated with caution. For instance, as already underscored, it is important that intermediaries not be required to monitor user content or reach their own judgments regarding its legality. Thus, any obligation imposed upon them should be limited to removal of illegal content upon due notification by an institution with comparably greater competence in judging the legality of content and distinguishing between protected and unprotected speech.[171] Such an institution could be a court, issuing an order on application by an administrative or law enforcement agency.[172] An administrative or law enforcement agency could also more directly play this role where the content is patently and indisputably illegal.[173] Both courts and, to a lesser extent, government agencies, are in better positions than intermediaries to make judgments about the legality of particular content in accordance with the interests of society and the law.[174] The vast majority of intermediaries already self-regulate and voluntarily comply with re-

---

170. Zimmerman, *supra* note 78 (noting that the proposal would "make service providers — from Facebook to a solo blogger — responsible for enforcing every relevant state and local criminal law in the country against their users, fracturing that national policy into one that effectively cedes a significant degree of control over Internet regulation to state and local law enforcement officials").

171. Of course, a failure to duly remove the illegal content within a prescribed period of time can then itself entail other penalties, including financial ones. *See* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 575 (2001) ("As a normative matter, comparative institutional analysis chooses the best institution by determining the outcome that best furthers a particular social policy goal . . . . That goal could be economic efficiency, but the analyst could choose from a wide range of goals, including, for example, the equitable distribution of resources.").

172. An *ex parte*, expedited procedure would be desirable, similar to the process for obtaining a warrant but imposing a higher burden on the agency to demonstrate the illegality of the content.

173. This suggestion is a slight derogation from the Finnish approach, which uses a court procedure for the removal of content that is not manifestly illegal but considers any notice to be sufficient for content that is manifestly illegal. *See* Act on Provision of Information Society Services, 458/2002, c. 5, § 22 (Fin.); Gerald Spindler, *Study on the Liability of Internet Intermediaries*, Markt/2006/09/E, at 41 (Nov. 12, 2007), http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

174. This point may raise an "illegal prior restraint" flag in the reader's mind. A trend is, however, emerging in which courts will order the removal of content judged defamatory. *See infra* note 177 and accompanying text.

quests from administrative or law enforcement agencies to remove illegal content.[175] Codifying this practice should not impose a substantial new burden on the private or public actors involved.

The above necessarily invites the further question: Illegal according to which law? Here is the problem of harmonization. Requiring intermediaries to conform to fifty state criminal statutes is untenable. This Note proposes *either* identifying a small class of content that is illegal under state laws across the country (i.e., child pornography, etc.) and excluding such content from the intermediary safe harbor *or* applying the European "law of origin" principle that would require intermediaries to comply only with the criminal laws of the state in which they legally reside. While the first approach would likely lead to greater harmonization, prevent the enforcement of bizarre or idiosyncratic laws, and counter any benefits of corporate forum shopping for legal residence, the latter approach is workable and accords to a greater degree with state jurisdiction over criminal law.

B. Unadjudicated Content: Poster Known

The arguments supporting section 230 CDA-style immunity for intermediaries are at their strongest where the poster is known and the content at issue has not yet been judged illegal. In such circumstances, the U.S. approach operates exactly as it should. It directs the claimant to pursue the defamer rather than the intermediary and also absolves the intermediary from judging the content's legality (or lack thereof), which a court is better placed to do. The policy rationales underlying the U.S. cybertort liability system do not support imposing liability merely because an actor is the least cost avoider or has the deepest pockets.

The U.K.'s 2013 Defamation Act adopts this aspect of the U.S.' approach.[176] The Canadian and European legislatures would be wise to consider it as well, even in cases of intermediary knowledge or editorial control.

C. Unadjudicated Content: Poster Unknown

Anonymous speech raises what may be the most challenging obstacle to intermediary liability schemes, given the difficulties inherent in pursuing an anonymous poster directly to obtain the removal of allegedly illegal or defamatory content. It provokes two interrelated, yet distinct, questions: When should allegedly defamatory anonymous speech be removed by intermediaries? And when should the identity of an anonymous poster be unmasked?

---

175. *See supra* notes 79 and 81 and accompanying text.

176. Defamation Act, 2013, c. 26 §§ 5(2)–(3)(a), 10 (U.K.).

For anonymous defamatory content to be removed without assigning any judgment role to intermediaries, some other actor must judge the content defamatory, in which case we find ourselves in the "content already determined to be illegal" scenario discussed above. Or, there must be a presumption in favor of removal following a notice or complaint. Pursuant to the U.S. constitutional doctrine of prior restraint, however, courts are loathe to enjoin individuals' speech, especially prior to giving the speaker — here an anonymous poster — the opportunity to participate in a full and adversarial adjudication.[177] A presumption in favor of removal would therefore be very problematic. Moreover, a notice-and-takedown system akin to that found in section 512 of the Digital Millennium Copyright Act[178] would be ripe for abuse.[179]

A possible solution is to exclude anonymous content from the scope of section 230 CDA's safe harbor if it has been declared *prima facie* illegal or defamatory by a competent authority. Such a declaration would have no effect on the liability of the poster or even an immediate effect on the liability of the intermediary, as it would merely open the way to, not determine the outcome of, an action in defamation against either party. Nevertheless, once an intermediary receives notice that particular anonymous content has been duly declared *prima facie* illegal or defamatory, the intermediary would be unable to rely on section 230 CDA as a shield from liability if the intermediary does not promptly remove the content. Since the intermediary could therefore be held liable as the content's publisher, it would have a strong incentive to remove the impugned content. Should the content remain posted, the victim of the *prima facie* illegal or defamatory post would, at minimum, be guaranteed the ability to identify at least one defendant — the intermediary — in future legal proceedings. This proposal would not force intermediaries to make judgments about the legality of all of their users' content or even of the content of which they have specific knowledge. However, it would require that, where

177. Oakley, Inc. v. McWilliams, 879 F.Supp.2d 1087, 1089, 1092 (C.D. Cal. 2012) (ruling that the harm caused by defendant is outweighed by the "harm that would be done to our constitutional traditions if courts were to carve out exceptions to the traditional rule and enjoin speech. . . . Injunctions against any speech, even libel, constitute prior restraints . . . ."). *But see* Ardia, *supra* note 169, at 1, 2, 42–43, 51 ("A survey of more than 242 decisions involving injunctions directed at defamatory speech reveals that at least fifty-six decisions have granted or affirmed injunctions, with an especially sharp increase in such decisions after 2000. . . . [N]early half involved speech on the Internet." Ardia concludes that "it is clear that a trend is emerging within both state and federal courts that permits injunctions if the speech in question was adjudged to be defamatory.").

178. Pub. L. 105-304, § 512(c)(1), 112 Stat. 2860 (1998) [DMCA].

179. Indeed, the DMCA takedown regime has been exploited to silence critical speech. *See Unintended Consequences: Twelve Years Under the DMCA*, ELEC. FRONTIER FOUND. 1–2 (Mar. 3, 2010), https://www.eff.org/files/eff-unintended-consequences-12-years_0.pdf. *But see* Medenica & Wahab, *supra* note 4, at 263 (advocating for a DMCA-like takedown regime under the CDA).

content is declared *prima facie* illegal or defamatory, intermediaries either to rely on the outcome of the *prima facie* adjudication or to be prepared to take responsibility for the content themselves.

A streamlined procedure should be developed for the adjudication of whether anonymous content is *prima facie* illegal or defamatory. The victim of the allegedly illegal or defamatory post should be required to petition a court or a designated administrative agency for a declaration as to the content's *prima facie* legality.[180] Intermediaries should be given notice of the application and have the option of making submissions to the adjudicative body, but need not — and in the vast majority of cases should and would not — intervene themselves. Intermediaries should, however, be required to use all reasonable means at their disposal to notify the original poster of the dispute.[181] Accordingly, the original poster could choose to come forward and intervene, or possibly participate anonymously through counsel. If the poster identified him or herself, the intermediary's involvement in the matter would cease, since the case would then fall into the "known poster" scenario discussed earlier.

The burden of proving *prima facie* illegality or defamation should rest with the party alleging unlawfulness, and the adjudicative body should be rigorous in ensuring that the impugned speech does not amount to protected expression (such as opinion). The standard of proof for ordering exclusion from the section 230 safe harbor should be a high one, requiring a showing of *prima facie* illegality or defamation by clear and convincing evidence. Also, the applicant or his or her counsel should be under an affirmative duty to disclose all known, relevant material facts, be they favorable or adverse to the applicant's

---

180. This method is similar to the procedural approach applicable to the "Right to be Forgotten" recognized recently by the Court of Justice of the European Union. *See generally infra* note 185. Under the Court's ruling, a search engine need not comply with a single takedown request sent to it directly — it can refuse them or simply refer them all to the relevant national administrative ("supervisory") or "judicial authority." *See* Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos, ¶¶ 77, 82 (May 13, 2014), http://curia.europa.eu/juris/liste.jsf?num=C-131/12; Charles Arthur, *What Is Google Deleting Under the 'Right To Be Forgotten' — and Why?*, GUARDIAN (July 4 2014), http://www.theguardian.com/technology/2014/jul/04/what-is-google-deleting-under-the-right-to-be-forgotten-and-why. The ruling of the administrative agency is also appealable to a judicial authority. *See* Council Directive 95/46/EC, art. 28, 1995 O.J. (L 281) 31, 47 [hereinafter Data Protection Directive]. The petition to the court should include, *inter alia*, the information required by the U.K.'s 2013 Defamation Act, namely the precise statement being impugned, the meaning which the complainant attributes to the statement, and a confirmation that the complainant does not have sufficient information about the poster to bring legal proceedings directly against that person. *See* The Defamation (Operators of Websites) Regulations, supra note 122, art. 2, ¶¶ 2(b)–(d).

181. A procedure similar to that found in the U.K.'s 2013 Defamation Act could be adopted. Defamation Act, 2013, c. 26 § 5 (U.K.). A message could also be posted next to the allegedly defamatory content alerting readers of the suit.

interest.[182] Penalties could be applied to discourage frivolous applications. As noted above, upon receiving notice of a declaratory order, intermediaries could choose to either remove the *prima facie* illegal or defamatory anonymous content or keep the content posted and waive their section 230 CDA immunity, retaining only the traditional defenses provided to publishers (e.g., truth, opinion). It is likely that in most instances intermediaries would favor removing the *prima facie* illegal or defamatory content rather than risking liability.[183] Again, this proposal would not force intermediaries to make legal judgments, but intermediaries could make such judgments if they so desire.

The availability of such an institutionalized procedure is important in light of the "changing face of defamation litigation."[184] Plaintiffs are often private individuals; defendants are bloggers or individual posters on social networking sites. For many online defamation victims, restoring their online reputation (and the purity of the first page of search results when their names are Googled) is the ultimate goal.[185] Online, "'the truth rarely catches up with a lie.'"[186] Ad-

182. The duty should be akin to that imposed on lawyers appearing *ex parte* by the American Bar Association's MODEL RULES OF PROF'L CONDUCT R. 3.3(d) (1983) ("In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.").

183. I note, however, that it is not unheard of for intermediaries to rally to their users' defense when they feel that a legal procedure is being abused to stifle legitimate expression. *See, e.g.*, Nate Anderson, *YouTube Sails Out of Safe Harbor To Reinstate Marriage Video*, ARS TECHNICA (May 14, 2009), http://arstechnica.com/tech-policy/2009/05/youtube-sails-out-of-safe-harbor-to-reinstate-marriage-video/; Timothy B. Lee, *YouTube Restores Obama Videos, Refuses To Explain Takedown Policies*, ARS TECHNICA (July 19, 2012), http://arstechnica.com/tech-policy/2012/07/youtube-restores-obama-videos-refuses-to-explain-takedown-policies/ (YouTube spokesperson stated that "in cases where [YouTube is] confident that the material is not infringing, or where there is abuse of [its] copyright tools" it may reinstate the challenged content, thereby losing the protection of the DMCA safe harbor). This is liable to occur in cases where the intermediary feels the content is being improperly impugned.

184. Ardia, *supra* note 169, at 10–14.

185. The so-called "Right to be Forgotten," recently recognized under the Data Protection Directive, *supra* note 180, arts. 12(b), 14(a), (L 281) 42–43, by the Court of Justice of the European Union, Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/liste.jsf?num=C-131/12, provides a route by which individuals may attempt to purge search results of private and undesirable links containing information that is "inadequate, irrelevant or no longer relevant, or excessive . . . ." *Id.* at ¶ 94. The right as recognized by the Court is not, however, unqualified. It applies only when the individual's name is used as the search query. *See id.* at ¶¶ 80, 94. Moreover, there is a balancing test involved for removal. Although an individual's privacy rights "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name . . . that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question." *Id.* at ¶ 97; *see also id.* at ¶¶ 81, 96, 99; Jef Ausloos, *European Court Rules Against Google, in Favour of Right To Be Forgotten*, LSE MEDIA POLICY PROJECT (May 13, 2014),

ditionally, awards of monetary damages often constitute Pyrrhic victories for defamation victims.[187] Many victims obtain only "nominal compensation,"[188] and those who secure larger awards must contend with defendants who are unable to pay.[189] More importantly, however, "reputational injuries are not readily translatable into monetary relief; money can neither restore a diminished reputation nor make. . . emotional distress go away,"[190] particularly in our vastly interconnected online world. An adjudicative procedure circumscribing the safe harbor to content that is not *prima facie* illegal or defamatory does not burden intermediaries with the unenviable task of deciding what is and what is not defamatory. But this procedure also discourages intermediaries from permitting evident and injurious libels to perpetually live on in cyberspace. Accordingly, it is a step in the right direction.

The second question posed at the beginning of this subpart — when to unmask the identity of an anonymous user — remains in flux. This question involves a balancing between protecting individuals against defamation and preserving the expression and privacy rights of posters. The precise value and protection to be afforded anonymous speech has not yet been decided in this country[191] or in most others.[192]

---

http://blogs.lse.ac.uk/mediapolicyproject/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/.

186. Barrick Gold Corp. v. Lopehandia, (2005) 71 O.R. 3d 416, at ¶ 32 (C.A.), *citing* Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation and Discourse in Cyberspace*, 49 DUKE L.J. 855, 862–65 (2000).

187. *See generally* Ardia, *supra* note 169.

188. James H. Hulma, *Vindicating Reputation: An Alternative to Damages as a Remedy for Defamation*, 30 AM. U. L. REV. 375, 375 (1981); *see also* Ardia, *supra* note 169, at 16 ("[A] plaintiff must incur substantial legal costs to see a defamation lawsuit through to completion, but '[v]ery few libel plaintiffs suffer enough provable pecuniary loss to justify litigating' their case." (internal citations omitted)).

189. *See, e.g.*, Laura Parker, *Jury Awards $11.3M over Defamatory Internet Posts*, USA TODAY (Oct. 11, 2006), *available at* http://usatoday30.usatoday.com/tech/news/2006-10-10-internet-defamation-case_x.htm (reporting plaintiff knew before trial that defendant was unable to pay and did not have even $1 million, let alone the $11 million jury award).

190. Ardia, *supra* note 169, at 16; *see also* Barry J. Waldman, Comment, *A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach*, 6 RICH. J.L. & TECH. 9, para. 67 (1999), *available at* http://jolt.richmond.edu/v6i2/note1.html (noting that the damaged "pride and self worth of an individual often go beyond the bounds of mere monetary loss.").

191. *Compare* Doe v. Cahill, 884 A.2d 451, 457–58 (Del. 2005) (summary judgment for plaintiff), *with* Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1170–72 (2008) (requiring *prima facie* showing of elements of libel for divulgence of anonymous user's identity), *and* Dendrite International, Inc. v. Doe No. 3, 775 A.2d 756, 760–61, 771 (N.J. App. Div. 2001) (applying summary judgment standard followed by a balancing of plaintiff's prima facie case and poster's interest in anonymity), *and* Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999) (applying motion to dismiss standard), *and In re Subpoena Duces Tecum to America Online*, 2000 WL 1210372 *8 (Va. Cir. Jan. 31, 2000) (applying a good faith standard). *See also* Lidsky, *supra* note 186, at 1377–81 (pointing out divergent standards but suggesting courts are beginning to converge); Tara E. Lynch, Note, *Good Samaritan or Defamation Defender? Amending the Communications Decency Act To*

Once the identity of the poster is determined however, the case would fall into the second category described above, and the intermediary would benefit from full immunity. The question of when it is appropriate to unmask anonymous users does not pertain directly to the topic of this Note and is not addressed herein. However, future legal developments in this area should be informed by a desire for greater certainty, an emphasis on cross-jurisdictional harmonization, and an acknowledgment that not all anonymous speech is necessarily entitled to identical protection.

V. CONCLUSION

This Note is written with the conviction that if one remains "very conscious of the social, political and legal context of the receiving jurisdiction,"[193] one can draw inspiration from the lived experiences and challenges of comparable jurisdictions.

Section 230 CDA has permitted free speech online, and the Internet in general, to flourish in the United States. On occasion, however, its application has yielded unsatisfactory results. By learning from legal approaches of Canada, the European Union, and the United Kingdom, and by keeping in mind both the major cyber-trends at play and the policy choices that define the United States' own approach, this Note seeks to refine and improve the current American treatment of online intermediary liability. In particular, while ensuring that intermediaries continue to be absolved from assessing the legality of their users' content, the proposal set forth aims to provide defamed

---

Correct the Misnomer of Section 230 . . . Without Expanding ISP Liability, 19 SYRACUSE SCI. & TECH. L. REP. 1, 3 (2008).

192. With respect to Canada, see for example MCCONCHIE LAW, *supra* note 98, which explains that a potential libel plaintiff has up to three options to identify an anonymous defamer: (1) instituting a lawsuit against a "John Doe" defendant and seeking to obtain through the discovery of third parties information about the identity of "John Doe"; (2) petitioning for a "bill of discovery" or a "Norwich Order" against a named defendant who has information that would permit the identification of the defamer; or (3) exploiting special rights under certain courts' rules of practice which provide for pre-action discovery (e.g., Nova Scotia). The threshold for disclosure under the first and third options is relatively low, and usually amounts to proof of relevance and that the plaintiff is not embarking on a "fishing expedition." *See* Mosher v. Coast Publ'g Ltd., 2010 NSSC 153, ¶¶ 6–7; Dufault v. Stevens, 1978 CanLII 366 (B.C.C.A.) at ¶ 9. In the case of Norwich Orders, the test is somewhat more onerous and requires consideration of multiple factors as well as the guarantees of freedom of expression and privacy under the Canadian Charter of Rights and Freedoms. *See* Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c. 11 (U.K.) guaranteeing both a personal right to life, liberty, and security, and a right against unreasonable search and seizure). *See also* Pierce v. Canjex Publ'g Ltd., 2011 BCSC 1503, ¶ 12; Doucette v Brunswick News, 2010 NBQB 233; Warman v. Wilkins-Fournier, 2011 ONSC 3023 at ¶¶ 46–54. There are, however, certain tactical and procedural benefits to bringing a petition without having to commence a John Doe lawsuit. *See* Baynham & Reid, *supra* note 52.

193. Rosalie Jukier, *Contract Law: What Can Jersey Learn from the Quebec Experience?*, 14 JERSEY & GUERNSEY L. REV. 131, 149 (2011).

users with a greater ability to have their online permanent records expunged of falsehoods.