Who Should Be Liable for Online Anonymous Defamation?

Ronen Perry† and Tal Z. Zarsky††

INTRODUCTION

The advent of Web 2.0 technologies and applications has enabled average people—who were previously mere consumers of online content—to publish their own content on various websites, such as blogs, consumer-evaluation platforms (such as Amazon, eBay, and TripAdvisor), news websites (through reader comments), social networking services (such as Facebook, Twitter, and LinkedIn), media-sharing websites (such as Instagram and YouTube), and collaborative-writing projects (such as Wikipedia). Some of these user contributions may be defamatory, and one of the most complex and intriguing legal questions in this context is: Who should be liable for defamatory statements made online by anonymous (or pseudonymous) users? This Essay critically evaluates the answers given in various Western jurisdictions and argues that economic analysis supports a revolutionary liability regime, which we call "residual indirect liability."[1]

Our main theoretical contribution lies in recognizing that the legal response to online anonymous defamation should be viewed and analyzed as a combination of two components. The first is the ability (or inability) to bring an action against the content provider—the platform that enables the defamatory statement. Such an action may require modification of substantive law—the recognition of some sort of indirect liability.[2] The second component is the ability (or inability) to bring an action against the speaker—the anonymous user. Such an action does not require modification

† Academic Visitor, Faculty of Law and Centre for Socio-Legal Studies, University of Oxford; Professor of Law and Director of the Aptowitzer Center for Risk, Liability, and Insurance, University of Haifa.

†† Professor of Law, University of Haifa.

1 This Essay's argument is an abridged, restructured, and updated version of an argument first put forth in Ronen Perry and Tal Z. Zarsky, *Liability for Online Anonymous Speech: Comparative and Economic Analyses*, 5 J Eur Tort L 205 (2014).

2 Indirect liability is imposed on one party for another's wrongdoing. See Restatement (Third) of Torts: Apportionment of Liability § 13 & comment a (2000) (discussing the imputation of liability on one party for another's tortious conduct).

of substantive defamation law but does entail adaptation of procedural law, namely, establishing a deanonymization process.

Because this framework provides two potential defendants, each of whom can be either liable or nonliable, at first glance there seem to be four possible liability regimes: (1) neither the speaker nor the content provider is liable, (2) only the speaker is liable (exclusive direct liability), (3) only the content provider is liable (exclusive indirect liability), or (4) both may be liable. To our knowledge, the first option does not exist in any jurisdiction, and for good reason: forgoing liability undermines the delicate balance that has developed in defamation law between the right to reputation and the freedom of speech.[3] In this Essay, we reject the other three alternatives and advocate an outside-the-box solution: the principle of "residual indirect liability."

I. EXCLUSIVE DIRECT LIABILITY

The second possible regime—exclusive direct liability—exists in the United States. Under American law, it is almost impossible to bring a lawsuit against a content provider for users' defamatory statements, even if the content provider knew about the statements' defamatory nature. Traditional defamation law has distinguished among three types of intermediaries: "common carriers," such as telephone companies, which only transmit information and are not liable for defamation;[4] "distributors," such as bookstore owners, which distribute content without having control over it and are liable only if they knew or had reason to know about the defamatory nature of the publication;[5] and "publishers," such as newspapers, which exercise significant control over published content and are subject to strict liability.[6] In the context of online anonymous defamation, this framework has generated skewed incentives.

---

3 For the purposes of this Essay, we assume that, in each jurisdiction, defamation law reflects a proper balance between these two interests, taking into account the values and preferences of the respective society. Thus, we do not aim to challenge the existing boundaries of liability for defamation but rather aim to investigate which combination of direct and indirect liability implements that balance in the most cost-effective way in the context of online anonymous speech.

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

5 Id at 651–52.

6 Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law* 184 (Aspen 4th ed 2011).

In *Cubby, Inc v CompuServe Inc*,[7] the court found that CompuServe, which provided users with online access to a daily newsletter but did not review its content, was a mere distributor and therefore not liable for false and defamatory statements made in the virtual newsletter.[8] Conversely, in *Stratton Oakmont, Inc v Prodigy Services Co*,[9] the court held that Prodigy, a bulletin board operator that exercised some editorial control over user-generated content, was a publisher, and thus could be held liable for defamatory statements made by an anonymous user with respect to a brokerage firm.[10] At least some of the statements about the firm (whose story was depicted in the Martin Scorsese film *The Wolf of Wall Street*) were later found to be true.[11] But it was too late for Prodigy. The joint reading of *Cubby* and *Stratton Oakmont* created an unwarranted incentive for content providers to avoid moderating online discourse, because moderating content exposed them to the risk of liability.[12]

Pressures from the Internet industry quickly led to the enactment of § 230 of the Communications Decency Act of 1996,[13] whereby online service providers should not be considered publishers of "any information provided by another information content provider."[14] In *Zeran v America Online, Inc*,[15] the court held that under § 230 a message board operator could not be found liable for defamatory postings by an anonymous user, even though the operator had relevant knowledge after a certain point and would have been considered a publisher under traditional defamation law.[16] Following *Zeran*, § 230 has provided online

---

7 776 F Supp 135 (SDNY 1991).

8 Id at 141.

9 1995 WL 323710 (NY Sup).

10 Id at *4–5. For a recent discussion of the impact of *Stratton Oakmont*, see Anupam Chander, *How Law Made Silicon Valley*, 63 Emory L J 639, 650–51 (2014) (discussing how Congress reacted to the holding of *Stratton Oakmont* by enacting § 230 of the Communications Decency Act of 1996).

11 Joe Nocera, *Sex and Drugs and I.P.O.'s: Martin Scorsese's Approach in 'The Wolf of Wall Street'* (NY Times, Dec 19, 2013), archived at http://perma.cc/69RN-KFD3.

12 See *Zeran v America Online, Inc*, 129 F3d 327, 331 (4th Cir 1997).

13 Pub L No 104-104, 110 Stat 133, 137, codified as amended at 47 USC § 230.

14 47 USC § 230(c)(1).

15 129 F3d 327 (4th Cir 1997).

16 Id at 330–32.

content providers (be they publishers or distributors under traditional law) with effective immunity[17] in a variety of contexts and from a broad range of causes of action.[18]

On the other hand, American courts can order content providers to disclose information about anonymous wrongdoers. The right to anonymity is well established under American law, and in some instances—especially when pertaining to speech and assembly—it receives constitutional protection.[19] But when there is sufficient evidence to establish a cause of action against an anonymous wrongdoer, courts enable victims to apply for a John Doe subpoena, ordering a third party—here the content provider or the Internet Service Provider (ISP)—to divulge information it possesses about the anonymous wrongdoer.[20] There is still some controversy about the standard of evidence for establishing the plaintiff's claim, which must be met prior to issuing such an order,[21] but this procedural tool's availability is undisputed.

From an economic perspective, the speaker's liability is a special case of direct tort liability, so its economic justifications are similar—efficient deterrence is the primary goal.[22] However, in the case of online anonymous defamation, direct liability raises several problems. First and foremost, it entails a special effort in

---

[17] However, empirical studies have shown that more than one-third of such claims survive the § 230 defense, and accordingly websites often have to engage in long and expensive legal battles. See Chander, 63 Emory L J at 655 (cited in note 10); 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 Loyola LA L Rev 373, 493 (2010).

[18] For an extensive list of cases, see Chander, 63 Emory L J at 653 n 58 (cited in note 10). The author concludes that § 230 "largely immunized online service providers from secondary liability for most torts committed through their service." Id at 651.

[19] See A. Michael Froomkin, *Anonymity and the Law in the United States*, in Ian Kerr, Valerie Steeves, and Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* 441, 442 (Oxford 2009).

[20] Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 Yale L J 320, 325 (2008) (examining the efficacy of John Doe subpoenas and suggesting a change to the system).

[21] See Solove and Schwartz, *Information Privacy Law* at 600 (cited in note 6). See also Gleicher, 118 Yale L J at 325, 337, 340–50 (cited in note 20) (identifying seven cases addressing distinct standards and adding the "good faith standard"—a slightly altered "summary judgment" rule in a case that involved trespass to chattels—as well as an altered "prima facie" rule). Courts have begun using a stricter standard for "unmasking" anonymous third parties. Id at 343. See also, for example, *Doe v 2TheMart.com Inc*, 140 F Supp 2d 1088, 1096–97 (WD Wash 2001) (quashing a subpoena request for identification of anonymous online users because the request failed to show that the information related to the core claim).

[22] See generally Alain Sheer and Asghar Zardkoohi, *An Analysis of the Economic Efficiency of the Law of Defamation*, 80 Nw U L Rev 364 (1985) (analyzing the goals and consequences of defamation law from an economic perspective).

identifying the wrongdoer. The victim needs to obtain the anonymous speaker's Internet Protocol (IP) address from the content provider and then obtain the anonymous speaker's identity from the ISP, as identified by the IP address. Because these two steps jeopardize both the anonymous speaker's freedom of speech and his or her right to privacy, the legal process is cautious and complex and therefore very costly to navigate. Moreover, sophisticated users can hide their IP addresses by, for example, using anonymizing proxy servers or anonymizing software such as Tor.[23] Even when the real IP address used for wrongdoing can be ascertained, it may be very difficult to attribute the defamatory statement to a specific person if the wrongdoer was connected to a publicly accessible router (for example, at a coffee shop, hotel, or library)[24] or—perhaps illegally—to another person's private router.[25] An action against the speaker may also be impossible if neither the content provider nor the speaker's ISP retains a log of users' activities for a long-enough period (as occurred in *Zeran*).[26] Finally, a legal disclosure mechanism would often be restricted by territorial boundaries, enabling anonymous speakers who

---

[23] See Doug Lichtman and Eric Posner, *Holding Internet Service Providers Accountable*, 14 S Ct Econ Rev 221, 234 (2006) (explaining that sophisticated wrongdoers can "conceal their tracks by routing messages through a convoluted path that is difficult for authorities to uncover"); Raymond Placid and Judy Wynekoop, *Tracking Down Anonymous Internet Abusers: Who Is John Doe?*, 85 Fla Bar J 38, 39 (2011) (discussing the use of proxy servers, enabled by services such as Tor, that can mask anonymous posters' IP addresses). In the related context of online anonymous copyright infringement, a federal district court explicitly admitted that "the technology that enables [wrongdoing] has outpaced technology that prevents it." *Hard Drive Productions, Inc v Does 1-90*, 2012 WL 1094653, *7 (ND Cal) (denying a discovery request to identify anonymous online users in a copyright infringement case).

[24] In fact, this was one of the reasons for denying a John Doe subpoena in the copyright infringement case of *VPR Internationale v Does 1-1017*, 2011 WL 8179128, *2 (CD Ill) ("The list of IP addresses attached to VPR's complaint suggests, in at least some instances, a similar disconnect between IP subscriber and copyright infringer. The ISPs include a number of universities, such as Carnegie Mellon, Columbia, and the University of Minnesota, as well as corporations and utility companies.").

[25] See, for example, Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks* (NBC News, Apr 24, 2011), archived at http://perma.cc/L5VC-HYHB (describing cases in which homeowners were initially accused by federal agents for downloading child pornography but it later came to light that other parties had connected to the homeowners' wireless routers to commit these offenses).

[26] *Zeran*, 129 F3d at 329 n 1. The cost of information retention is correlated with the amount of daily traffic and the required duration of retention. More importantly, retention laws should not infringe basic rights. On April 8, 2014, the European Court of Justice held that the EU Data Retention Directive, Directive 2006/24/EC, which required telecom companies to store user data for up to two years, was invalid because it infringed on the right to privacy and the right to the protection of personal data. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*, Case C-293/12, 2014 ECJ CELEX LEXIS 238, *19–20 (Court of Justice 2014).

make defamatory statements on foreign websites or through foreign ISPs to get off scot-free. For example, the Supreme Court of Virginia recently examined the "territorial limits of [its] subpoena power."[27] It vacated a John Doe subpoena issued at the request of a Virginia carpet-cleaning business to a California-based business-rating website (Yelp), which published anonymous users' negative reviews of the plaintiff, because the statements were published outside its jurisdiction.[28] If the defamatory statements were published in a different country, rather than a different state, the plaintiff would face even greater obstacles.

In summary, identifying an online anonymous speaker might be very difficult. If the speaker is not identified, he or she evades liability, the costs of anonymous defamation are not fully internalized, and the potential wrongdoers are not efficiently deterred. If, on the other hand, the speaker is identified through a costly process, wrongdoers may internalize the costs of their wrongdoing, but the administrative costs may outweigh the benefits in terms of cost-reducing deterrence. Alternatively, the high administrative costs associated with identifying the primary wrongdoer might render another party (for example, the content provider) a more cost-effective target for enforcement efforts. Exclusive direct liability can raise additional problems, which we shall not elaborate on here due to space constraints, such as the relatively high likelihood that there will be judgment-proof defendants.

II. EXCLUSIVE INDIRECT LIABILITY

The third possible regime—exclusive indirect liability—seems to apply in Israel. On the one hand, Israeli law recognizes content providers' liability under certain circumstances. First, § 11 of the local Defamation Act[29] provides that if a communication medium publishes defamatory content, its operator can be held liable.[30] However, because the term "communication medium" covers only newspapers, radio, and television,[31] the potential use of § 11 in cases of online anonymous defamation is very

---

27 *Yelp, Inc v Hadeed Carpet Cleaning, Inc*, 770 SE2d 440, 444 (Va 2015).

28 Id at 445–46.

29 5714-1954 (1964–66) (Isr), in 62 *Laws of the State of Israel* 254 (Ministry of Justice, trans).

30 Id.

31 Id.

limited. Second, negligent supervision of user-generated content may result in liability for negligence.[32]

On the other hand, there is no procedural tool for obliging intermediaries to disclose information about anonymous users, so such users have de facto immunity. In *Mor v Barak ITC*,[33] the Israeli Supreme Court held that there is no procedural framework for granting an order that obliges a content provider to reveal an anonymous user's identity, and that such a framework should not be devised through the judicial system.[34] As a matter of fact, the Court's holding reflects a conscious preference for freedom of speech in general and anonymous speech in particular, rather than a genuine lack of procedural tools. This judicial policy was also affirmed in the related context of online anonymous copyright infringement.[35] While several attempts have been made to introduce a deanonymization procedure through primary legislation,[36] none has succeeded.

An exclusive indirect liability regime overcomes some of the problems associated with direct liability—including underdeterrence of anonymous speakers—but raises new difficulties. First, the cost of precautions available to content providers may be prohibitively high. Human monitoring of user-generated content entails hiring and training staff to read such content and distinguish between legitimate and nonlegitimate content. The cost per statement is substantial, and it is incurred with respect to all user-generated content—as opposed to the cost of identifying an anonymous speaker under a direct liability regime, which is incurred only in the rare case of a legal complaint about a defamatory statement. Automated monitoring requires the development and implementation of technologies that preclude defamatory statements while allowing legitimate speech. Once the mechanism has been developed, it can be implemented at a very low marginal cost—but automated systems are still expected to make more judgment mistakes than trained humans, and human correction mechanisms are costly. Alternatively, content providers

---

[32] Permission Civ App 1700/10 *Dubitsky v Shapira*, *6–7 (unpublished, Isr S Ct 2010).

[33] Permission Civ App 4447/07 *Mor v Barak ITC–Intl Telecommunications Corp*, 63(3) PD 664 (Isr S Ct 2010).

[34] Id at 717.

[35] Civ App 9183/09 *The Football Association Premier League v John Doe*, *33 (unpublished, Isr S Ct 2012).

[36] See, for example, Disclosure of User Information in Electronic Communications Network Bill, 2011 HH 36 (Isr); Disclosure of User Information in Electronic Communications Network Bill, 2012 HH 1376 (Isr).

may be required to employ a "notice-and-takedown" procedure, in which the content provider removes user-generated content when notified that this content is suspected of being defamatory.[37] The main advantage of this method is that it significantly reduces monitoring costs. But an automatic notice-and-takedown system enables anyone with the desire to silence another's speech to do so easily and to engage in mass censorship,[38] whereas integrating human discretion in the system increases the costs.

Moreover, most user-generated content is legitimate and socially beneficial. Web 2.0 users "create positive externalities enjoyed by advertisers, information providers, merchants, friends, and acquaintances."[39] Yet indirect liability makes content providers internalize the expected harms caused by (rare) defamatory statements, without capturing the full social benefits of their activities.[40] This may result in overdeterrence in the form of excessive monitoring and overzealous censorship by content providers.[41]

Finally, even if content providers choose the proper level of care, uncertainties may arise with respect to the defamatory nature of each statement. These uncertainties force content providers to choose between two types of potential errors: (1) false negatives, namely, identifying a defamatory statement as nondefamatory; and (2) false positives, namely, identifying a nondefamatory statement as defamatory. Because a content provider's liability derives from the publication of a defamatory statement by a user, a false negative carries the risks of litigation

---

[37] A notice-and-takedown regime applies to online copyright infringements in the United States. See 17 USC § 512. See also Douglas Lichtman and William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 Harv J L & Tech 395, 396–99 (2003) (discussing the common-law doctrines of contributory infringement and vicarious liability as methods utilized by courts to hold third parties liable for copyright infringement).

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

[39] Lichtman and Posner, *Holding Internet Service Providers Accountable* at 225 (cited in note 23) (referring to ISP subscribers in general).

[40] Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 Cornell L Rev 901, 917–18, 921 (2002).

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

and liability whereas a false positive does not. In our case, acting on a false positive does not seem to have a real cost at all (removal is almost costless). This imbalance induces content providers to remove suspicious yet nondefamatory speech: to avoid liability, companies would rather err on the side of silencing speech.[42] In addition, they may be induced to block provocative users, disable user contributions, or reduce demand for Web 2.0 technologies, thus impeding progress and innovation.

III. CONCURRENT LIABILITY

The fourth possible regime—concurrent liability—exists in the European Union. In the absence of relevant EU Regulations, a comprehensive analysis of the law applicable to the issues at hand calls for a separate examination of the national law in each member state, and state laws differ in many respects.[43] In this Essay we merely strive to delineate the contours of the European framework. These are drawn by the E-Commerce Directive[44] and by two decisions of the European Court of Human Rights in the case of *Delfi AS v Estonia*.[45] These sources define a general model, which can be compared to the alternatives even without delving into the intricacies of its implementation in each member state.

On the one hand, a victim of online anonymous defamation can frequently bring an action against the content provider. True, Article 14 of the E-Commerce Directive provides that some intermediaries (such as hosting service providers) are liable only if they knew about the wrongful statement and failed to remove it following the victim's request (a notice-and-takedown regime).[46] But many content providers are not considered intermediaries for these purposes. In *Delfi*, the European Court of Human Rights held that a news website was liable for defamation in anonymous

---

[42] See *Zeran*, 129 F3d at 333:

> Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. . . . Thus, [indirect liability] has a chilling effect on the freedom of Internet speech.

[43] Thibault Verbiest, et al, *Study on the Liability of Internet Intermediaries* *14 (Nov 12, 2007), archived at http://perma.cc/Y9WQ-6TXN ("National implementation and court practice differ between member states considerably when assessing actual knowledge.").

[44] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 OJ L178 1 (July 17, 2000).

[45] App No 64569/09 (Eur Ct Hum Rts 2013).

[46] Directive 2000/31/EC, 2000 OJ L178 at 13 (cited in note 44).

user comments.[47] The Court agreed that the website was a publisher rather than an intermediary, and that it therefore was not exempt from the duty to monitor or from liability, despite implementing a notice-and-takedown system.[48] In mid-June 2015, the Grand Chamber of the Court upheld the earlier decision, possibly limiting its application to news portals.[49]

On the other hand, the European framework enables the court to order content providers to disclose information about anonymous speakers. Article 15(2) of the E-Commerce Directive allows member states to establish obligations for service providers to transfer users' identifying information to competent authorities, including courts.[50] Of course, disclosure processes should comply with the Data Protection Directive,[51] the E-Privacy Directive,[52] and national data protection laws, rendering such processes complex and state specific.[53] Regardless, there are examples of disclosure orders in cases of online anonymous defamation. For instance, at the request of Irish-based airline Ryanair, the Irish High Court issued an order requiring Eircom, the Irish national telecommunications provider, to disclose the identities of anonymous users who posted defamatory comments about the airline.[54]

Concurrent liability has two advantages. First, by imposing liability on content providers in addition to online speakers, it overcomes the main flaw of exclusive direct liability: underdeterrence resulting from the high cost of identifying and pursuing anonymous speakers (and to a lesser extent from the problem of

---

47 *Delfi*, App No 64569/09 at *33–34. See also generally Mart Susi, *International Decision:* Delfi AS v. Estonia, 108 Am J Intl L 295 (2014) (discussing the *Delfi* decision).

48 *Delfi*, App No 64569/09 at *31–32.

49 *Delfi AS v Estonia*, App No 64569/09, *34 (Grand Chamber 2015).

50 Directive 2000/31/EC, 2000 OJ L178 at 13 (cited in note 44).

51 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 OJ L281 31 (Nov 11, 1995).

52 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communication), 2002 OJ L201 37 (July 31, 2002).

53 See Verbiest, et al, *Study on the Liability of Internet Intermediaries* at *77–82 (cited in note 43).

54 *Ryanair Seeks to ID 'Defamatory' Online Parties* (Irish Examiner, Feb 13, 2013), archived at http://perma.cc/GV7F-D7PP. For further discussion of Irish case law, see Verbiest, et al, *Study on the Liability of Internet Intermediaries* at *78–79 (cited in note 43). Irish law makes use of Norwich Pharmacal orders to uncloak anonymous speakers, a measure originating in the United Kingdom (and discussed in Part IV).

judgment-proof defendants). If the speaker is not sufficiently deterred because he or she can be identified only at a very high cost or not at all, or if he or she cannot fully compensate the victim, indirect liability incentivizes content providers to take the necessary precautions. Second, parties who are jointly liable for a particular harm have an interest in reducing their own shares of the burden. Because any difficulty in identifying and pursuing speakers will result in greater expected liability for the content provider, the latter has an incentive to facilitate the identification of anonymous speakers. To do so, content providers may collect user information and volunteer this information in the case of a lawsuit.[55]

However, concurrent liability also has several disadvantages. First, to the extent that both parties are at risk of being liable and that each has a somewhat different perception of what may constitute defamation, imposing liability on both may restrict freedom of speech more than singling out one defendant ("double censorship").[56] Second, a combination of direct and indirect liability may result in an aggregation of the implementation costs of both. Content providers will be led to monitor user-generated content at a high cost that could be saved under an effective direct liability regime. At the same time, lawsuits will be brought against anonymous speakers at high administrative costs that could be saved under an effective indirect liability regime.

IV. RESIDUAL INDIRECT LIABILITY

So far we have established the following: exclusive direct liability entails prohibitively high identification costs, exclusive indirect liability involves high monitoring costs, and concurrent liability aggregates these two types of costs. In our opinion, the efficient solution for online anonymous defamation lies beyond the four classical categories explained in the Introduction and involves an innovative combination of direct and indirect liability. In a legal regime that we call "residual indirect liability," the speaker is exclusively liable, but if he or she is not reasonably reachable, the content provider becomes liable. We found an

---

[55] Content providers might not be very keen to drag their users into court, because this may harm their business. But the ability to share the burden will surely result in some increase in the likelihood of data collection.

[56] The set of statements considered defamatory by either party is the union of the set of statements considered defamatory by the speaker and the set of statements considered so by the content provider, which is equivalent to or larger than each set individually.

interesting development in this direction in England, in the recently enacted Defamation Act 2013[57] ("Defamation Act"). For over forty years, English law has recognized the Norwich Pharmacal Order, by which a third party who becomes involved in the tortious acts of another is obliged to submit information that can assist the victim in establishing his or her claim against the wrongdoer, regardless of whether the third party was voluntarily involved.[58] Such orders have frequently been issued in the context of online anonymous defamation.[59]

The Defamation Act links the speaker's availability to the content provider's liability. Section 5(2) stipulates that a website operator is generally not liable for a defamatory statement posted on the website if it was not the one who posted that statement.[60] However, the defense can be defeated (and the content provider exposed to liability) if the victim had insufficient information to identify and bring proceedings against the speaker, the victim gave notice of the complaint, and the content provider did not properly respond to the complaint.[61] A proper response requires either obtaining the speaker's contact information and providing it to the victim, or removing the defamatory content.[62]

Under this innovative regime, costly monitoring may become redundant, and overdeterrence caused by noninternalization of the vast economic benefits of Web 2.0 technologies and by the asymmetric response to errors in judgment is avoided. Theoretically, if content providers under a residual liability regime allow postings by unreachable speakers, they might still need to monitor to avoid liability. Even so, monitoring will be limited to content generated by unidentifiable speakers, so the cost will be much lower than in the case of exclusive indirect liability or concurrent liability. In practice, content providers would probably prefer to avoid liability through cheaper means such as (1) obtaining user identification data, at least when an automatic content analysis algorithm identifies suspected defamation, or (2) removing content generated by unreachable speakers on notification of its defamatory potential. At the same time, this regime incentivizes content providers to take measures that reduce the cost of

---

57 Ch 26 (UK). The Act was enacted by the Parliament of the United Kingdom but generally extends only to England and Wales. Defamation Act, ch 26 § 17(2).

58 See *Norwich Pharmacal Co v Customs and Excise Commissioners*, 1974 App Cas 133, 133–34, 175 (HL 1974).

59 See, for example, *Totalise PLC v The Motley Fool Ltd*, [2001] EWHC 706 (QB).

60 Defamation Act, ch 26 § 5(2).

61 Defamation Act, ch 26 § 5(3)–(4).

62 See Defamation Act, ch 26 § 5(3)(c), (5).

identifying anonymous wrongdoers (measures like collecting user identification data), and thereby deters wrongdoing. Finally, it does not raise the characteristic problems of concurrent liability, particularly cost aggregation.

Admittedly, this method is not perfect, but its main flaws are either minor or solvable. For example, on the constitutional level, collecting and providing user information may jeopardize the right to speak with anonymity (especially in the United States)[63] and the right to privacy (especially in the European Union).[64] However, these problems seem solvable: databases can and should be protected, and information may be disclosed only when a court determines that several preconditions—including, for example, a high likelihood that an action for defamation will succeed—are met. The English Defamation Act provides a somewhat different solution by allowing the speaker to decide whether he or she wishes to directly confront the victim or prefers that the statement simply be removed. On the economic level, a content provider may get off scot-free by providing information about the speaker, even when the latter is judgment-proof. In such cases, no one bears the full burden, so the incentives are impaired. However, this problem seems minor: while content providers usually have deeper pockets than users, the scope of the harm caused in the typical online defamation case may not be beyond the speaker's compensation capacity. The harm may be particularly small in the case of anonymous defamation, given the relatively weak reliability and credibility of anonymous speakers. If there are nonetheless settings in which speakers cannot normally compensate for the harm caused, an extension of content providers' liability under the residual indirect liability regime may be appropriate.

In summary, residual indirect liability simultaneously solves the main problems of exclusive direct liability and exclusive indirect liability without raising the problems of concurrent liability. While it may raise some other difficulties, these complications are mostly insignificant or easily solvable. Thus, this model should be

---

[63] See *McIntyre v Ohio Elections Commission*, 514 US 334, 357 (1995) (finding that an author's decision to remain anonymous is protected by the First Amendment); *Doe v 2TheMart.com, Inc*, 140 F Supp 2d 1088, 1092 (WD Wash 2001) ("A component of the First Amendment is the right to speak with anonymity. . . . The right to speak anonymously extends to speech via the Internet.").

[64] See, for example, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources*, Case C-293/12, 2014 ECJ CELEX LEXIS 238, *19–20 (Court of Justice 2014) (finding that the EU Data Retention Directive infringed the right to privacy and the right to the protection of personal data).

seriously considered by legislatures interested in efficiently regulating online anonymous defamation.[65]

CONCLUSION

This Essay examines various solutions to the problem of online anonymous defamation. The American model bars content providers' indirect liability but facilitates identification of the speaker. From an economic perspective, the main problem with this model is that direct liability for online anonymous defamation entails special efforts in identifying and pursuing the speaker. If the speaker is not identified, the costs of defamation are not fully internalized and potential wrongdoers are not efficiently deterred. If the speaker is identified through a costly process, the administrative costs may outweigh the benefits in terms of cost-reducing deterrence.

The Israeli model recognizes content providers' liability in some circumstances but does not provide procedural tools for identifying the speaker. The basic problem with exclusive indirect liability is the relatively high cost of precautions. Monitoring is very costly, and while a notice-and-takedown scheme may reduce costs, an automatic system may result in excessive limitation of the freedom of speech—and human discretion once again entails very high costs, especially for websites with heavy traffic. Another problem is that content providers do not capture the full social benefits of their activities, so bearing the costs may result in overdeterrence. A third problem is the asymmetric legal response to errors with respect to the defamatory nature of statements (a false negative carries the risks of litigation and liability whereas a false positive does not).

The EU framework enables the victim to request identification of the speaker and simultaneously bring an action against the content provider. Although there is variance among member states, this model seems to comply with the relevant Directives and European Court decisions. Concurrent liability ensures that proper measures are taken to avoid defamation even if the anonymous speaker cannot be identified and pursued at a reasonable

---

[65] For alternative solutions to the problem of online defamation, see Paul Ehrlich, Note, *Communications Decency Act § 230*, 17 Berkeley Tech L J 401, 401–02, 411–19 (2002) (arguing for either a return to distributor liability or a combination of blanket immunity and elimination of anonymity); Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J Telecomm & High Tech L 101, 102, 117 (2007) (discussing a safe harbor system "requiring intermediaries to retain and disclose the identity of their customers in response to a subpoena").

cost. Moreover, it incentivizes each content provider to facilitate the identification of anonymous speakers in order to reduce its own expected burden, thereby increasing the likelihood of internalization by the primary wrongdoer. But concurrent liability may restrict freedom of speech more than singling out one defendant, and it may lead to the aggregation of the implementation costs of direct and indirect liability.

The recently adopted English model enables the victim to pursue a claim against the speaker, and it imposes liability on the content provider if the speaker is unavailable. Residual indirect liability has several advantages: it significantly reduces the need for monitoring and prevents the overdeterrence associated with unaccounted benefits and asymmetric responses to errors; it incentivizes content providers to reduce the costs of identifying anonymous wrongdoers; and it does not raise the characteristic problems of multiple defendants, such as the excessive restriction of the freedom of speech or the aggregation of costs. This model may also raise difficulties on the legal and economic levels, but they seem to us either insignificant or solvable.