DEFAMATION AND INVASION OF PRIVACY IN THE INTERNET AGE

Neville L. Johnson, Douglas L. Johnson, Paul Tweed & Rodney A. Smolla*

I. INTRODUCTION

The era of anonymous defamation and Internet impersonation has arrived. Given a largely unregulated Internet landscape and boundless international access to information online, it is no surprise that the Internet has become a minefield of defamation and invasion of privacy violations.

* Neville L. Johnson and Douglas L. Johnson specialize in media and entertainment litigation, and are partners at Johnson & Johnson, LLP, in Beverly Hills, California. Paul Tweed specializes in media and entertainment litigation and is a Senior Partner at Tweed, with offices in London, Dublin and Belfast. He is the author of PRIVACY AND LIBEL LAW: THE CLASH WITH PRESS FREEDOM (2012). Rodney A. Smolla is Dean and Professor of Law at the Widener University, Delaware Law School, and author of the treatise LAW OF DEFAMATION (1986). Zita Aradi, while a student at the University of California, Berkeley; Ashley Hunt Conlogue, then a student at Loyola Law School, Los Angeles; and Karine Panosian and Nadia Sokolova, then students at Southwestern Law School, contributed to this article.

Problems with access and anonymity are compounded by the fact that Internet content is largely permanent, allowing victims of Internet defamation and invasions of privacy to suffer continuous harm to their reputation and right to be left alone. In yesteryear, the effects of print libel disappeared as newspapers and magazines were consigned to waste baskets or to the far reaches of stacks in a library. With Internet defamation, however, offending content almost never comes down once it has been posted. In addressing the changes in technology and media, the following will discuss current strategy and legal liabilities for defamation, including international perspectives on litigation abroad.

At the center of increasing Internet defamation is § 230 of the Communications Decency Act (CDA).[1] Passed in 1996, the Act gives Internet service providers (ISPs) virtually complete immunity against claims for Internet defamation. Although § 230 was initially approved with lofty goals of developing the Internet and promoting ISP self-regulation, the Act substantially underestimated the shape the Internet would take and its long-term effects. The rise of social media websites and Internet chat forums have completely transformed the way individuals interact and share information. Notwithstanding the Internet's positive impacts on society, it has also provided individuals with the unlimited ability to post defamatory content online.

The harms caused by callous and sometimes relentless defamers are enormous. Numerous harrowing defamation stories from our legal experience demonstrate why this issue deserves greater political attention.[2] In one case, for example, a successful attorney was incessantly taunted by a disgruntled former suitor who created a website virtually dedicated to defaming the attorney. While certain ISPs complied with takedown requests, others required injunctions. Even as counsel successfully enjoined offending websites, the defamer, who could never be physically located, continuously changed ISPs. Eventually, the defamer opted to use a foreign ISP to avoid U.S. jurisdiction over the website entity.

In another case, a California resident was falsely impersonated on Facebook by an individual living in Europe.[3] This individual executed a vendetta against the California resident by creating a false Facebook profile,

1. Communications Decency Act (CDA) of 1996, 47 U.S.C. § 230 (2012).

2. Victims' identities have been concealed to ensure their safety and privacy.

3. Impersonations have become so widespread that there are a number of support groups dedicated to raising awareness and building a sense of community for victims. See, for example, organizations such as WORKING TO HALT ONLINE ABUSE, http://www.haltabuse.org (last visited Aug. 28, 2018); and WITHOUT MY CONSENT, https://withoutmyconsent.org (last visited Aug. 28, 2018).

advertising that the victim sought to engage in homosexual activity and was looking for contact from all interested parties. Much like the first example, such personal attacks on the victim significantly impacted the victim's professional life and inflicted a great deal of personal distress. Most unfortunate of all is that the current legal framework made it very difficult for either injured party to recover from such defamation.

II. SECTION 230

A. *History Behind Section 230*

§ 230 of the CDA arose as an attempt to resolve the inconsistent rulings in *Cubby, Inc. v. Compuserve, Inc.*, and *Stratton Oakmont, Inc. v. Prodigy Services Co.*, regarding the treatment of ISPs as distributers or publishers of online content. In *Cubby*, the plaintiffs sued Compuserve for hosting defamatory content on a web page known as "Rumorville."[4] Compuserve argued that it was merely an electronic library that gave subscribers access to information sources and special interest forums, classifying it as a distributer of information content and thus relieving Compuserve of liability. Granting summary judgment to Compuserve, the court held that, since the ISP functioned the way a typical print distributor would, it exercised little editorial control and so could not be held responsible for defamation.[5]

In *Stratton Oakmont*, however, the court came to the opposite conclusion, ruling that Prodigy (the ISP) was liable as a publisher.[6] Unlike Compuserve, Prodigy maintained some editorial control over its webpages. Given this minimal control, the court determined that the ISP functioned like a full-fledged publisher and therefore should be liable for the content uploaded to its pages.[7] *Stratton Oakmont* created serious problems for ISP self-regulation by increasing the probability that ISPs would be held responsible for their information content.

---

4. Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135, 137 (S.D.N.Y 1991).

5. *Id.* at 140-41.

6. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 712, at *3-4 (N.Y. Sup. Ct. Dec. 11, 1995), *superseded by statute*, Communications Decency Act of 1996, Pub. L. No. 104-104, § 230, 110 Stat. 56, 137-139, *as recognized in* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

7. *Stratton Oakmont, Inc.*, 1995 N.Y. Misc. LEXIS 712, at *4.

To mitigate the effects of *Stratton Oakmont*, and induced by the media and ISP lobbies, Congress passed § 230 of the Communications Act in 1996.[8] § 230 passed with virtually no opposition as legislators saw ISP immunity as a way to promote Internet growth, protect free speech, and encourage ISP self-regulation. Unfortunately, the section did not achieve these goals as envisioned. Instead of promoting good faith efforts to prevent defamation and invasions of privacy, ISPs have since used their § 230 immunity as an affirmative defense against Internet libel lawsuits.

B. *Defamation Litigation After the Passage of Section 230*

One of the first cases to successfully utilize § 230 as a defense was *Zeran v. America Online, Inc.*[9] In *Zeran*, plaintiff Kenneth Zeran was defamed by an anonymous Internet poster who created false advertisements about Mr. Zeran on an online forum. The advertisements suggested Mr. Zeran had produced insensitive T-shirts about the Oklahoma City bombing and that he was looking to sell these T-shirts to all interested buyers, and provided Zeran's home number for inquiries.[10] Although America Online (AOL) eventually removed the posts at Zeran's request, Zeran later sued AOL for negligence, arguing that AOL failed to quickly and adequately respond to the notices posted on the Internet bulletin.[11] The court disagreed, and, in looking to § 230, held that plaintiffs seeking to hold ISPs like AOL liable for defamation for failure to exercise some editorial powers (in this case, for not taking down defamatory posts) would be equivalent to placing the ISPs in the publisher's role.[12] Thus, Zeran's claims were preempted by § 230.[13]

---

8. *See* Communications Decency Act of 1996, Pub. L. No. 104-104, § 230, 110 Stat. 56, 137-139 ("It is the policy of the United States . . . to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.") (codified as amended at 47 U.S.C. § 230(b) (2012)); Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

9. *Zeran*, 129 F.3d at 228, 330-31 (upholding the district court's grant of summary judgement in favor of AOL on the grounds that § 230 of the Communications Decency Act "plainly immunize[d] computer service providers like AOL from liability for information that originate[d] with third parties").

10. *Id.* at 329.

11. The court notes that Kenneth Zeran received an influx of abusive calls and death threats. In just five days after the original post, Zeran "was receiving an abusing phone call approximately every two minutes." *Id.*

12. *Id.* at 328.

13. *Id.* at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for

Since *Zeran*, courts continue to provide strong protections for ISPs and have upheld immunity in even questionable situations. *Reit v. Yelp!, Inc.* is one such example wherein dentist Glenn Reit sued Yelp for defamation after noticing that Yelp had selectively removed positive reviews regarding Reit's dental practice but left negative reviews.[14] Although Reit argued that Yelp's practices were part of a directed "business model," the court found that such activity was within Yelp's editorial powers and thus protected by § 230.[15]

In similar fashion, the court held in *Asia Economic Institute v. Xcentric Ventures, LLC* that a website could not be held responsible for the content of third-party consumer reports, even though the website mechanically altered the reports so that they would be more visible to Internet traffic using search engines such as Google.[16] The court explained that "increasing the visibility of a statement is not tantamount to altering its message."[17] The court thus extended § 230 immunity to any website that did not alter the substantive content displayed on its site.[18]

An ISP's selective removal or alteration of posts is also different from actively posting comments to their own site. In *Jones v. Dirty World Entertainment Recordings, LLC*, for example, a cheerleader sued the online tabloid "The Dirty" for several allegedly defamatory submissions published by the tabloid, several anonymous postings, and remarks posted by the manager.[19] Jones requested that The Dirty remove the stories, but her request was denied.[20] She subsequently filed a lawsuit against the website and its owners, asserting defamation, false light, and intentional infliction of emotional distress.[21] The district court held that Dirty World was not immune under the CDA because Dirty World developed the information.[22] On appeal, however, the decision was reversed because the district court construed the term "develop," taken from the *Roomates.com* case, too

its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.").

14. Reit v. Yelp!, Inc., 907 N.Y.S.2d 411, 412 (N.Y. Sup. Ct. 2010).

15. *Id.* at 412-14.

16. Asia Econ. Inst. v. Xcentric Ventures, L.L.C., No. CV 10-01360 SVW(PJWx), 2011 U.S. Dist. LEXIS 145380, at *21-23 (C.D. Cal. May 4, 2011).

17. The court also noted that liability would only be found in situations where the host had made substantive alterations to the content of the postings. *Xcentric Ventures, L.L.C.*, 2011 U.S. Dist. LEXIS 145380, at *18-20.

18. Xcentric operates the website ripoffreport.com. *See infra* note 121.

19. Jones v. Dirty World Entm't Recordings, L.L.C., 755 F.3d 398, 409-10 (6th Cir. 2014).

20. *Id.* at 403.

21. *Id.* at 404-05.

22. *Id.* at 409.

broadly. The court explained that such a broad interpretation would defeat the purposes of the CDA and would swallow the immunity that § 230(c) provided for the "exercise of a publisher's traditional editorial functions."[23]

Immunity for ISP hosts extends even so far as to protect those who affirmatively republish information. *Barrett v. Rosenthal* exemplifies how extensive immunity is for ISPs.[24] In *Rosenthal*, an alternative medicine advocate republished a defamatory article on her message board, which discussed two "quackbusters" who campaigned against her practices.[25] Even though the host took an active role in selecting and disseminating the article, she was granted § 230 immunity because she was found to be "a mere distributor" of content.[26] In so stating, the court provided comprehensive immunity to all providers who merely "republish" content.[27]

§ 230 immunity even protects ISPs that host illegal or obscene material. In *Chicago Lawyers' Committee v. Craigslist, Inc.*, Chicago Lawyers' Committee sued Craigslist for hosting offensive and racist housing advertisements.[28] Some of the discriminatory language included statements such as "No Minorities" and "Requirements: Clean, Godly Christian Male."[29] While Craigslist maintained a company policy of removing offensive content if such content was reported, the court ruled that Craigslist was not required to pre-screen content for potential violations. The court reasoned that to hold Craigslist liable for third party content hosted on their pages would be

23. *Id.* (rejecting an interpretation of "development" that would make a website operator "responsible for the development of content created by a third party merely by displaying or allowing access to it" as over-inclusive) (citing Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997); Fair Hous. Council v. Roommates.com, L.L.C., 521 F.3d 1157, 1167 (9th Cir. 2008) ("It's true that the broadest sense of the term "develop" could include the functions of . . . just about any function performed by a website. But to read the term so broadly would defeat the purposes of [§] 230 by swallowing up every bit of the immunity that the section otherwise provides.")).

24. Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006).

25. Barrett v. Rosenthal, 5 Cal. Rptr. 3d 416, 420-21 (Ct. App. 2003) (identifying that the title of the allegedly defamatory messages contained the words "Slea[z]y 'Quackbuster' Scam"), *rev'd*, 146 P.3d 510 (Cal. 2006).

26. Barrett v. Rosenthal, 146 P.3d 510, 529 ("We conclude there is no basis for deriving a special meaning for the term 'user' in [§] 230(c)(1), or any operative distinction between 'active' and 'passive' Internet use. By declaring that no 'user' may be treated as a 'publisher' of third party content, Congress has comprehensively immunized republication by individual Internet users.").

27. *Id.*

28. Chi. Lawyers' Comm. for Civil Rights Under Law, Inc., v. Craigslist, Inc., 519 F.3d 666, 668 (7th Cir. 2008).

29. Chi. Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc., 461 F. Supp. 2d 661, 688 (N.D. Ill. 2006), *rev'd*, 519 F.3d 666 (7th Cir. 2008).

tantamount to identifying Craigslist as an information publisher, which the CDA barred.[30]

Additionally, in *Doe II v. Myspace, Inc.*, Myspace, a large social networking website, was immune from liability for the sexual assault of teenage girls who had met their assailants through the website.[31] The victims argued that Myspace was responsible for the assault because it should have implemented age verification software and maintained stricter privacy settings. The court ruled otherwise. Because the victims' claims were predicated on holding Myspace liable as a publisher of third-party content, the CDA barred their claims.[32] The *Myspace* ruling illustrates not only the level of immunity § 230 affords, but also the almost "wild west," jungle behavior the Act facilitates on the Internet.[33]

Recently, however, several cases illustrate a shift in accountability for websites whose users later become victims of sexual assault as a result of their use of the website. This shift is marked by the Ninth Circuit case, *Doe v. Internet Brands, Inc.*[34] In *Internet Brands*, an aspiring model created a

30. *Craigslist, Inc.*, 519 F.3d at 670 (quoting Doe v. GTE Corp., 347 F.3d 655, 659-60 (7th Cir. 2003).

31. Doe II v. Myspace, Inc., 96 Cal. Rptr. 3d 148, 156 (Ct. App. 2009).

32. *Id.* at 156-57.

33. In an attempt to do an "end-run" around the virtually unlimited protection against defamation actions offered by the CDA, a broad range of torts have been asserted against ISPs who host defamatory content. Most have been flatly defeated through the assertion of CDA immunity. *See, e.g.*, Herrick v. Grindr, L.L.C., 306 F. Supp. 3d. 579, 584 (S.D.N.Y. 2018) (finding the CDA barred a products liability claim and the plaintiff's claim that Grindr was required to "do more to remove impersonating profiles" because each claim required holding Grindr responsible "for the content created by one of its users"); Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 540 (E.D. Va. 2003) ("[G]iven that the purpose of § 230 is to shield service providers from legal responsibility for the statements of third parties, § 230 should not be read to permit claims that request only injunctive relief."); PatentWizard, Inc. v. Kinko's, Inc., 163 F. Supp. 2d. 1069, 1071-72 (D.S.D. 2001) (citing Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997)) (finding CDA immunity from defamation liability); Blumenthal v. Drudge, 992 F. Supp. 44, 52-53 (D.D.C. 1998) (barring defamation claims under the CDA for statements made in an on-line gossip column even though defendants had contracted for the reports, retained certain editorial rights as to its content, and aggressively promoted the reports); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 719 (Ct. App. 2002) (unfair competition claims found to be "inconsistent with and barred by [§] 230"); Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d. 772, 780, 781 (Ct. App. 2001) (citing Ben Ezra, Weinstein, & Co. v. Am. Online, Inc., 206 F.3d 980, 983-84 (10th Cir. 2000)) (barring state claims for misuse of public funds, nuisance, and premises liability as well as declaratory and injunctive relief); Doe v. Am. Online, Inc., 783 So. 2d 1010, 1018 (Fla. 2001) (concluding that the plain language of the CDA preempted "any actions" including a negligence action); Schneider v. Amazon.com, Inc., 31 P.3d 37, 39, 41 (Wash. Ct. App. 2001) (preempting claims for negligent misrepresentation, interference with business expectancy, and contractual liability under the CDA).

34. Doe v. Internet Brands, Inc., 767 F.3d 894 (9th Cir. 2014).

profile on the Model Mayhem website in hopes of procuring employment.[35] At the same time, two other users took advantage of Model Mayhem to further a rape scheme.[36] These individuals would contact female members, invite them to a fake audition, then drug and rape the victims.[37] The complaint alleged that Internet Brands, shortly after purchasing the website in 2008, learned of the illegal activities transpiring on the site and failed to warn its users of the danger.[38] Internet Brands sought to bar Doe's claim by asserting CDA immunity.[39] The court ruled, however, that this claim fell outside the scope of the CDA because Doe was not seeking to hold Internet Brands liable for its content. Rather, the plaintiff's claim sought liability for Internet Brands' "fail[ure] to warn her . . . about how third parties targeted and lured victims through Model Mayhem."[40] The court explained that a "failure to warn claim had nothing to do with Internet Brands' efforts, or lack thereof, to edit, monitor, or remove [content]. Thus, liability would not discourage the core policy of [§] 230(c)['s] 'Good Samaritan' filtering of third party content."[41] The court went further and distinguished this case from *Doe II v. Myspace, Inc.*, stating that "[t]he tort duty asserted here does not arise from an alleged failure to adequately regulate access to user content"

35. *Id.* at 895.

36. *Id.* at 895-96.

37. *Id.* at 896. Related to the concern of fake profiles and trolling was the New York State Senate Bill S5871A, which would have imposed harsher penalties to those who impersonate others via website or other electronic channels. Since this bill did not complete the legislative process by the time that the 114th Congress adjourned, it was not made into law and considered "dead." Dead bills can be reintroduced to a new Congress, usually with a new bill number. S5871A was reintroduced to the 115th Congress as New York State Senate Bill S2848, but again did not complete the legislative process by the time that Congress adjourned. This bill has yet to be reintroduced to the 116th Congress which is currently in session. The push for adoption of such laws was due in part to Meaghan Jarensky, who was impersonated on Match.com by an ex-lover of Jarensky's then boyfriend. Alison Leigh Cowan, *Fighting a Fake Dating Profile, Together*, N.Y. TIMES (Mar. 19, 2016), http://www.nytimes.com/2016/03/20/fashion/weddings/brett-barakett-meaghan-jarensky-marriage.html?_r=0. The profile caused a great deal of trouble for Jarensky in her personal and professional life. *Id.* She now uses her non-profit organization to press for adoption of similar laws in other states. *Id.* Growing concern regarding online trolling, shaming, and harassment has also sparked an increase in resources available for victims of online harassment. One such resource is called "Crash Override Network," a private NGO network of experts to help combat online harassment. *See* CRASH OVERRIDE NETWORK, http://www.crashoverridenetwork.com (last visited Oct. 7, 2018). Crash Override Network was founded by Zoe Quinn, a videogame developer, who was herself the victim of online abuse. *About the Network*, CRASH OVERRIDE NETWORK, http://www.crashoverridenetwork.com/about.html (last visited Oct. 7, 2018).

38. Doe v. Internet Brands, Inc., 767 F.3d 894, 896 (9th Cir. 2014).

39. *Id.*

40. *Id.* at 897-99.

41. *Id.* at 898.

or to monitor internal communications that might send up red flags about sexual predators.[42]

C. *The Future of Defamation Litigation*

Is there any way to succeed in litigation for online defamation? The quick answer is, not easily. The first issue is whether additional claims can be brought. In *Barnes v. Yahoo!, Inc.*, for example, the plaintiff sued her ex-boyfriend for creating fake personal pages impersonating the plaintiff.[43] Barnes immediately requested that Yahoo take the content down and alerted local news outlets of the story after she received an influx of emails and visits from men expecting sexual favors.[44] Yahoo, wishing to avoid public outcry over the incident, assured Barnes that they would take down the profile. Two months later, the profile remained and Barnes sued. To avoid § 230 preemption, Barnes argued that § 230 only relieved an ISP of liability for the publication of defamatory content, but that the Act did not remove responsibility for its eventual take down, especially once the ISP had been notified of the content's tortious nature.[45] Because Yahoo promised that it would remove the profile, Barnes successfully asserted a claim for promissory estoppel and thereby prevailed in a case that the CDA would have otherwise stymied.[46]

Considering the high barriers to successful defamation suits against ISPs, very few cases demonstrate what is required to lift § 230 immunity. One such case, however, is *Fair Housing Council v. Roommates.com, LLC.*[47] In this case, the court found Roommate.com liable for facilitating unlawful user content. The court distinguished Roommates.com from comparable sites, like Craigslist.org, because, unlike other sites which simply hosted user content, Roommates.com solicited its user's preferences on gender, race, and sexual orientation. Roommates.com then provided content based on such choices and concealed listings that did not conform to those preferences.[48]

---

42. *Id.* at 899 (citing Doe II v. MySpace, Inc., 96 Cal. Rptr. 3d 148 (Ct. App. 2009) (holding that the CDA bars tort claims based on a duty to restrict access to minors' MySpace profiles).

43. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).

44. *Id.* at 1098-99.

45. *Id.* at 1102.

46. *Id.* at 1109. However, don't expect ISPs to make this same "mistake" again.

47. Fair Hous. Council v. Roommates.com, L.L.C., 521 F.3d 1157 (9th Cir. 2008), *withdrawn and superseded by* Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016).

48. *Roommates.com, L.L.C.*, 521 F.3d at 1166; *see* Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 672 (7th Cir. 2008) ("But given § 230(c)(1) it

The court reasoned that such a "collaborative effort" between the website host and the individual poster better classified Roommates.com as a "content provider," rather than a "republisher," and therefore placed Roommates.com outside the protection offered under § 230.[49] While *Roommates.com* demonstrates that defamation lawsuits against ISP hosts are possible in cases where the provider affirmatively acts to create content, there are still substantial barriers which make it exceedingly difficult to proceed against Internet hosts in defamation and privacy cases.

Content providers going beyond traditional editorial functions are less likely to receive CDA immunity. *Fraley v. Facebook, Inc.*, in which Facebook generated commercial endorsements for companies "liked" by their members utilizing members' likenesses, illustrates this point.[50] The court in *Fraley* rejected Facebook's CDA immunity claim, rationalizing that Facebook went beyond traditional editorial functions by "transform[ing] the character" of member submissions into endorsements without their members' consent.[51] Similarly, in *Perkins v. LinkedIn Corp.*, the court rejected LinkedIn's CDA immunity defense where the plaintiffs alleged that LinkedIn created and developed the content of the reminder email, arranged the plaintiffs' names and likenesses in those emails to give the impression that the plaintiffs were endorsing LinkedIn, and offered no opportunity for the plaintiffs to edit those emails.[52]

III. THE NEED FOR INTERVENTION BY THE UNITED STATES SUPREME COURT

The one hope that could alter the bleak picture above is intervention by the Supreme Court of the United States. If the Supreme Court, led by Justices who believe in fidelity to the statutory text they are interpreting, were to take a fresh look at *Zeran* and its progeny, it could effectively reboot and restart all of § 230, starting the interpretation over in alignment with what Congress wrote and intended. § 230, as it is widely applied by courts today, is a creature of judicial invention, untenably divorced from its intended function.

The sweeping immunity that courts have bestowed on Internet service providers cannot be squared with the plain meaning of the statutory text, with the antecedent common law doctrines and judicial decisions that informed

---

cannot sue the messenger just because the message reveals a third party's plan to engage in unlawful discrimination.").

49. *Roommates.com, L.L.C.*, 521 F.3d at 1167.

50. Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 790 (N.D. Cal. 2011).

51. *Id.* at 802.

52. Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1222, 1249 (N.D. Cal. 2014).

the enactment of the statute, with the statute's legislative history, or within any plausible common-sense understanding of the public policy objectives Congress sought to achieve. The U.S. Supreme Court has not yet interpreted § 230. Until the Supreme Court does finally and authoritatively rule, it remains within the right and duty of state and federal courts to continue the ongoing debate over what Congress truly intended when it passed the statute. Until it has been decided correctly, it has not been decided. Acceptance of review by the U.S. Supreme Court would permit the Court to begin with a return to the basics.

The title of § 230 signals its animating purpose: "Protection for private blocking and screening of offensive material."[53] Subsections (a) and (b) contain a list of findings and policy objectives, which, in combination, reflect a congressional intent to balance "the vibrant and competitive free market that presently exists for the Internet"[54] against the congressional purpose "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[55] The operative provision of the statute, subsection (c), contains a subtitle that further illuminates the congressional purpose: "Protection for "Good Samaritan" blocking and screening of offensive material."[56] Subsection (c) provides in its entirety:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent,

53. Communications Decency Act of 1996, Pub. L. No. 115-164, sec. 4, § 230(e), 132 Stat. 1253, 1254-55 (clarifying that § 230 does not affect crime enforcement of prohibited behavior, specifically "providers and users of interactive computer services of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking and for other purposes").

54. 47 U.S.C. § 230(b)(2).

55. 47 U.S.C. § 230(b)(4).

56. 47 U.S.C. § 230(c).

> harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[57]

Aside from subsection (c), the only other salient language in the statute resides in two statutory definitions. The statute defines the term "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[58] The statute defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[59]

On its face, and considering its captions, the operative language and definitions, § 230 provides ISP who take affirmative steps to screen and block third party content that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" a defense from liability.[60] § 230 does not, however, explicitly create universal ISP immunity for the content of third parties. A more modest reading of the statutory text is permissible because such reading harmonizes the captions, operative language and definitions of the Act, considered in its entirety. This point was well made by Judge Frank Easterbrook in an opinion for the United States Court of Appeals for the Seventh Circuit:

> [§] 230(c)(2) tackles this problem not with a sword but with a safety net. A web host that does filter out offensive material is not liable to the censored customer. Removing the risk of civil liability may induce web hosts and other informational intermediaries to take more care to protect the privacy and sensibilities of third parties. The district court held that subsection

57. *Id.*

58. 47 U.S.C. § 230(f)(2) ("The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.").

59. 47 U.S.C. § 230(f)(3) ("The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.").

60. The Communications Act states "[n]o provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected[.]" 47 U.S.C. § 230(c)(2)(A).

> (c)(1), though phrased as a definition rather than as an immunity, also blocks civil liability when web hosts and other [ISPs] refrain from filtering or censoring the information on their sites[.]
>
> If this reading is sound, then § 230(c) as a whole makes ISPs indifferent to the content of information they host or transmit: whether they do (subsection (c)(2)) or do not (subsection (c)(1)) take precautions, there is no liability under either state or federal law. As precautions are costly, not only in direct outlay but also in lost revenue from the filtered customers, ISPs may be expected to take the do nothing option and enjoy immunity under § 230(c)(1). Yet § 230(c)—which is, recall, part of the 'Communications Decency Act'—bears the title 'Protection for 'Good Samaritan' blocking and screening of offensive material,' hardly an apt description if its principal effect is to induce ISPs to do nothing about the distribution of indecent and offensive materials via their services. Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?[61]

Judge Easterbrook continued, stating:

> True, a statute's caption must yield to its text when the two conflict, but *whether* there is a conflict is the question on the table. Why not read § 230(c)(1) as a definitional clause rather than as an immunity from liability, and thus harmonize the text with the caption? On this reading, an entity would remain a 'provider or user'—and thus be eligible for the immunity under § 230(c)(2)—as long as the information came from someone else; but it would become a 'publisher or speaker' and lose the benefit of § 230(c)(2) if it created the objectionable information. The difference between this reading and the district court's is that § 230(c)(2) never requires ISPs to filter offensive content, and thus § 230(e)(3) would not preempt state laws or common-law doctrines that induce or require ISPs to protect the interests of third parties, such as the spied-on plaintiffs, for such laws would not be 'inconsistent with' this understanding of § 230(c)(1).[62]

---

61. Doe v. GTE Corp., 347 F.3d 655, 659-60 (7th Cir. 2003) (citing Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997); Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980 (10th Cir. 2000); Green v. Am. Online, Inc., 318 F.3d 465 (3d Cir. 2003); Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003)).

62. *Id.* at 660 (first citing Trainmen v. Baltimore & Ohio R.R., 331 U.S. 519, 528-29 (1947); and then citing Carlisle I v. United States, 517 U.S. 416, 421 (1996)). *Compare* Doe v. GTE Corp., 347 F.3d 655, 659-60 (7th Cir. 2003); *with* City of Chicago v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010) ("Subsection (c)'s caption, 'Protection for 'Good Samaritan' blocking and screening of offensive material" bodes even less well for StubHub! . . . . As earlier decisions in this circuit establish, subsection (c)(1) does not create an "immunity" of any kind.") (citing *GTE Corp.*, 347 F.3d at 660; and Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008)).

The Seventh Circuit does not stand alone in its § 230 assessment. The Ninth Circuit expressed similar willingness to accept a more narrow construction of § 230 in 2003.[63]

The context surrounding enactment § 230 could not be more straightforward. Congress passed the statute in reaction to the evolution of common law doctrines defining when a person or entity is deemed "a publisher or speaker" as those doctrines were beginning to be applied in the early days of the Internet. Congress saw that the common law might evolve to create disincentives that would discourage Internet service providers from doing the right thing, affirmatively seeking to screen and block offensive content posted on Internet sites by third parties.

The legislative history of § 230 soundly buttresses this interpretation. The key legislative committee report on the bill explained:

> This section provides 'Good Samaritan' protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material. One of the specific purposes of this section 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. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.[64]

Senator Coats, one of the two main authors of the CDA, made clear while discussing § 230 that its intention was to prevent ISPs that try to keep offensive material off the Internet "from being held liable as a publisher for defamatory statements for which they would not otherwise have been liable."[65] § 230, understood against this backdrop, was indeed nothing more

---

63. Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003); *see* Doe v. Internet Brands, Inc., 824 F.3d 846, 851-52 (9th Cir. 2016) ("As the heading to [§] 230(c) indicates, the purpose of that section is to provide '[p]rotection for 'Good Samaritan' blocking and screening of offensive material.' That means a website should be able to act as a 'Good Samaritan' to self-regulate offensive third party content without fear of liability."); Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008) ("§ 230 (c)(1) provides 'broad immunity from liability for unlawful third-party content.' That view has support in other circuits") (citing Univ. Comm'n Systems, Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007); Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003); Green v. Am. Online, Inc., 318 F.3d 465 (3d Cir. 2003); Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980 (10th Cir. 2000); and Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997)).

64. THOMAS BLILEY, TELECOMMUNICATIONS ACT OF 1996, H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 124, 199-200.

65. 141 CONG. REC. S8293, S8345 (daily ed. June 14, 1995) (statement of Sen. Coats); *see* Batzel v. Smith, 333 F.3d 1018, 1029 (9th Cir. 2003) (restating Congress's concerns that "[i]f efforts

nor less than the caption "Good Samaritan" implies. Internet service providers who function as "Good Samaritans," acting laudably to delete offensive material harmful to others from their websites, are not to be treated as responsible for offensive material merely because they take make such laudable efforts. § 230 must thus be read as a modest congressional elaboration on the common law, most particularly, the common law of defamation:

> The common law of libel distinguishes between liability as a primary publisher and liability as a distributor. A primary publisher, such as an author or a publishing company, is presumed to know the content of the published material, has the ability to control the content of the publication, and therefore generally is held liable for a defamatory statement, provided that constitutional requirements imposed by the First Amendment are satisfied . . . . A distributor, such as a book seller, news vendor, or library, may or may not know the content of the published matter and therefore can be held liable only if the distributor knew or had reason to know that the material was defamatory.[66]

As the court in *Grace v. eBay, Inc.* originally and correctly held, § 230 speaks only to "publisher or speaker" liability, but leaves untouched liability predicated on an ISP's status as a distributor or transmitter, with its concomitant higher standard of notice and culpability.[67]

While *Zeran* spawned many offspring, these cases are no more legitimate than *Zeran* itself. *Zeran* wrenched § 230 from its common law antecedents and legislative history. *Zeran* focused exclusively on one sentence of § 230, the naked statement in § 230(c)(1) that Internet service providers are not to be "be treated as the publisher or speaker of any information provided by another information content provider," as if this stood alone as the *sole* load-bearing declaration giving meaning to the statute.[68] *Zeran* improperly failed to read this language in the context of the

---

to review and omit third-party defamatory, obscene or inappropriate material make a computer service provider or user liable for posted speech, then website operators and Internet service providers are likely to abandon efforts to eliminate such material from their site") (first citing S. REP. NO. 104-230, at 194 (1996), H.R. CONG. REP. NO. 104-458, at 194 (1996), 141 CONG. REC., at H84691-70 (statement of Rep. Cox), and then citing Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997)).

66. Grace v. eBay, Inc., 16 Cal. Rptr. 3d 192, 198-99 (Ct. App. 2004), *opinion superseded by* Grace v. eBay, Inc., 99 P.3d 2 (Cal. 2004), *and appeal dismissed*, Grace v. eBay, Inc., 101 P.3d 509 (Cal. 2004) (internal citations omitted).

67. *Id.* at 197-99.

68. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (quoting 47 U.S.C. § 230(c)(1)).

captions and other operative provisions of § 230. That context would have harmonized the passage with the entirety of the statute, rendering it merely "definitional," thereby connecting the overall meaning of § 230 to the modest adjustment of the common law that Congress manifestly intended.

The time has come to unequivocally reject *Zeran*. The analysis in *Zeran* proves too much, leading inexorably to results that stretch far beyond anything Congress could have remotely intended. It was never Congress's intent to make the law of the land the law of the jungle: "[T]he Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[69] In addition, "Congress has not provided an all-purpose get-out-of-jail-free card for businesses that publish user content on the Internet, though any claims might have a marginal chilling effect on Internet publishing businesses."[70]

Zeran supplied an overly-broad interpretation of § 230 based on the court's fear that the Internet was a sort of fragile newborn of precarious health and in need of extraordinary paternalistic support from government to keep it alive. That fear, exaggerated even in its time, has long since proved unfounded. The Internet in general, and social media platforms in particular, have assumed dominating influence and power in society. What is needed *today* is a sensible construction of § 230 that does not empower Internet platforms carte blanche to operate in derogation of other societal entities, who are bound by the rule of law, or competing societal values, such as protection of individual privacy, reputation, and dignity. As the Ninth Circuit observed:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.[71]

The court in *Grace* got it right in declaring its disagreement "with the *Zeran* court's conclusion that for providers and users of interactive computer services to be subject to distributor liability would defeat the purposes of the

69. Fair Hous. Council v. Roommates.com, L.L.C., 521 F.3d 1157, 1164 (9th Cir. 2008).

70. Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016).

71. *Roommates.com, L.L.C.*, 521 F.3d at 1164 n.15.

statute and therefore could not be what Congress intended."[72] In fact, *Zeran* calibrated the incentives all backwards when weighed against what Congress clearly sought to accomplish. The *Grace* court explained that the "broad immunity provided under *Zeran* . . . would eliminate potential liability for providers and users even if they made no effort to control objectionable content, and therefore would neither promote the development of technologies to accomplish that task nor remove disincentives to that development as Congress intended."[73] *Zeran* instead operates to "eliminate a potential incentive to the development of those technologies, that incentive being the threat of distributor liability."[74]

The Supreme Court of the United States will not lack for opportunities to finally accept review in a § 230 case. Decisions invoking extreme interpretations of § 230 proliferate. In July 2018, for example, the California Supreme Court, in a three-justice plurality opinion written by Chief Justice Cantil-Sakauye and joined by Justices Chin and Corrigan, adopted a sweeping interpretation of § 230, holding that the Internet review site Yelp could not be forced to abide by a court order emanating from a defamation case in which Yelp was not even a party, ordering a defendant to take down a defamatory review. The case, *Hassell v. Bird*,[75] arose from a defamation action brought by a lawyer, Dawn Hassel, against a former client, Ava Bird. The basis for this action stemmed from an Internet review Bird posted of Hassell after Bird terminated Hassell's representation in a personal injury matter. Hassell alleged that Bird's review contained false defamatory statements of fact. After repeated efforts to engage Bird in the litigation, a California trial court entered a default judgment against Bird.[76] The default judgment, entered only after a "prove up" hearing in which Hassell established the predicate for liability, included a money damages award and an injunction against Bird ordering her to take down the offending Yelp posts

72. Grace v. eBay, Inc., 16 Cal. Rptr. 3d 192, 201 (Ct. App. 2004), *review granted and opinion superseded*, Grace v. eBay, Inc., 99 P.3d 2 (Cal. 2004), *review dismissed*, Grace v. eBay, Inc., 101 P.3d 509 (Cal. 2004).

73. *Id.*

74. *Id.* (first citing Sewali K. Patel, Note, *Immunizing Internet Service Providers from Third-Party Internet Defamations Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 683-85 (2002); and then citing Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 616-23 (2001)).

75. Hassell v. Bird, 420 P.3d 776 (Cal. 2018), *cert. denied sub nom.* Hassell v. Yelp, Inc., No. 18-506, 2019 WL 271967, at *1 (U.S. Jan. 22, 2019).

76. *Id.* at 778.

containing the defamatory falsehoods.[77] The court also ordered Yelp to remove the reviews.[78]

Yelp contested the order to remove, arguing that it could not be bound by an injunction in a case in which it was not an underlying party, and arguing that § 230 conferred upon Yelp immunity from the order to take down the material.[79] The plurality opinion of Chief Justice Cantil-Sakauye, relying on the broad immunity other courts had conferred under *Zeran* and its progeny, held that § 230 immunized Yelp.[80] A concurring opinion by Justice Kruger took a narrower view of § 230, but agreed with the plurality that § 230 precluded application of the injunction against Yelp:

> The injunction of course recognizes that Yelp is—as a matter of fact—the publisher of Bird's reviews; the reviews cannot come down without Yelp's cooperation. But that is not the pertinent question. The question is instead whether the injunction necessarily holds Yelp legally responsible for, or otherwise authorizes litigation against Yelp solely because of, its editorial choices. As the case comes to us, I agree with the plurality opinion that the answer to that question is yes.[81]

In a blistering dissent by Justice Cuellar, joined by Justice Stewart, Justice Cuellar attacked all aspects of the sweeping interpretation that § 230 has acquired. Justice Cuellar's opinion provides the perfect roadmap for review by the U.S. Supreme Court. As Justice Cuellar explained, it is as if the immunities courts have found in § 230 were written in invisible ink.[82] Justice Cuellar attacked the plurality's narrow ruling that the immunity

---

77. *Id.* at 780-81.

78. *Id.* at 781.

79. *Id.*

80. *Id.* at 788, 793.

81. *Id.* at 801 (Kruger, J., concurring).

82. 82.Justice Cuellar, dissenting, stated that:

> By its terms, [§] 230 conspicuously avoids conferring complete immunity from all legal proceedings. Its language expressly permits the enforcement of certain federal criminal laws as well as state laws consistent with the section. (§ 230(e)) In the context of state law, the [§] 230 only prohibits causes of action from being brought and liability from being imposed under state laws that are inconsistent with the section. (§ 230(e)(3)) From the statute's terms, an inconsistent state law is one in conflict with the terms in [§] 230(c). An inconsistent state law under [§] 230(c)(1) is a state law cause of action or liability that treats an interactive computer service as the publisher or speaker of information provided by another information content provider. And an inconsistent state law under [§] 230(c)(2) is a state law cause of action that seeks to hold an interactive service provider liable for voluntary actions taken in good faith to restrict access to obscene, lewd, harassing, or otherwise objectionable material. If [§] 230 conferred complete immunity on an interactive service provider, as the plurality opinion implies, then lurking somewhere in the statute one would need to find an enormously consequential codicil of categorical absolution written in invisible ink to preempt the statute's more nuanced scheme. There's no such codicil. Nor does Yelp even face 'liability' here at all.

Id. at 810-11 (Cuellar, J., dissenting).

recognized in *Zeran* was meant to immunize Yelp from the take down in the case before the California Supreme Court given that Yelp was in no serious sense being held responsible for "tort liability" arising from content posted by others.[83]

Far more significantly, however, Justice Cuellar's opinion cut at the very roots of *Zeran*. "Our society's legal commitments balance the value of free expression and a relatively unregulated Internet against the harms arising from damaging words or private images that people are not lawfully free to disseminate,"[84] he wrote. In passing § 230, Congress did not intend for the Internet to be the wild, wild west – a place with no respect for the rule of law: "To the extent the Communications Decency Act merits its name, it is because it was not meant to be—and it is not—a reckless declaration of the independence of cyberspace."[85] Yet until the U.S. Supreme Court intervenes, it appears that state and federal courts will likely continue to apply § 230 in manner that largely does render cyberspace a lawless space.[86]

---

83. *Id.* at 812 (Cuellar, J., dissenting).

> All of which underscores why it is a contrast between apples and oranges—or apples and Oreos, for that matter—to compare a defendant's explicit targeting by a civil lawsuit with a person or entity's remedial responsibility to avoid helping others engage in prohibited conduct. A defendant to a state law cause of action may be subject to an adverse judgment triggering a responsibility to provide monetary or equitable relief to the plaintiff, and may incur litigation expenses to defend itself. In contrast, an entity that has not been sued is required only to refrain from engaging in prohibited actions. Yelp has not been sued, and its only responsibility in light of the judgment and injunction against Bird is to avoid violating that court order. [§] 230 does not extend protection to a provider or user who violates an injunction by instead promoting third party speech that has been deemed unlawful by a California court. Yelp has an obligation not to violate or assist in circumventing the injunction against Bird, but that does not impose a legal obligation upon Yelp that treats it as a publisher or speaker of third party content.

Id.

84. *Id.* at 824 (Cuellar, J., dissenting).

85. *Id.* (Cuellar, J., dissenting).

86. *Id.* at 824-25 (Cuellar, J., dissenting).

> Nothing in [§] 230 allows Yelp to ignore a properly issued court order meant to stop the spread of defamatory or otherwise harmful information on the Internet. Instead the statute's terms and scheme, applicable case law, and other indicia of statutory purpose make clear that Internet platforms are not exempt from compliance with state court orders where no cause of action is filed against, and no civil liability is imposed on, the provider for its publication of third party speech. Yelp may be subject to a properly issued injunction from a California court. Where an entity had the extensive notice and considerable involvement in litigation that Yelp has had in this case, due process concerns are far less likely to impede a court from fashioning a proper injunction to prevent aiding and abetting of unlawful conduct. But whether Yelp aided, abetted, or otherwise acted sufficiently in concert with or colluded to advance Bird's defamatory conduct must be addressed using the proper legal standard for an injunction to run to a nonparty, as we explained in Berger and Ross. Because we cannot establish that the superior court made the necessary factual findings regarding Yelp's conduct in this situation, applying

A. *Anonymity*

Aside from § 230 preemption, however, there are many other legal hurdles plaintiffs face in defamation litigation. Consider poster anonymity. Although the law allows victims to sue the poster in place of the ISP, this is not always feasible given that the poster may be seriously imbalanced mentally, a sociopath, psychotic, broke, anonymous, and/or can't be physically located. This problem is further complicated because protections to maintain poster anonymity are strong in the U.S. such that requests to subpoena an anonymous poster's identity are often denied.

Dendrite International, Inc. v. Doe exemplifies this trend. In *Dendrite International*, a company attempted to compel an ISP to reveal the identity of "Doe No. 3" for posting defamatory comments and trade secrets on a message board.[87] Although the court allowed Dendrite to conduct limited discovery to uncover the identities of the anonymous posters involved, it rejected a motion to compel Yahoo to identify the remaining defendant, Doe No. 3.[88] In delivering its opinion, the court established a five-prong test to determine whether an entity may be granted a motion to compel: there must be a showing that (1) the plaintiff made efforts to notify the anonymous poster and allowed a reasonable time for him/her to respond; (2) the plaintiff identified the exact statements made by the poster; (3) the complaint set forth a prima facie cause of action; (4) there was sufficient evidence for each element of its claim; and (5) the court balanced the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented.[89]

Doe v. Cahill used some of the prongs of the *Dendrite* test to formulate a "summary judgment" standard.[90] In *Cahill*, local politician, Patrick Cahill, sued for defamatory comments posted about him on a blog and subpoenaed Comcast to uncover the identity of the poster.[91] After receiving notice of the subpoena, the anonymous poster filed a protective order to prevent the disclosure of his or her identity. The Delaware Supreme Court determined that because the defamatory comments were "incapable of a defamatory

---

a legal standard consistent with the views expressed in this opinion, we would vacate the judgment of the Court of Appeal and remand for further proceedings not inconsistent with this opinion.

Id.

87. Dendrite Int'l, Inc. v. Doe, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

88. *Id.*

89. *Id.* at 760-61.

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

91. *Id.* at 454.

meaning," the case did not pass the summary judgment test required to compel Comcast to comply with the subpoena, and thus the poster's identity was kept anonymous.[92]

B. *Jurisdictional Barriers*

Another issue is jurisdiction. Often, defamatory material is posted online in one state which directly affects individuals of another state. To deal with such cases, the courts have deferred to the "Calder effects test" established in *Calder v. Jones*.[93] As applied to cases of Internet defamation, the court must find a "purposeful direction" or showing that the publication was an intentional act that was expressly aimed at the forum state, and with knowledge that the force of the publication would be felt in the forum state.[94] If purposeful direction is met, the courts are willing to grant jurisdiction in cases that may have otherwise been barred by failure to meet minimal contacts requirement or establish requisite levels of interactivity. The use of this standard reflects a general loosening of requirements to establish personal jurisdiction such that plaintiffs only need to establish that statements were directed at the forum state.[95]

C. *International Litigation and Libel Tourism*

The problems with defamation litigation in the U.S. are especially striking when compared to libel laws around the world. The U.K., for example, particularly England, has had more liberal libel laws which make success in defamation lawsuits much more feasible. However, intense pressure from the U.S. and U.K. publishing industries complaining about the growth of "libel tourism" (which, incidentally, is not supported by the actual

92. *Id.* at 467.

93. Calder v. Jones, 465 U.S. 783 (1984).

94. *Id.* at 790 (finding that the acts by the petitioners was not mere negligence, but instead "intentional, and allegedly tortious, actions [which] were expressly aimed at California," thus they were awarded no protection).

95. Several recent lawsuits support this trend. *See, e.g.*, CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1077 (9th Cir. 2011) ("The 'effects' test, which derives from the Supreme Court's decision in Calder . . . requires that 'the defendant allegedly must have (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state.'") (quoting Brayton Purcell, L.L.P. v. Recordon & Recordon, 606 F.3d 1124, 1128 (9th Cir. 2010)); Mavrix Photo, Inc. v. Brand Techs., Inc., 647 F.3d 1218, 1228 (9th Cir. 2011) (quoting Brayton Purcell, L.L.P. v. Recordon & Recordon, 606 F.3d 1124, 1128 (9th Cir. 2010)); Silver v. Brown, 382 Fed. Appx. 723 (10th Cir. 2010).

statistics)[96] led to introduction of the 2013 U.K. Defamation Act (except Northern Ireland).[97] The U.K. is now subject to a single publication rule, similar to that exemplified by California Civil Code §§ 3425.1 to 3425.5.[98] The California code states that any mass publication of information constitutes one single communication and thus allows for only one cause of action for libel. Additionally, the statute of limitations begins to run as soon as the statements are published.[99]

Substantively, U.S. law diverges from U.K. law in that the U.S. assumes defamatory statements are true, while the U.K. presumes that they are false.[100] Thus, if an individual brings a claim for defamation in the U.K., it becomes the defendant's burden to prove that the libelous statements were true. Not only are libel defendants required to prove the "substantial truth of every material fact," failure to do so may result in an aggravated damages judgment.[101] This contrasts with the U.S. law, where defendants, especially media defendants, are strongly shielded from potential litigation. In libel cases brought by public officials or public figures on matters of public concern, U.S. courts require proof that a defendant acted with actual malice.[102] Because the courts have not clearly defined how much evidence is sufficient in proving this burden, most look to evidence showing that the publisher specifically knew the statement was false.[103] This is often

96. *Libel Tourism is a Very Rare Thing in UK Courts, Finds Study*, OUT-LAW.COM, https://www.out-law.com/page-11343 (last visited Sept. 12, 2018); *Number of Defamation Cases Falls by a Third in a Year*, THOMSON REUTERS (Nov. 16, 2015), https://inforrm.files.wordpress.com/2015/09/thomson-reuters-press-release.pdf (showing a twenty-seven percent decrease in the number of defamation cases overall from 2013/2014 to 2014/2015).

97. Defamation Act 2013, c. 26, § 8 (Eng.).

98. CAL. CIV. CODE §§3425.1-3425.5 (Deering 2018).

99. *Id.* § 3425.3.

100. *See* HARRY MELKONIAN, DEFAMATION, LIBEL TOURISM, AND THE SPEECH ACT OF 2010, at 2 (2011).

101. Raymond W. Beauchamp, Note, *England's Chilling Forecast: The Case for Granting Declaratory Relief to Prevent English Defamation Actions from Chilling American Speech*, 74 FORDHAM L. REV. 3073, 3078 (2006) (citing Maureen Mulholland, *Defamation*, *in* CLERK & LINDSELL ON TORTS 22, 22-81 (Anthony M. Dugdale ed., 18th ed. 2000)); Sarah Staveley-O'Carroll, Note, *Libel Tourism Laws: Spoiling the Holiday and Saving the First Amendment?*, 4 N.Y.U.J.L. & LIBERTY 252, 256, 257 (2009) (citing Hearing on H.R. 6146 Before the Subcomm. on Commercial and Administrative Law of the H. Comm. on the Judiciary, 111th Cong. 3 (2009) (written statement of Laura R. Handman, Partner, Davis Wright Tremaine LLP)).

102. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 283 (1964) (establishing the "actual malice" standard when a defamation suit is brought regarding public officials on matters relating to their performance or fitness for office).

103. Thomas Sanchez, Note, *London, Libel Capital No Longer?: The Draft Defamation Act of 2011 and the Future of Libel Tourism*, 9 U.N.H.L. REV. 469, 486 (2011) (citing Murphy v. Boston Herald, Inc., 865 N.E.2d 746, 752-53 (Mass. 2007); and MELKONIAN, *supra* note 100, at 24)).

impossible to prove, however, because such evidence is very difficult to obtain. Since plaintiffs can almost never meet this burden of proof, most media defendants in the U.S. are strongly safeguarded against liability for defamation.[104]

Yet, even if litigation overseas appears more promising, there is a serious question as to whether the U.S. will enforce a foreign judgment. Dr. Rachel Ehrenfeld famously tested the waters on this issue when she sued Saudi billionaire, Khalid bin Mahfouz, in U.S. Federal Court to prevent enforcement of a foreign libel ruling against her book, *Funding Evil*.[105] The book made a number of allegations about the Mahfouz family's involvement in international terrorist networks, including that the family personally financed these groups.[106] In the countersuit, Dr. Ehrenfeld argued that Mahfouz's litigation infringed upon her First Amendment rights and had a chilling effect on otherwise valuable journalism.[107] Although she eventually took the case to the New York Court of Appeal, the lawsuit was dismissed for lack of jurisdiction over Mr. Mahfouz.[108] After the lobby of Dr. Ehrenfeld and the media, several state legislatures responded by passing laws to prevent the enforcement of foreign defamation judgments. States that began to adopt such libel tourism laws include California, Florida, Illinois and New York.[109]

Federal legislation was also passed in August of 2010. The SPEECH Act,[110] as it is known, effectively bars the enforcement of foreign defamation judgments unless they meet First Amendment standards.[111] Of course, the

104. The standard in most American states for suits brought by private figure plaintiffs on matters of public concern is negligence. *Id.* at 484-85 n.84 (quoting RESTATEMENT (SECOND) OF TORTS § 558 (AM. LAW INST. 1977)).

105. *See* Ehrenfeld v. Bin Mahfouz, 881 N.E.2d 830, 832-33 (N.Y. 2007) (explaining that, in 2004, the English court had entered a default judgment against Ehrenfeld and publisher Bonus Books which provided an award of damages and an injunction prohibiting further publication of the allegedly defamatory statements in England and Wales); Bin Mahfouz & Ors v. Ehrenfeld, [2005] EWHC 1156 (QB).

106. RACHEL EHRENFELD, FUNDING EVIL 35-36 (expanded ed. 2005) (2003).

107. *See* Ehrenfeld v. Mahfouz, 489 F.3d 542, 550 (2d Cir. 2004).

108. *Ehrenfeld*, 881 N.E.2d at 833. This decision by the New York Court of Appeal was later affirmed by the Second Circuit in Ehrenfeld v. Mahfouz, 518 F.3d 102 (2d Cir. 2008).

109. See codes in California (CAL. CIV. PROC. CODE §§ 1716, 1717 (Deering 2018)); Florida (FLA. STAT. §§ 55.605 (2)(h); 55.6055 (Deering 2018)); Illinois ((735 ILL. COMP. STAT. 5/2-209(b-5); 5/12-621 (b)(7) (repealed 2012) (Deering 2012)); and New York (N.Y. C.P.L.R. §§ 302(d); 5304 (b)(8) (McKinney 2008)).

110. Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act of 2010, 28 U.S.C. §§ 4101-4105 (2012).

111. 28 U.S.C. § 4102(a)(1)(A)-(B).

reality is that there have been very few, if any, attempts to enforce U.K. libel judgments in the U.S., primarily on account of the stance taken by the courts here that they would only enforce a judgment that could otherwise have been obtained within the jurisdiction of that particular state. Accordingly, the SPEECH Act probably has more of a symbolic impact rather than an actual effect on international libel laws, although it does send out a fairly unsubtle warning to Americans that they should not seek to undermine First Amendment rights in overseas courts.

Nonetheless, U.S. citizens can still take legal action against U.K. and other European publications in the British courts without fear of reprisals back home. Indeed, citizens failing to avail themselves of the more favorable U.K. libel laws could create an adverse inference among the public to the effect that they must be guilty of the allegations being made against them; otherwise, they would have litigated immediately like their U.K. counterparts! The successful lobbying campaign undertaken in the U.S. (some would say that it has been the most effective since that undertaken by the tobacco industry several decades ago),[112] has directly impacted the thinking of U.K. legislators. It contributed, in no small measure, to the introduction of the English Defamation Act, which aims to make "libel tourists" suits more difficult to bring in the High Court of London. The Defamation Act makes such suits more difficult by imposing stricter criteria that requires a claimant to demonstrate not only their close connections with

---

> [A] domestic court shall not recognize or enforce a foreign judgment for defamation unless the domestic court determines that– (A) the defamation law applied in the foreign court's adjudication 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; or (B) even if the defamation law applied in the foreign court's adjudication did not provide as much protection for freedom of speech and press as the first amendment to the Constitution of the United States and the constitution and law of the State, 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 of the United States and the constitution and law of the State in which the domestic court is located..

Id.

112. For example, Facebook spent almost $10 million in 2015 on lobbying, while Google spent $5.5 million in only the first three months of 2015. *Lobbyists Representing Facebook Inc., 2015*, OPENSECRETS.ORG, https://www.opensecrets.org/lobby/clientlbs.php?id=D000033563&year=2015 (last visited Oct. 29, 2018); *see* Diane Bartz, *Google Lobbying Spending Reached New High in Early 2015*, REUTERS (Apr. 21, 2015, 9:00 AM), http://www.reuters.com/article/us-google-lobbying-idUSKBN0NC1UO20150421.

the U.K., but also that the U.K. is the most appropriate forum to bring the claim.[113]

Furthermore, although leaving the burden of proof firmly on a publisher's shoulders, a "serious and substantial" harm test was introduced, thereby raising the bar for those who might otherwise have desired to sue for what the Court would regard as more trivial claims. U.K. legislation has also removed the automatic right to jury trial, with the intention being to both limit the number of claims coming before the Courts and the level of damages being awarded by juries. However, this legislation has not been introduced in Northern Ireland, which, along with the Republic of Ireland, remains a "plaintiff friendly" jurisdiction.

D. *Anti-SLAPP Statutes*

Meeting First Amendment standards is not the only essential hurdles in foreign libel pleadings; there are also anti-SLAPP motions. Especially in California, anti-SLAPP statutes present a serious problem to plaintiffs considering litigation for defamation in connection with public issues. This is because Code of Civil Procedure section 425.16 allows defendants to file a motion to dismiss a complaint entirely, provided that the defendant show that their activity fell within the rights of petition or free speech. Once this has been done successfully, the burden then shifts to the plaintiff to show that they have a reasonable probability of prevailing in the action.[114] Should the plaintiff fail to meet this burden, the defendant is entitled to both attorney's fees and court costs.[115]

---

113. Defamation Act 2013, c. 26, § 9(2) (Eng.). The Act states:

> A court does not have jurisdiction to hear and determine an action to which this section applies unless this court is satisfied that, of all the places in which the statement complained of has been published, England and Wales is clearly the most appropriate place in which to bring an action in respect to the statement.

Id.

114. CAL. CIV. PROC. CODE § 425.16(b)(1) (Deering 2018) ("A cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue shall be subject to a special motion to strike, unless the court determines that the plaintiff has established that there is a probability that the plaintiff will prevail on the claim.").

115. *Id.* § 425.16(c)(1) ("Except as provided in paragraph (2), in any action subject to subdivision (b), a prevailing defendant on a special motion to strike shall be entitled to recover his or her attorney's fees and costs.").

Moreover, pursuant to section 425.16(g) once a motion for anti-SLAPP is filed, discovery is stayed unless the courts grant permission.[116] Thus, anti-SLAPP statutes become a powerful tool to not only dissuade individuals from bringing forth legitimate claims for defamation, but also effectively punishes them for doing so by making litigation extremely costly and difficult.

Global Telemedia International, Inc. v. Doe provides insight into the implications of California's anti-SLAPP legislation.[117] There, Global Telemedia attempted to sue posters to an online bulletin board for defamation with regards to negative comments posted about the firm and its officers. The defendants successfully argued an anti-SLAPP defense on the grounds that statements regarding a publicly traded company constituted speech about public issues and were therefore protected.[118] Because the plaintiffs had not shown a probability of success on their claims for defamation, the case was dismissed and Global Telemedia was not able to seek damages for its alleged harms.[119]

IV. WHAT CAN BE DONE?

In light of the problems with current litigation on defamation, including § 230 of the CDA, jurisdictional issues, and anti-SLAPP statutes, recourse is obviously exceedingly difficult. While some remedies are available to defamation victims, most plaintiffs are left at the mercy of the particular ISP they are dealing with to take down the content.[120]

Among the most common options for plaintiffs are to sue the poster directly, to seek injunctive relief and take down the offensive post, and to sue for damages and obtain ownership of the defamatory websites. Some ISPs

116. *Id.* § 425.16(g) ("All discovery proceedings in the action shall be stayed upon the filing of a notice of motion made pursuant to this section. The stay of discovery shall remain in effect until notice of entry of the order ruling on the motion. The court, on noticed motion and for good cause shown, may order that specified discovery be conducted notwithstanding this subdivision."). Discovery is not stayed in federal court.

117. Glob. Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d 1261 (C.D. Cal. 2001).

118. *Id.* at 1266.

119. *Id.* at 1270-71.

120. Our experience with such ISPs has been extremely poor, as the ISPs are extremely difficult to get ahold of and indifferent to obvious cases of defamation and invasion of privacy. Usually, there is no phone number to call, every communication must be by email. Supposedly Facebook, Twitter, Google and Microsoft have agreed to collaborate with EU officials by reviewing hateful speech and taking down "problematic posts" within 24 hours. *See* Lisa Eadicicco, *Facebook and Google Are Coming to War Against Hate Speech*, TIME (May 31, 2016), http://time.com/4352179/facebook-twitter-google-hate-speech/. Our experience has been that Google will take down defamatory material after a judgment find defamation, but this policy is nowhere publicly stated.

have become so emboldened, however, that they are completely non-responsive or disregard injunctions since there are no legal repercussions for doing so. *Blockowicz v. Williams* illustrates this behavior, as even after the defamation victims secured injunctions against the three offending websites, they were unable to seek enforcement of the injunctions against the remaining offender, ripoffreport.com.[121] With the combination of § 230 immunity and a longstanding tradition of directing injunctions exclusively to the parties of a lawsuit, the court ruled that ripoffreport.com was not legally required to respect the injunction. The reason was twofold: First, because § 230 made ripoffreport.com immune to liability for the posts, they could not be considered parties to the lawsuit. Second, since the website was not a party, the only way to hold ripoffreport.com accountable for injunctions under the Federal Rules of Civil Procedure was to show that the ISP acted in active concert with the poster. Since ripoffreport.com did nothing to aid or abet the defamatory posts made by third party users, it was not liable, and a sister court order finding defamation could not require the content to be removed!

Another option is to sue abroad. Although the SPEECH Act makes enforcement of foreign judgments more difficult, it will not matter if a victim is still able to enforce against a European distributor and/or entity defendant

121. Blockowicz v. Williams, 630 F.3d 563 (7th Cir. 2010). Ripoffreport.com ("Ripoff") takes a particularly aggressive stance against the removal of potentially defamatory material from its website, with a stated company policy to never remove reports once they are uploaded. Ripoff refuses to remove statements from its website, even after they have been determined to be defamatory by lower courts, certainly an arguably morally repugnant policy. In *Xcentric Ventures, LLC v. Smith*, the facts demonstrated that Ripoff had an application process in place to remove defamatory posts; it required a $2,000 non-refundable fee. Ripoff allowed for submission of evidence from both parties which was then submitted for review to the "VIP Arbitration Program" developed by Ripoff. Xcentric Ventures, L.L.C. v. Smith, No. C15-4008-MWB, 2015 U.S. Dist. LEXIS 109965, at *11-12 (N.D. Iowa Aug. 19, 2015) (holding that Xcentric had failed to demonstrate a likelihood of success on their claim to declaratory and injunctive relief due substantial evidence that Xcentric materially contributed to the alleged illegality of the information at issue while also stating that the holding was not a final decision as to CDA immunity). The company states it has successfully litigated over 20 times with a defense of CDA immunity. Information on the arbitration process is available at Ripoff's website. *See Set the Record Straight: Arbitration Program*, RIPOFF REPORT, https://www.ripoffreport.com/arbitration (last updated Dec. 14, 2017) (providing information on the arbitration process); s*ee also* GW Equity, L.L.C. v. Xcentric Ventures, L.L.C., No. 3:07-CV-976-O, 2009 WL 62173 (N.D. Tex. Jan. 9, 2009); Intellect Art Multimedia, Inc. v. Milewski, No. 117024/08, 2009 WL 2915273 (N.Y. Sup. 2009 Sept. 11, 2009); Whitney Info. Network, Inc. v. Xcentric Ventures, L.L.C., No. 2:04-cv-47-FtM-34SPC, 2008 WL 450095 (M.D. Fla. Feb. 15, 2008); Global Royalties, Ltd. v. Xcentric Ventures, L.L.C., 544 F. Supp. 2d 929 (D. Ariz. 2008).

which has assets in foreign countries such as the U.K.[122] In some cases, it may be possible to sue in several territories at once. For example, a "triple threat" lawsuit may be brought, thereby bombarding an ISP with legal action from Dublin, London, and Belfast simultaneously.

Overall, however, there is an extreme lack of remedies for defamation. In response to this scarcity, websites such as reputation.com have emerged in an attempt to manually manipulate search engines to "push down" defamatory content on web searches.[123] While the effectiveness of these "self help remedies" is debated, their existence is indicative of the problems in current U.S. law to stem the tide of Internet libel. The increasing prevalence of services such as reputation.com attests to the fact that online defamation and invasion of privacy is a growing problem for individuals and businesses.

A common trend that is also causing serious concern in many quarters is that of ISPs' relocating to what they regard as the safe havens of the U.S. and Iceland. Such moves are intended to put the ISP outside the reach of the U.K. libel courts and to allow the more ruthless operators to function with a large degree of impunity. On the other hand, the likes of Facebook and Google have decided to take advantage of Ireland's more favorable tax and other laws to establish a European basis in Dublin, thereby submitting themselves to European Union privacy and other data protection laws. This has already created problems for Facebook, which has been the subject of several high-profile litigations. One such case was brought by a group of Austrian students and in turn led to the Irish Data Protection Commissioner entering Facebook's Dublin premises to examine its records.[124]

A. *Developments in Privacy Law*

Recent years have seen a number of significant developments in the fields of privacy and data protection in the U.K. and Ireland. In 2014, in a landmark decision, the Court of Justice of the European Union (CJEU)[125] ruled that search engines such as Google are "*data controllers*" in respect to

122. *See* SPEECH Act, 28 U.S.C. §§ 4101-4105 (2012).

123. *See* Susan Adams, *Six Steps to Managing Your Online Reputation*, FORBES (Mar. 14, 2013, 6:17 PM), http://www.forbes.com/sites/susanadams/2013/03/14/6-steps-to-managing-your-online-reputation/#7f8c5f4fc1ac.

124. See Kevin J. O'Brien, *Austrian Law Student Faces Down Facebook*, N.Y. TIMES (Feb. 5, 2012), https://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html for details of the campaign initiated by the group of Austrian students. *See also* Cormac O'Keeffe, *Facebook Won't 'Like' its Seventeenth Complaint*, IRISH EXAMINER (Aug. 27, 2011), https://www.irishexaminer.com/ireland/facebook-wont-like-its-17th-complaint-165606.html.

125. Case C-131/12, Google, Inc. v. González, 2014 EUR-lex CELEX LEXIS 62012CJ0131 (May 13, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131.

their search engine results, that EU data protection laws apply to their processing of the data of EU citizens and that individuals can therefore request that links appearing in search engine results relating to the individual can be disabled where the data is outdated and irrelevant. This effectively created a "right to be forgotten" online, and Google was forced to develop procedures to deal with the flood of take down requests.[126] Data Protection rights have been strengthened even further by the implementation of the European Union General Data Protection Regulation (GDPR), which codifies the "right to be forgotten" and introduces punitive sanctions for companies who breach data subjects' rights.[127]

Further positive reinforcement of privacy rights occurred in November 2015 when the Court of Appeal in London upheld the High Court's *Weller v. Associated Newspapers Ltd.* decision that MailOnline was liable for misuse of private information and/or breaches of the Data Protection Act by publishing seven unpixellated photographs of Paul Weller's children taken whilst they were on shopping trip in Los Angeles.[128] Interestingly, the Court noted that, while it was lawful to take the photographs in California and it would have been lawful to publish them in California, this did not invalidate the children's right to a reasonable expectation of privacy in respect to publication in the U.K.

A further shift in the legal balance between privacy rights and freedom of expression occurred in the 2018 case of *Sir Cliff Richard OBE v. BBC.*[129] The legal battle arose over the BBC's coverage of a police raid on the plaintiff's premises during an investigation into historical sexual assault allegations. In reaching a decision, the court held that "[a]s a matter of general principle, a suspect has a reasonable expectation of privacy in relation

126. Google's procedure for removing search results is available as part of their FAQ section at https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en. *See also Transparency Report: Search Removals Under European Privacy Law*, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/ (last visited Oct. 28, 2018) (detailing Google's removal efforts following the CJEU González ruling).

127. Council Regulation 2016/679, ¶ 65 2016 O.J. (L 119) 1 (EU) (codifying the "right to be forgotten"); Council Regulation 2016/679, art. 83, ¶ 1, 2016 O.J. (L 119) 1 (EU) ("Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive."). Article 83 provides that companies may be fined a specific percentage of their annual global turnover for failing to comply with the provisions of the Regulation. *Id.* ¶ 2.

128. Weller v. Associated Newspapers, Ltd. [2015] EWCA (Civ) 1176 [94]-[95] (Eng.).

129. Richard v. British Broad. Corp. [2017] EWHC (Ch) 1837 (Eng.).

to a police investigation[.]"[130] This expectation to privacy was not lost by the fact that the media had become aware (although perhaps in that case by being made aware) of the investigation into Sir Cliff. The judgment has been hailed by privacy rights advocates as it will undoubtedly serve to strengthen an individual's privacy rights in the context of criminal investigations, although each case will have to be decided on its own particular circumstances.

B. *Solutions*

While it has been said that legislation takes five or more years to tackle the issues related to new and emerging technologies, it is clear that, over twenty-two years later, reform on this issue is far past due. One way to amend § 230 of the Communications Decency Act is to create a new policy that is structurally similar to the Digital Millennium Copyright Act (DMCA).[131] The DMCA originated because, much like defamation, copyright has encountered a number of violations on the unregulated domain of the Internet.[132] To mitigate this issue, the government developed a system of notice and takedown procedures to help minimize the volume of violations over the Internet.[133] Arguably this model could be directly applicable to a problem like Internet defamation, where individuals must also deal with inappropriate or unauthorized content being posted on the web.[134] If ISPs can be forced to takedown copyrighted material, why aren't similar protections afforded to victims of defamation where their very livelihood is at stake? Amending the laws in this arena is necessary if privacy rights and

130. *Id.* ¶ 248.

131. Digital Millennium Copyright Act (DMCA) of 1998, 17 U.S.C. § 101 (2012).

132. These include including free music downloading, media sharing, and uploading of YouTube videos.

133. 17 U.S.C. § 512(c)(1)(A) (providing no liability for service providers where "the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement"). Internet intermediaries and hosts are shielded from copyright infringement liability only where they act expeditiously to remove infringing material after being properly notified by the copyright owner of the infringing material. § 512(a). Such notice must only contain the "address" of the copyrighted material, and a statement by the copyright owner that the use of the material is not authorized. 17 U.S.C. § 512(c)(3). The original poster then has the option of filing a counter-notice stating that the material is non-infringing, which may result in the information being re-posted. 17 U.S.C. § 512(g)(2).

134. Some argue that DMCA- like libel law is almost unworkable as it would require ISPs to create new infrastructure to deal with processing defamation related claims. Unlike copyright infringement claims which are concrete and clear, analyzing claims for defamation are more subjective and would likely require in house counsel to determine the legitimacy of an Internet defamation claim.

protections against libel and impersonation are to be seriously protected. The new protections may require, for example, that ISPs have a dedicated ombudsman easily available and accessible to discuss the issues.

Likewise, as there is no Constitutional protection for defamatory content or content that invades privacy, why can't Congress pass a law requiring a retraction or deletion of private information? The ISPs typically counter with the argument that it would be burdensome to do so. Really? Facebook and Google, for example, are two of the largest corporations in the world. If the traditional news media can abide by these rules, why can't ISPs? The harm that is caused by defamation and wrongful invasions of privacy can have ruinous effects on victims, their families, and their business endeavors. These are not isolated instances.

That Facebook was incompetent in protecting the United States from Russian influence during the 2016 Presidential campaign has been the subject of many articles and Congressional hearings.[135] We sense a sentiment in the United States and Congress for increased regulation of the ISPs. Despite the formidable lobbying efforts of the technology companies and ISPs,[136] and the concomitant fear of legislators to cross them, this can be accomplished.[137]

---

135. *See, e.g.*, 163 CONG. REC. S1136 (Feb. 14, 2017) (statements of Sen. Durbin) ("November 8, 2016, was not just election day. It was a day that will live in cyber infamy because it turns out that one of the leading enemies of the United States, the nation of Russia, was directly engaged in the Presidential campaign that resulted in the election on November 8. This is not speculation. It is a fact based on conclusions that came from 17 different intelligence agencies that confirmed this reality."); 164 CONG. REC. H3347-48 (Apr. 17, 2018) (statements of Rep. Hartzler) ("Russia's interference in the 2016 Presidential election by spreading disinformation on social media is troubling, and it showcases Russia's success in weaponizing the Internet. Russia has exploited political divisions with the intention to cause individuals to question the legitimacy of our democracy. That is Russia's ultimate goal, not to sway the outcome of elections, but to call into question the very foundations that make our democracy strong by provoking mistrust and instability into democratic institutions."); Elizabeth Weise, *Russian Fake Accounts Showed Posts to 126 Million Facebook Users*, USA TODAY (Oct. 30, 2017, 6:19 PM), https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/.

136. Google spent over $18 million lobbying politicians in 2017, the first time a technology company has spent the most on lobbying costs in at least twenty years. In addition, "Facebook spent $11.5 million on lobbying activities in 2017, Amazon spent over $12.8 million, Microsoft spent $8.5 million, and Apple spent $7 million." Alana Abramson, *Google Spent Millions More Than its Rivals Lobbying Politicians Last Year*, TIME (Jan. 24, 2018), http://time.com/5116226/google-lobbying-2017.

137. On April 11, 2018, President Trump signed into law H.R. 1865, the "Allow States and Victims to Fight Online Sex Trafficking Act of 2017" (commonly known as "FOSTA"). The law is intended to limit the immunity provided under § 230 of the CDA for online services that knowingly host third-party content that promotes or facilitates sex trafficking. The ISP's initially

This is an ever-present issue in the digital world that victims, as individuals, are powerless to do anything on their own. We, as a society, cannot continue to turn a blind eye to dangers of completely unchecked Internet use when so many livelihoods are regularly threatened. The constituencies for such changes are the past, present, and future victims of Internet libel who are not organized and are powerless against the Internet lobbies supporting the status quo.

The danger is that while Western democracies largely ignore the growing instances of Internet abuse, countries such as China have shown their impatience by taking sweeping and draconian measures against the likes of Google, causing it to shut down completely within China's jurisdiction. The time is surely right for an International Tribunal to be established to examine the options available across the board for the international community to counter this serious problem, which will not be resolved any time soon.

Until such action is taken, regulation of Internet content is done largely on an ad hoc basis by corporations such as Google, which, because of its international presence, must attempt to strike a balance between different international free speech and content laws. Google treats content removal requests on a case-by-case basis and uses a broad set of criteria to guide its decisions, including the wording of local law and whether the request is sufficiently narrow in scope.[138] The result is a virtual ethical tightrope for American companies who host content internationally. A Google spokesperson stated that the scope of the problem was "really alarming" and "a consistent problem" because "laws are different around the world."[139] With the kind of assets, market share and profits of the major ISPs, there is no reason these entities cannot meet the needs of modern society. The ISPs, simply put, are reluctant, if not outright refusing, to deal with the moral and societal implications of conduct, which is repugnant to the best interests of society. If it can work in the EEC, it can work in the USA.[140]

In the U.K., section 5 of the English Defamation Act, establishes a procedure where a defamation action is contemplated against the operator of

---

resisted this law, but ultimately caved in the face of public sentiment. *See* FOSTA, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

138. Google's current policy can be found at https://support.google.com/websearch/answer/2744324?hl=en.

139. Paul Sonne, *Google's Censorship Juggle*, WALL ST. J., June 18, 2012, at B3.

140. Since May 29, 2014, Google has received 744,041 "requests to delist" and 2,845,899 URLs requested to be delisted. Of these, 1,075,046 (or 44%) of the URLs requested were in fact delisted. So, it can be done both efficiently and effectively. *Transparency Report: Search Removals Under European Privacy Law*, *supra* note 126.

a website.[141] In providing a potential defense for an operator, the section is also intended to enable a claimant to "identify" and pursue the individual who actually posted the offending material rather than the operator.[142] However, this has had little appreciable impact on the fundamental and increasing problem of online abuse threats, harassment, and breaches of privacy.

This escalatory problem is a serious issue that will ultimately have to be addressed by the international community at large, as recent events have demonstrated all too clearly. Change is due, and we predict it will happen for the better, and hopefully sooner rather than later.

---

141. Defamation Act 2013, c. 26, § 5 (Eng.).

142. *Id.*