TWITTER TROUBLE: THE COMMUNICATIONS DECENCY ACT IN INACTION

Julie Hsia*

The Communications Decency Act affords Internet service providers (ISPs) immunity from liability for defamation, among other crimes, to allow self-policing of websites. However, due to this immunity, websites have no incentive to remove defamatory content, which undermines the entire purpose of the Communications Decency Act. To improve this statute and promote the removal of defamatory content, the United States should follow in the footsteps of countries with more effective Internet laws. This Note presupposes that a higher percentage of Twitter removal requests in which Twitter has withheld some content indicates a higher efficacy of the Internet laws in those countries. The data published by Twitter shows that France, Germany, Japan, the Netherlands, and Russia are the top five countries in terms of percentage of removal requests with which Twitter has complied. Four of these five countries have laws similar to the notice and takedown provision of the Digital Millennium Copyright Act, which requires an Internet service provider to quickly remove content once made aware of its unlawful nature. Therefore, a notice and takedown provision with a critical opinion safe harbor should be added to the Communications Decency Act.

* J.D. Candidate 2017, Columbia Law School; B.A. 2014, Wesleyan University. Many thanks to Professor Philippa Loengard for her invaluable guidance and feedback on this Note. Additional thanks to Samantha Adler, Hilary Greenwald, and the staff of the Columbia Business Law Review for their outstanding editing and assistance in preparing this Note for publication. Lastly, special thanks to my family and friends for their love and support.

I. INTRODUCTION

The Communications Decency Act of 1996 ("CDA"), and specifically Section 230, affords users of Internet services and Internet Service Providers ("ISPs") immunity from defamation liability (excluding criminal laws and federal intellectual property law) and encourages self-policing of websites.[1] However, because websites have this immunity, they are not legally required to remove defamatory content.[2]

1 47 U.S.C. §230(c) (2012). The statute states in part:

> 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. . . 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, 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

From a business standpoint, it might make sense to allow potentially defamatory statements to remain on a website as a way to increase discussion and viewership. Many websites suggest posting controversial content to increase traffic.[3] Such controversial (and potentially defamatory) content could increase the website's users (i.e., those who respond to the controversial/defamatory statement) and notoriety among viewers.

Since leaving up defamatory posts can increase traffic and because ISPs face no liability due to the CDA, ISPs and websites have little incentive to self-police such conduct that would be tortious absent the CDA immunity. This Note will examine whether the immunity provided to websites by the CDA actually disincentivizes, rather than promotes, self-policing, monitoring, and removal of defamatory content. Further, this Note argues that the laws of other countries are more effective at incentivizing websites to remove defamatory content.

Part II of this Note provides an overview of the CDA and describes the current state of United States Internet law with respect to defamation. In Part III, this Note uses data disclosed biannually by Twitter[4] on the number of removal

> others the technical means to restrict access to material described in paragraph (1) [subparagraph (A)].

Id.

2 Joanna Schorr, *Malicious Content on the Internet: Narrowing Immunity Under the Communications Decency Act,* 87 ST. JOHN'S L. REV. 733, 737 (2013).

3 *See, e.g.,* David Attard, *101 Effective Ways to Increase Website Traffic with Social Media,* DART CREATIONS, https://www.dart-creations.com/increase-website-traffic/human-techniques/101-ways-to-increase-website-traffic-with-social-media.html [https://perma.cc/C9Q8-47XM] (last visited Feb. 21, 2017); Shanna Mallon, *Get More Blog Traffic NOW with These 25 Masterful Tips*, POST PLANNER, http://www.postplanner.com/get-more-blog-traffic-now-25-tips/ [https://perma.cc/6BMT-X4QZ] (last visited Feb. 21, 2017).

4 Twitter is an online information network which allows users to post 140-character messages (called Tweets) to its website. *Getting Started*

requests received as well as Twitter's compliance with those requests to determine which countries have a significant percentage of removal requests granted by Twitter. Specifically, this Note uses Twitter's compliance with removal requests as a proxy for the effectiveness of a country's Internet laws. Part IV examines the laws of the five countries with the highest removal percentage on Twitter to find similarities in their defamation or Internet legislation. Finally, Part V proposes that Congress add a notice and takedown provision and a critical opinion safe harbor to the CDA that mirrors those found in the laws of international counterparts.

II. BACKGROUND

Following the rise of the Internet, the United States government faced a number of challenges in applying preexisting defamation laws to the new form of communication. This Note addresses specifically the application of defamation laws to the Internet in the United States and the resulting liability (or lack thereof) for ISPs. Section I.A provides an overview of defamation law and how it has been applied to Internet communications. Section I.B discusses the history behind the CDA and analyzes the resulting interpretation of the statute by courts. Lastly, Section I.C examines the previous solutions that other scholars have formulated to resolve the problems created by the CDA.

with Twitter, TWITTER, https://support.twitter.com/articles/215585?lang=en [https://perma.cc/AN3W-KCMG] (last visited Feb. 21, 2017).

A. Defamation Law

1. History of Defamation Law as Applied to Print Sources

Defamation law is well-established with respect to print sources such as newspapers and tabloids.[5] Defamation, the invasion of an individual's interest in having a good reputation and a good name, includes both libel (written statements) and slander (oral statements).[6] While defamation laws vary by state, in order to make a prima facie case of defamation, a plaintiff must generally show: (1) that the defendant produced a false statement purporting to be fact; (2) publication or communication of that false statement to a third person; (3) fault; and (4) damages or harm to the subject of the statement.[7]

The landscape of defamation law continues to balance First Amendment free speech concerns with a plaintiff's right to reputation.[8] For example, in *New York Times v. Sullivan*, an elected Alabama official sued the New York Times for publishing a libelous advertisement after police allegedly took action against students who had participated

5 *See, e.g.*, Milkovich v. Lorain Journal Co., 497 U.S. 1 (1990); Curtis Publ'g. Co. v. Butts, 388 U.S. 130 (1967); N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964).

6 Albert v. Loksen, 239 F.3d 256, 265 (2d Cir. 2001).

7 *E.g.*, Fleming v. Rose, 350 S.C. 488, 494 (S.C. 2002); Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 240 (2007).

8 Medenica & Wahab, *supra* note 7, at 239 (stating that "[t]he law of defamation has evolved as a tug-of-war between a plaintiff's right to enjoy his reputation and a defendant's right to freedom of speech under the First Amendment"); Patricia Spiccia, Note, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given,* 48 VAL. U. L. REV. 369, 374 (2013) (asserting that "[d]efamation law has been referred to as a 'tug-of-war' between two fundamental rights—the plaintiff's right to her reputation and a defendant's First Amendment right to free speech.").

in a civil rights demonstration.[9] The United States Supreme Court held that defamation plaintiffs must show "actual malice"—knowledge that the defamatory statement was false or made with reckless disregard of whether it was false or not—for statements made about public officials[10] In *Gertz v. Robert Welch, Inc.*, the Supreme Court refused to extend the *New York Times* "actual malice" requirement to statements concerning private individuals.[11] Nevertheless, the *Gertz* court suggested that opinions cannot form the basis for a defamation action since "under the First Amendment there is no such thing as a false idea."[12]

2. Defamation Law as Applied to Internet Sources

Once the Internet came into existence, courts struggled to apply defamation law to online postings and Internet users. In order to determine which defamation standard to use, courts must decide who counts as a celebrity on the Internet. Do all users count as public figures because they actively chose to use and post content on the Internet? Or do only users with a significant following count, and if so, how large must that following be? For example, when applying the *New York Times* standard, courts have had to analogize to previous defamation in print media cases and consider whether Internet users more closely resemble a celebrity who thrust themselves into the public (and thus become

9 *N.Y. Times Co.*, 376 U.S. at 256–59.

10 *Id.* at 279–80. In *Curtis Pub. Co. v. Butts*, the Supreme Court extended this protection to "public figures." 388 U.S. 130, 155 (1967) ("We . . . hold that a 'public figure' who is not a public official may also recover damages for a defamatory falsehood . . . on a showing of highly unreasonable conduct constituting an extreme departure from the standards of investigation and reporting normally adhered to by responsible publishers.").

11 Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974). In the case, the petitioner was a private attorney who had been called a Communist after representing a youth killed by a policeman. *Id.* at 323.

12 *Id.* at 339–40.

subject to the actual malice standard)[13] or a divorcee whose divorce happened to become sensationalized even though she did not interject herself into a matter of public controversy.[14] One of the most substantial questions courts have grappled with is who constitutes a "publisher" of a defamatory statement. For instance, potential publishers may include the original posters, any re-posters, and the host websites. It is often extremely difficult for potential plaintiffs to track down the original poster, due to the anonymity of the Internet. In addition, even if a potential plaintiff identifies the original poster, that individual may be judgment-proof due to a lack of assets.[15] Therefore, most early cases involved plaintiffs suing ISPs.

Congress defines ISPs as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[16] Conversely, information content providers—those who substantially contribute to the content of the website—are essentially considered publishers, and therefore they are not immune from defamation suits because the immunity provisions of the CDA would not apply.[17]

3. The Publisher-Distributor Dichotomy

Using traditional defamation law principles, courts have attempted to distinguish among common carriers, distributors, and publishers.[18] From a policy standpoint, the

13 *N.Y. Times Co.*, 376 U.S. at 254.

14 Time, Inc. v. Firestone, 424 U.S. 448 (1976).

15 Matthew G. Jeweler, Note, *The Communications Decency Act of 1996: Why §230 Is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers*, 8 U. PITT. J. TECH. L. & POL'Y 3, 30 (2007).

16 47 U.S.C. § 230(f)(2) (2012).

17 Schorr, *supra* note 2, at 744.

18 Ryan Gerdes, *Scaling Back §230 Immunity: Why the Communications Decency Act Should Take a Page From the Digital Millennium Copyright Act's Service Provider Immunity Playbook*, 60 DRAKE L. REV. 653, 655–56 (2012).

law aims to hold accountable those who can actually influence the substance of the defamatory statement.[19] Therefore, common carriers (like telegraph or phone companies) have immunity because it would be difficult for them to control the information that is communicated over their networks.[20] Similarly, distributors (such as bookstores) have immunity because they do not have complete control over the information communicated in the materials they distribute, although they would incur liability if they "know or have reason to know of [the] defamatory character" in those materials.[21] Therefore, early suits revolved around whether ISPs constituted publishers or distributors.[22] Early cases stated that the distinction between publisher and distributor primarily depended on whether the online service provider exercised editorial discretion over the website and thus influenced the content available, in which case it would be classified as a publisher rather than a distributor.[23] However, in part due to the difficulty of separating publishers from distributors, the CDA eradicated the publisher-distributor dichotomy for Internet sources.[24]

B. The Communications Decency Act

To support the then-burgeoning Internet industry, the government enacted the CDA in 1996 to allow for growth and to prevent numerous lawsuits from stifling startup companies.[25]

---

19 *Id.* at 656–57.

20 *Id.* at 656.

21 David V. Richards, Note, *Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by §230 of the Communications Decency Act*, 85 TEX. L. REV. 1321, 1334 (2007).

22 *See, e.g.*, Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

23 *See, e.g.*, Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

24 *See* 47 U.S.C. § 230(c)(1) (2012); Spiccia, *supra* note 8, at 386;.

25 47 U.S.C. § 230(b) (2012) ("It is the policy of the United States—(1) to promote the continued development of the Internet and other

The CDA states that ISPs shall not be treated as a publisher or speaker of any information provided by an information content provider.[26] In addition, the CDA eliminates civil liability for interactive computer service providers or users for "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."[27] Therefore, given the policy to promote the development of the Internet, under the Act, ISPs cannot be held liable in defamation suits for any content published by others on their websites. [28]

1. Legislative History of the Communications Decency Act

Congress enacted the CDA in response to two Internet defamation cases: *Cubby, Inc. v. CompuServe, Inc.*[29] and *Stratton Oakmont v. Prodigy Services Co.*[30] These two cases attempted to determine whether an ISP resembles a publisher or distributor and created an incentive for ISPs not to exercise editorial control over their websites.[31] In response to the disincentives to monitor and remove content created by these cases, Congressmen Christopher Cox and Ron Wyden introduced the Online Family Empowerment Act (which eventually became the CDA) to allow websites to

interactive computer services and other interactive media; (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.").

26 47 U.S.C. §230(c)(1) (2012).

27 47 U.S.C. § 230(c)(2)(A) (2012).

28 *See* Spiccia, *supra* note 8, at 386.

29 776 F. Supp. 135 (S.D.N.Y. 1991).

30 No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

31 *See* Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U.L. REV. 647, 657–58 (2001).

remove pornographic material without facing liability as a publisher of that content.[32]

a. *Cubby, Inc. v. CompuServe, Inc.*

In this 1991 case, Cubby, the developer of an electronic news and gossip publication, sued CompuServe, an online library and special interest forum host, for defamation.[33] Specifically, a competing gossip publication published allegedly false and defamatory statements about Cubby's publication, and CompuServe carried these statements on its "Journalism Forum."[34] Cubby claimed that CompuServe had acted as a publisher while CompuServe argued that it had acted as a distributor.[35] Normally, "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it."[36] However, distributors only incur liability if they know or have reason to know of the defamation.[37]

The U.S. District Court for the Southern District of New York analogized CompuServe to a library (albeit an electronic, for-profit one) and therefore found the company to be more like a distributor.[38] While CompuServe had the ability to choose which publications to carry, it lacked editorial control over the content of those selected publications because the server uploaded posts and made them available to subscribers instantaneously.[39] Moreover, a different company managed the database forums and the

32 *See* Nicholas Conlon, *Freedom to Filter Versus User Control: Limiting the Scope of § 230(C)(2) Immunity*, 14 U. ILL. J.L. TECH. & POL'Y 105, 114–15 (2014).

33 *Cubby*, 776 F. Supp. at 135, 137–38.

34 *Id.* at 138.

35 *Id.* at 138.

36 *Id.* at 139 (quoting Cianci v. New Times Publ'g Co., 639 F.2d 54, 61 (2d Cir. 1980)).

37 *Id.* (citing Lerman v. Chuckleberry Publ'g, Inc., 521 F. Supp. 228, 235 (S.D.N.Y. 1981)).

38 *Id.* at 140–41.

39 *Id.* at 140.

court found no agency relationship between CompuServe and that company.[40] Therefore, since CompuServe would have no reason to know of the defamatory statements, the court found that CompuServe had acted as a distributor and could not be held liable for the potentially defamatory statements.[41]

b. *Stratton Oakmont v. Prodigy Services Co.*

In another early Internet defamation case from 1995, Stratton Oakmont, a securities investment banking firm, sued Prodigy, the operator of a computer network that offered subscribers access to bulletin boards, for defamation.[42] An unidentified user had posted on Prodigy's "Money Talk" computer bulletin board that Stratton Oakmont had committed criminal and fraudulent acts in connection with the initial public offering of Solomon-Page Ltd. stock.[43] Unlike CompuServe, Prodigy took pride in being an online service that exercised editorial control over the content of messages posted on its computer bulletin boards.[44] This care and editing caused Prodigy's "Money Talk" to become one of the leading and most widely read financial computer bulletin boards in the United States. [45]

Prodigy's content guidelines asked users to refrain from posting insulting or harassing notes and informed users that such notes would be removed when brought to Prodigy's attention.[46] Prodigy also used a software program to prescreen all postings for offensive language so that the content would be appropriate for all readers.[47] According to

40 *Id*. at 142–43.

41 *Id*. at 140–41.

42 Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995).

43 *Id.*

44 *Id*. at *2.

45 *Id.*

46 *Id.*

47 *Id.*

Cubby, the host of a forum or bulletin board would expect to be classified as a distributor, and therefore would not be liable for defamatory statements made by others on its network. However, because Prodigy actively monitored posts for language and harassment, the New York Supreme Court in Nassau County found that Prodigy acted more like a newspaper that selected content and functioned as a publisher.[48] Therefore, the court found that Prodigy could be held liable for defamatory statements posted on its website.[49]

c. The Original Intent of the Communications Decency Act Suggests a Narrower Scope of Application

In response to the disincentive created by *Stratton Oakmont*, Congress passed the CDA to allow ISPs to monitor and remove content without fear of opening themselves up to liability.[50] Section 230 began as the Cox-Wyden Amendment with the goal of protecting children from sexually explicit content. Due to the disincentive created by *Stratton Oakmont* (liability for active monitoring of content for the ISP), Congress sought to protect "Good Samaritan" ISPs who attempt to screen indecent and offensive material from liability.[51] Based on a legislative history focused on removing sexually explicit content, commentators have suggested that Congress intended the scope of Section 230 to be fairly narrow, applying solely to defamation claims and good faith efforts to self-regulate objectionable content.[52]

---

48 *Id.* at *2–3, *5.

49 *Id.* at *5.

50 Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 212 (2002).

51 Spiccia, *supra* note 8, at 383.

52 *See id.* at 386 (stating that "although the legislative history and text of section 230 suggests that the statute's scope is narrow—applying only to defamation claims and good faith efforts to self-regulate—the Fourth Circuit in *Zeran v. America Online, Inc.* rejected such a narrow reading of the statute and instead broadly construed the scope of section 230's immunity to apply to claims other than defamation").

2. Judicial Interpretation of the Communications Decency Act

Despite the narrow wording of the CDA, which references Good Samaritan content removal,[53] courts have interpreted the statute very broadly.[54] In fact, a Fourth Circuit case has applied Section 230 immunity to non-defamation-based claims.[55]

a. *Zeran v. America Online, Inc.*

In *Zeran v. America Online, Inc.*,[56] an anonymous poster claiming to be Kenneth Zeran posted "offensive" material on America Online, gave out Zeran's phone number, and asked people to call for Ken.[57] After receiving a high volume of calls and derogatory messages, Zeran contacted America Online whereupon an employee assured Zeran that the post would be removed, though no retraction would be posted.[58] The unknown third party posted more and more messages with Zeran's phone number and offensive material.[59] At the peak of the harassment, Zeran received an abusive phone call approximately every two minutes.[60] Following the prank, Zeran sued America Online for unreasonably delaying the removal of defamatory messages posted by an unidentified third party user, refusing to post retractions of the defamatory messages, and failing to screen for defamatory postings.[61]

53 47 U.S.C. §230(c) (2012).

54 Spiccia, *supra* note 8, at 385–86 (asserting that "the judiciary has typically interpreted section 230 very broadly, almost always granting immunity to ISPs.").

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

56 *Id.*

57 *Id.* at 329.

58 *Id.*

59 *Id.*

60 *Id.*

61 *Id.* at 328.

The Fourth Circuit found that Section 230 provides immunity in instances where a computer service provider functions as a publisher.[62] The *Zeran* court construed this immunity to include all traditional editorial functions such as publication, removal, postponement, or alteration of content.[63] The court held that distributors would be considered publishers for the purposes of defamation law, and that the CDA immunizes ISPs acting as publishers from liability.[64] The court also rejected liability upon receipt of notice of the defamatory content because it would defeat the purpose of the CDA, which is to promote self-policing of websites.[65]

b. Narrowing the Scope of Immunity After *Zeran*

Zeran's interpretation of the CDA has been widely followed.[66] However, some cases have attempted to reign in the sweeping scope imputed to Section 230 by *Zeran*. For example, Judge Easterbrook of the Seventh Circuit criticized the broad *Zeran* immunity as making it easier for ISPs to take the do-nothing approach.[67] In another case, the Ninth Circuit declined to give Section 230 immunity to an ISP that contributed to the alleged unlawful content because it acted as an "information content provider" and therefore did not receive immunity under the CDA.[68]

---

62 *Id.* at 330.

63 *Id.*

64 *Id.* at 331–32.

65 *Id.* at 332–33.

66 Barrett v. Rosenthal, 146 P.3d 510, 518 (Cal. 2006) (stating that "[t]he *Zeran* court's views have been broadly accepted, in both federal and state courts" and citing over a dozen cases).

67 Spiccia, *supra* note 8, at 393–94 (citing Chi. Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc. 519 F.3d 666, 670 (7th Cir. 2008); Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003).

68 Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1168 (9th Cir. 2008). The Communications Decency Act states that no ISP "shall be treated as the publisher or speaker of any information *provided*

In *Fair Housing v. Roommates.com*, the Fair Housing Councils of the San Fernando Valley and San Diego sued Roommates.com for alleged violations of the Fair Housing Act.[69] Roommates.com matched people renting rooms with those looking for places to stay.[70] However, in order to use the website, users had to create a profile which required answering questions about the users' sex, sexual orientation, and presence of children.[71] The court found that Roommates.com, an ISP, also functioned as an "information content provider"—i.e., one who is "'responsible, in whole or in part, for the creation or development' of the offending content."[72] Roommates.com chose which required questions to publish and designed its search and email systems to limit the listings available to subscribers based on the discriminatory characteristics (e.g. sexual orientation and presence of children).[73] Because of this, the Ninth Circuit found Roommates.com to be an information content provider and held that it was not entitled to Section 230 immunity.[74] In particular, the *Fair Housing* court noted that, "Congress sought to immunize the *removal* of user-generated content, not the *creation* of content."[75]

3. Problems with the Communications Decency Act

Congress enacted Section 230 to remove the disincentive to regulate content that *Stratton Oakmont* created. However, removing a disincentive does not simultaneously create an

by another information content provider." 47 U.S.C. § 230(c)(1) (emphasis added). Based on this case, ISP immunity only applies for posts by independent, third parties.

69 *Id.* at 1162.

70 *Id.* at 1161.

71 *Id.* at 1165.

72 *Id.* at 1162, 1164 (quoting 47 U.S.C. § 230(f)(3) (2012)).

73 *Id.* at 1165.

74 *Id.* at 1164, 1167.

75 *Id.* at 1163.

incentive to self-regulate.[76] Many critics argue that the CDA does not encourage self-policing because ISPs receive immunity whether or not they attempt to regulate the content.[77] While the CDA allows those who wish to regulate content for unlawfulness, it does not impose a duty to police for those who refuse to remove content and abridge speech.

One of the policy goals of the CDA is "to promote the continued development of the Internet and other interactive computer services."[78] However, the digital landscape has changed such that Internet companies worth hundreds of billions of dollars[79] could withstand suits without risk of stifling the Internet.[80]

C. Previous Remedies for the Communications Decency Act

A large body of scholarship exists regarding potential solutions to the current CDA.[81] The two most common suggestions for creating incentives for ISPs to self-police and remove defamatory content involve a notice and takedown provision similar to that in the Digital Millennium Copyright Act or self-help measures such as counter speech, removal requests, or lawsuits.

---

76 Spiccia, *supra* note 8, at 400; Gerdes, *supra* note 18, at 667.

77 Spiccia, *supra* note 8, at 395.

78 47 U.S.C. § 230(b)(1) (2012).

79 *E.g.,* Thomas Halleck, *Google Inc. Races Apple to $1 Trillion Valuation*, INT'L BUS. TIMES (Oct. 13, 2014, 5:28 PM), http://www.ibtimes.com/google-inc-races-apple-1-trillion-valuation-1704135 [https://perma.cc/9BVH-V23S] (stating that Google is worth $364.99 billion).

80 *See* Gerdes, *supra* note 18, at 667.

81 *See, e.g.,*Amanda Groover Hyland, *The Taming of the Internet: A New Approach to Third-Party Internet Defamation*, 31 HASTINGS COMM. & ENT. L.J. 79 (2008) (suggesting the application of an actual malice standard to distributor liability); McManus, *supra* note 31, at 650, 668–69 (suggesting that Section 230 be repealed and that common law defamation be applied to ISPs); Spiccia, *supra* note 8, 411–15 (suggesting a notice and takedown provision based on the Digital Millennium Copyright Act).

1. Digital Millennium Copyright Act: Notice and Takedown

Congress enacted the Digital Millennium Copyright Act in an attempt to bring the United States into compliance with international standards regarding digital piracy. Of note, Section 512 of the Digital Millennium Copyright Act provides a safe harbor for ISPs against copyright infringement claims for content posted by their customers. Under Section 512, an ISP gets immunity only if it has (1) "adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers and account holders . . . who are repeat infringers;"[82] and (2) "accommodates and does not interfere with standard technical measures" that copyright holders rely on in protecting their works online.[83] However, in order to maintain immunity, an ISP that receives notice of copyright infringement must quickly remove or disable access to the allegedly infringing materials, notify the alleged infringer of the removal, forward any counter notices from the alleged infringer to the complainant, and replace the allegedly infringing material if the complainant has not filed a lawsuit after receiving the counter notice.[84]

Criticisms of Section 512 include the resulting chilling of speech, the questionable duty of ISPs to self-police for copyright infringement, and the sufficiency of the notice requirement.[85] Additionally, in the copyright sphere, critics have compared the ineffectiveness of the notice and takedown provision to a game of whack-a-mole; despite websites taking down infringing material many times, the same material will reappear on the same website (sometimes

82 17 U.S.C. § 512(i)(1)(A) (2012).

83 17 U.S.C. § 512(i)(1)(B) (2012); Medenica & Wahab, *supra* note 8, at 257.

84 Medenica & Wahab, *supra* note 7, at 258.

85 *Id.* at 258–62.

hours after removal).[86] Yet scholars have suggested a similar notice and takedown requirement for immunity in defamation actions under the CDA.[87] Of note, this solution requires a Congressional amendment to the CDA.[88]

2. Self-Help Measures

Scholars have also suggested a number of self-help measures that do not require Congressional action or judicial intervention.[89]

Reddit is an online forum in which users can post content and "upvote" or "downvote" content to determine the order in which the content appears, while most websites display content in chronological order. Reddit overtly chooses not to remove defamatory content. Instead, Reddit states that, "[t]he best way to deal with incorrect information on the Internet is to post the correct information next to it."[90] Therefore, to battle defamatory content, users could respond by countering the defamatory speech with the truth or evidence to the contrary. However, this method may not be effective enough to protect reputations and prevent damage because counter speech will not result in the removal of the defamatory content.[91] After all, even if the correct information is posted next to the defamatory statement, people can still read the defamatory statement and choose to believe it rather than the "correct information."

---

86 *See* Stephen Carlisle, *DMCA "Takedown" Notices: Why "Takedown" Should Become "Take Down and Stay Down" and Why It's Good for Everyone*, OFFICE OF COPYRIGHT, NOVA SE. UNIV. (July 23, 2014), http://copyright.nova.edu/dmca-takedown-notices/ [https://perma.cc/AGG8-E3V3].

87 *See, e.g.*, Medenica & Wahab, *supra* note 7, at 265.

88 *See, e.g.*, *id.*; David Lukmire, Note, *Can the Courts Tame the Communications Decency Act?: The Reverberations of* Zeran v. America Online, 66 N.Y.U. ANN. SURV. AM. L. 371, 407 (2010).

89 *See, e.g.,* Spiccia, *supra* note 8, at 396.

90 *Frequently Asked Questions*, REDDIT, https://www.reddit.com/wiki/faq [https://perma.cc/LJ3Y-QX92] (last visited Feb. 21, 2017).

91 Spiccia, *supra* note 8, at 407.

Many websites have a method of reporting inappropriate content.[92] However, contacting the ISP may be ineffective because the CDA provides immunity to websites that then are not required to remove defamatory content. Nonetheless, the CDA does not change intellectual property or criminal law, so ISPs would still be required to remove copyright infringing material in order to avoid liability.[93]

Users could bring private lawsuits against the original content publisher (that is, the poster of the defamatory content rather than the ISP) for an injunction to remove the defamatory content. However, because the Internet provides anonymity, it may be hard to determine whom to sue.[94] Additionally, by suing an individual rather than an ISP, it may be very difficult to collect judgment from the defaming individual (either due to jurisdictional or financial problems). Moreover, pursuing a lawsuit can be very expensive and takes time.

In sum, the CDA eliminates civil liability for ISPs who restrict access to objectionable material to promote the self-policing of websites. However, not only does this immunity allow ISPs to keep defamatory content without any incurring liability, it also does not incentivize websites to remove defamatory content from its servers. Therefore, the United

92 *See, e.g.*, *How Do I Report Inappropriate or Abusive Things on Facebook (ex. Nudity, Hate Speech, Threats)?*, FACEBOOK, https://www.facebook.com/help/212722115425932 [https://perma.cc/44U5-YNXM] (last visited Feb. 21, 2017); *Abuse & Spam*, INSTAGRAM, https://help.instagram.com/165828726894770 [https://perma.cc/HB5Z-TCQ6] (last visited Feb. 21, 2017); *Recognizing and Reporting Spam, Inappropriate, and Offensive Content*, LINKEDIN, https://www.linkedin.com/help/linkedin/answer/37822/recognizing-and-reporting-spam-inappropriate-and-offensive-content?lang=en [https://perma.cc/5CM6-7F9T] (last visited Feb. 21, 2017); *Flag Inappropriate Content*, YOUTUBE, https://support.google.com/youtube/answer/2802027?hl=en [https://perma.cc/33FT-VHFF] (last visited Feb. 21, 2017).

93 *See* 47 U.S.C. § 230 (2012).

94 *See* Jeweler, *supra* note 15, at 30.

States should look to the laws of other countries for more effective statutory structures.

III. TWITTER DATA

In this section, this Note analyzes data released by Twitter to determine the countries in which Twitter removes content after receiving requests from governmental entities. Twitter is an online information network which allows users to post 140-character messages (called "Tweets") to its website.[95] Unlike newspapers or blogs, Twitter prides itself on the instantaneous reporting and publication of posts so users can discover news as it happens.[96] In order to easily see Tweets by other users, an individual can "follow" other users so that any Tweets from those users appear in that individual's "Timeline" (the page that first appears when a user opens Twitter).[97] Like many social media platforms, users can like posts or share them (called "Retweeting") to let the author know what other users enjoy seeing and to broaden the audience of readers to the Retweeter's followers.[98]

Because Twitter publishes Tweets immediately, users can post defamatory or unlawful content that will be seen instantaneously by others. As a result, many countries submit removal requests asking Twitter to remove some content because it violates the laws of that country.[99] Upon receiving these removal requests, Twitter can choose to self-

95 *Getting Started with Twitter*, TWITTER, https://support.twitter.com/articles/215585?lang=en [https://perma.cc/DQD5-LAJY] (last visited Feb. 21, 2017).

96 *Id*.

97 *About Your Twitter Timeline*, TWITTER, https://support.twitter.com/articles/164083 [https://perma.cc/8YKJ-XN59] (last visited Feb. 21, 2017).

98 *The Twitter Glossary*, TWITTER, https://support.twitter.com/articles/166337 [https://perma.cc/P4C2-22H6] (last visited Feb. 21, 2017).

99 *See Removal Requests*, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2015 [https://perma.cc/U86E-U887] (last visited Feb. 21, 2017) [hereinafter *Jan. 2015 Removal Requests*].

police and remove that content or refuse to comply with the removal request and allow the content to remain available to the public. Twitter desires to promote free and unrestricted speech, and therefore would likely refuse to comply with any removal requests where doing so would not cause Twitter to incur any legal liability. Therefore, countries with whose removal requests Twitter complies a significant percentage of the time suggests more effective Internet laws by providing the proper incentive for Twitter to self-police its content.

Twitter publishes the number of removal requests that countries submit as a part of its transparency report (see Figure 1).[100] According to Twitter: "Governments generally make removal requests for content that may be illegal in their respective jurisdictions. For example, we may receive a court order requiring the removal of defamatory statements, or law enforcement may ask us to remove prohibited content."[101] The removal request data does not include requests regarding content that may violate the Twitter terms of service, such as copyright infringement.[102]

To promote transparency, Twitter lets users know how much they regulate speech by publishing the number of accounts and number of Tweets withheld (see Figure 2) in addition to the percentage of content withheld (see Figure 3).[103] Notably, any given removal request may specify more than one Twitter account or Tweet.

Twitter groups the data by country and date in six month increments.[104] Additionally, Twitter provides examples of what content they withhold and what types of requests they have received from different countries.[105] For example, Japan

100 *Id*.

101 *Id*.

102 *Id*.

103 *Id*.

104 See *infra* Appendices 1–7 for raw data.

105 *See, e.g.*, *Jan. 2015 Removal Requests*, *supra* note 99.

generally submits removal requests for defamation,[106] while France generally submits removal requests for posts containing illegal hate speech or discriminatory content.[107]

Many countries submit removal requests to Twitter, but as of June 2015, Twitter has only used their "Country Withheld Content" tool to withhold content in nine different countries based on removal requests: Brazil, France, Germany, India, Japan, Netherlands, Russia, Turkey, and the United Kingdom.[108]

Of note, the number of removal requests in which Twitter withholds content may be misleading as a representation of the efficacy of that country's Internet and defamation laws, as not all of the content withheld by Twitter relates to defamation actions. For example, in Russia, Federal Law 139 does not allow websites to publish content that promotes drug use or suicide.[109] Additionally, Twitter has suspended

106 *See, e.g.*, *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jul-dec-2014 [https://perma.cc/WG86-MLV2] (last visited Feb. 21, 2017) [*hereinafter Jul. 2014 Removal Requests*]; *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2014 [https://perma.cc/KMV5-7GLH] (last visited Feb. 21, 2017) [hereinafter *Jan. 2014 Removal Requests*]; *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jul-dec-2013 [https://perma.cc/5JUM-GX2X] (last visited Feb. 21, 2017) [hereinafter *Jul. 2013 Removal Requests*]; *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2013 [https://perma.cc/9TYN-JCD5] (last visited Feb. 21, 2017) [hereinafter *Jan. 2013 Removal Requests*].

107 *See, e.g.*, *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106; *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jul-dec-2012 [https://perma.cc/CAR4-MC9Z] (last visited Feb. 21, 2017) [hereinafter *Jul. 2012 Removal Requests*].

108 *Jan. 2015 Removal Requests*, *supra* note 99.

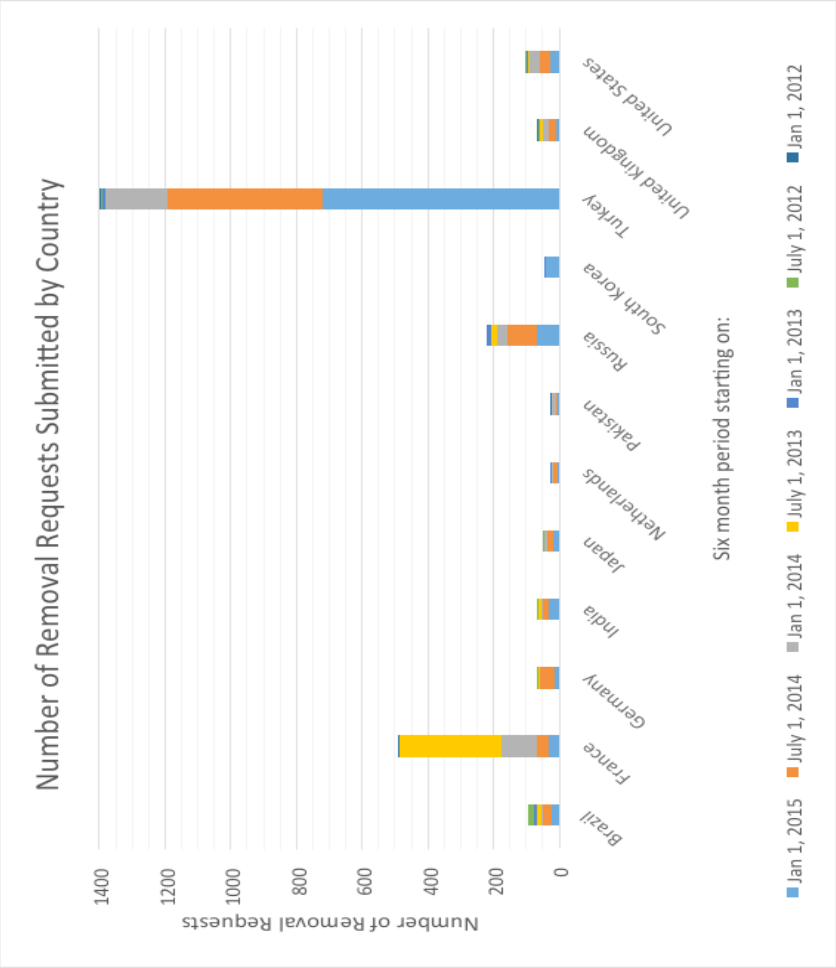
109 *E.g.*, *Jan. 2013 Removal Requests*, *supra* note 106.

two accounts in Germany because the account holders are banned neo-Nazi organizations.[110]

Figure 1 shows the number of removal requests submitted by each country, many of which Twitter declined to enforce.

110 *Jul. 2012 Removal Requests*, *supra* note 107; *Jan. 2013 Removal Requests*, *supra* note 106.

FIGURE 1: NUMBER OF TWITTER REMOVAL REQUESTS EACH COUNTRY SUBMITS[111]



111 *Jan. 2015 Removal Requests*, *supra* note 99; *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106; *Jul. 2012 Removal Requests*, *supra* note 107; *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2012 [https://perma.cc/74G5-9KAC] (last visited Feb. 21, 2017) [hereinafter *Jan. 2012 Removal Requests*].

Turkey, by far, submits the most removal requests, followed by France, and then Russia.[112] Interestingly, the three countries that submitted the most Twitter removal requests have had content withheld in the last three years.[113] However, the United States, despite submitting the fourth highest number of Twitter removal requests has never had a single Tweet or account withheld, perhaps due to the immunity the CDA provides Twitter.[114]

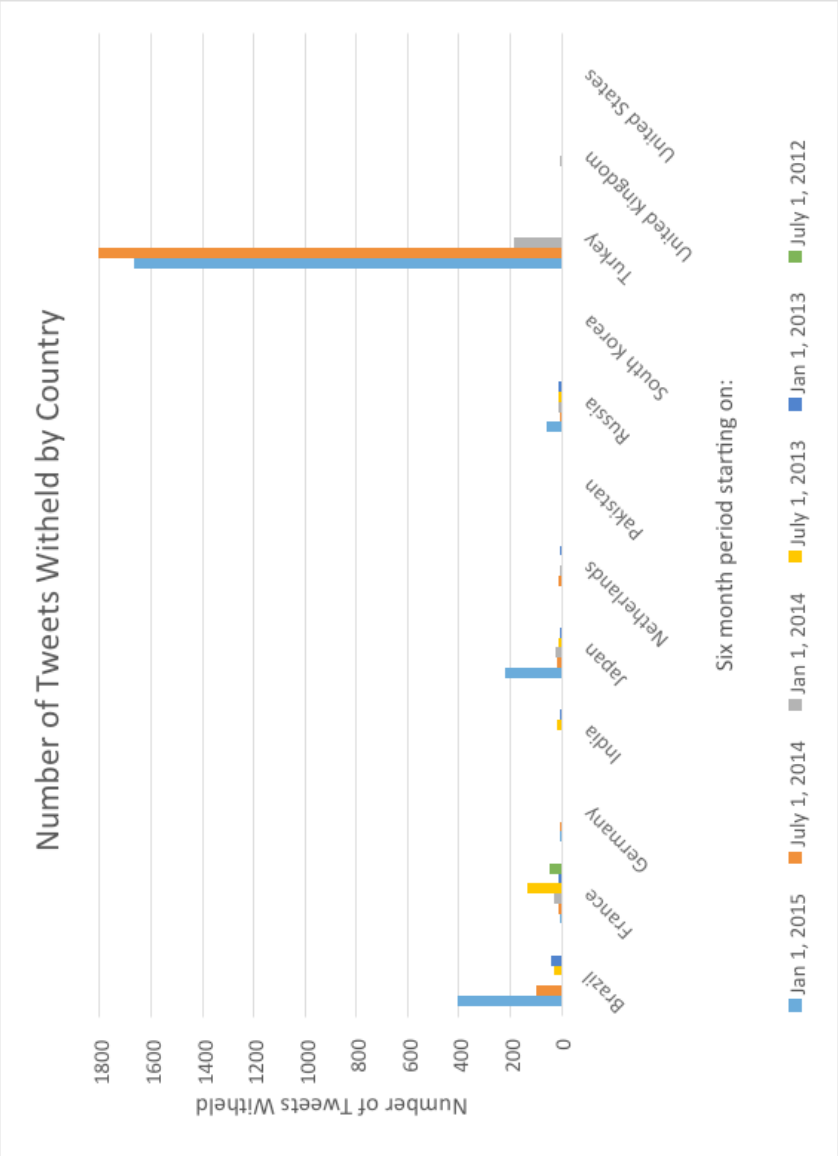
Figure 2 shows the number of Tweets that Twitter has withheld by country.

112 *Id.*

113 *Id.*

114 *Id.*

FIGURE 2: NUMBER OF TWEETS TWITTER HAS WITHHELD BY COUNTRY[115]



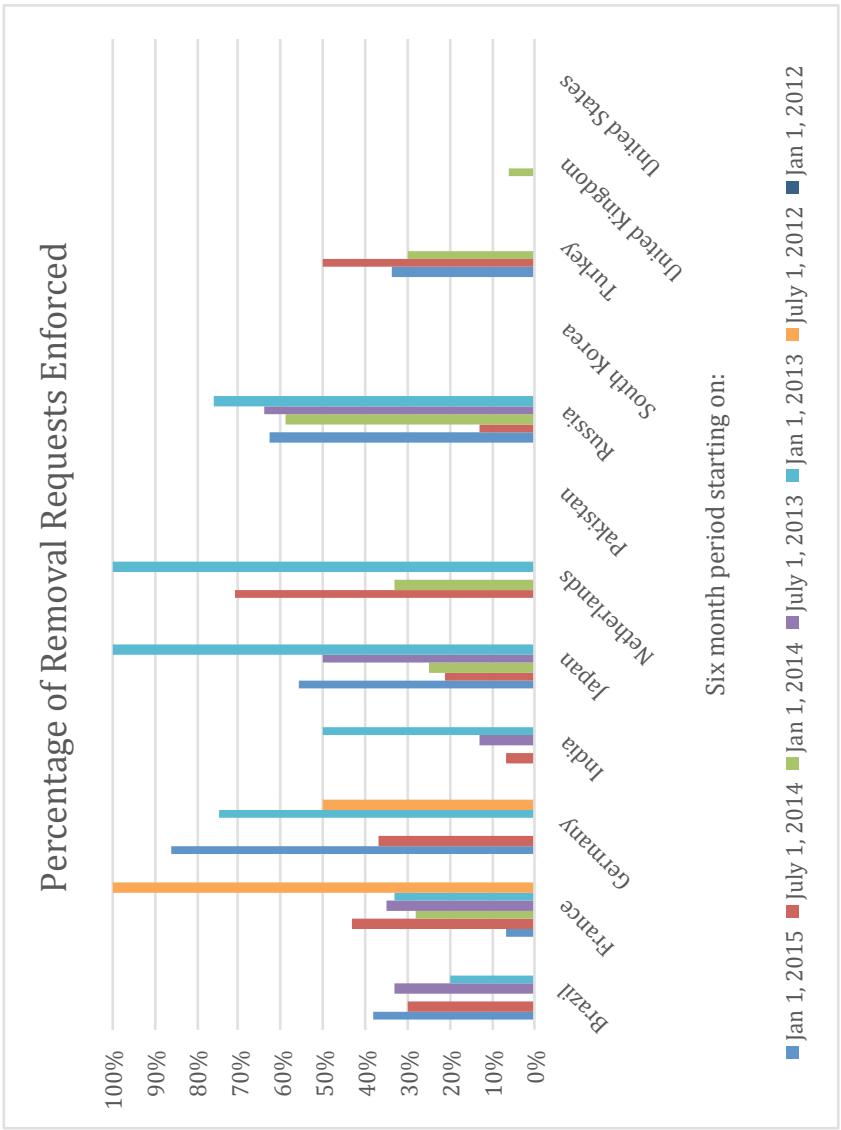
115 *Id.*

By far, Turkey has had the most number of Tweets withheld by Twitter. The countries with the most number of Tweets that Twitter has withheld after Turkey are Brazil, Japan, France, and Russia.[116]

Figure 3 shows the percentage of removal requests in which Twitter has withheld some content.

116 *Id.*

FIGURE 3: THE PERCENTAGE OF REMOVAL REQUESTS WHERE TWITTER HAS WITHHELD SOME CONTENT, BY COUNTRY[117]



117 *Id.*

Despite the high number of Tweets that Twitter has withheld in Turkey, the actual percentage of requests in which Twitter has withheld content in the country is lower than many of the other nine countries that have successfully had content withheld by Twitter due to the large number of Turkish removal request submissions to Twitter. Conversely, Germany and the Netherlands, who have had very few Tweets withheld, only submit a few removal requests annually and thus have extremely high withholding percentages. Therefore, using Twitter withholding as a proxy for effective Internet laws, it would appear that the laws in Germany and the Netherlands are more effective than the laws in Turkey.

In addition to Germany and the Netherlands, three other countries have high withholding percentages: France, Japan, and Russia. The removal requests from Japan are almost exclusively for defamation, which differs from the types of requests from other countries.[118] The removal requests from Germany include a few defamation claims and hate speech claims (the neo-Nazi organization accounts), but mostly involve prohibited symbols and illegal discriminatory content under the Youth Protection Act (Jugendschutzgesetz).[119] The removal requests from France and the Netherlands generally involve discriminatory content and hate speech,[120] such as anti-Semitic content.[121] The removal requests from Russia originate under Federal Law 139, which prohibits content

118 *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106.

119 *Jan. 2015 Removal Requests*, *supra* note 99; *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106; *Jul. 2012 Removal Requests*, *supra* note 107.

120 *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106; *Jul. 2012 Removal Requests*, *supra* note 107.

121 *See, e.g., UEJF Complains to Twitter of Anti-Semitic Tweets*, https://www.lumendatabase.org/notices/1878468 [https://perma.cc/MSE4-7XFR] (last visited Feb. 21, 2017).

that may promote drug use or suicide, and Federal Law 398, which allows Russian authorities to restrict access to extremist content or content that may lead to mass actions (such as government criticism or speech about demonstrations in Ukraine).[122]

While many of the removal requests from countries with effective Internet laws (based on using the percentage of Twitter removal requests in which some content is withheld as a proxy) do not pertain to defamation, examining the international counterparts to the CDA will still provide insight into potential improvements to the United States Internet laws. Therefore, Part IV will examine the laws of France, Germany, Japan, the Netherlands, and Russia.

IV. INTERNATIONAL DEFAMATION AND INTERNET SERVICE PROVIDER LIABILITY LAWS

A. Russia

1. Russian Internet Service Provider Liability Law

Federal Law 149 dictates the process by which the government can control and restrict access to certain Internet content.[123] However, Article 17 of Federal Law 149 states that liability for disseminating restricted information shall not be borne by the person (or hosting provider) providing services associated either with the transfer of information supplied by others (provided it is transferred without modifications and corrections) or with the storage of information and provision of access if the person had no way

122 *Jan. 2015 Removal Requests*, *supra* note 99; *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106.

123 Federal'nyi Zakon Ob Informatsii, Informatsionnykh Tekhnolog-Iyakh i o Zashchite Informatsii' [Federal Law on Information, Information Technologies and the Protection of Information] July 27, 2006, No. 149-FZ, art. 15.3.

of knowing the unlawfulness of the disseminated information.[124]

In 2012, Russia modified Federal Law 149 by essentially blacklisting websites hosting unwanted content until such content is removed.[125] Such a regime could not be used in the United States as it would violate the First Amendment.[126]

Federal Law 139—which forbids content relating to child pornography, drugs, and suicide—and Federal Law 398—which forbids content that appeals to mass riots, extremist activities, and participation in mass actions—are the legal basis for Twitter removal requests that originate in Russia.[127] Therefore, the high percentage of removal requests with which Twitter has complied does not accurately represent the efficacy of the laws dictating ISP liability for defamation, likely making it a poor example for the United States to follow.

2. Russian Defamation Law

The Russian Civil Code discusses defamation, specifically the non-material value of honor and good name, in Articles 150–152.[128] Under Article 152, a citizen has the right to sue an individual for discrediting his honor unless that individual can prove the statement was true. If successful, the citizen will have the right to publish an answer or

124 *Id*. art. 17.

125 Federal'nyi Zakon O Vnesenii Izmeneniy v Federal'nyi Zakon Ob Informatsii, Informatsionnykh Tekhnologiyakh i o Zashchite Informatsii [Federal Law On Modification of the Federal Law on Information, Information Technologies, and on Protection of Information] Dec. 28, 2013, No. 398-FZ.

126 *See* Guy W.C. Huber, *"Unfriending" the Internet: U.S. Government Domain Seizures and a Democratic Web*, 15 TUL. J. TECH. & INTELL. PROP. 243, 259 (2012).

127 *Jan. 2015 Removal Requests*, *supra* note 99; *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; J*an. 2013 Removal Requests*, *supra* note 106.

128 GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII [GK RF] [Civil Code] art. 150–52 (Russ.).

refutation in the original form of the publication and can collect damages. Article 152(6) allows a citizen to ask the court to recognize that the defamatory information has no correspondence to reality, even if the person who has spread the information cannot be identified (similar to a U.S. declaratory judgment).[129]

Some aspects of defamation law exist in the Russian Criminal Code, namely the inability to defame government officials,[130] judges,[131] or anyone in a court proceeding.[132] The Russian Administrative Code also contains provisions that address defamation.[133] Article 5.60 of the Russian Administrative Code defines "slander" as the "dissemination of wittingly false data besmirching the honor and dignity of another person."[134] Moreover, the Russian Administrative Code includes provisions specifically for those that fail to take measures to prevent slander in a work of art shown in public or in mass media.[135] While such monitoring seems only to apply to works of art, the fines levied for the failure to monitor vary from three to five thousand rubles (approximately $50–$85) for citizens, and from three hundred thousand to five hundred thousand rubles (approximately $5084–$8473) for legal entities.[136]

129 *Id.* art 152(6).

130 UGOLOVNYI KODEKS ROSSIISKOI FEDERATSII [UK RF] [Criminal Code] art. 319 (Russ.).

131 *Id*. art. 298.

132 *Id*. art. 297.

133 KODEKS ROSSIISKOI FEDERATSII RF OB ADMINISTRATIVNYKH PRAVONARUSHENIIAKH [KOAP RF] [Code of Administrative Violations] art. 5.60–5.61 (Russ.).

134 *Id.* art. 5.60(1).

135 *Id*. art. 5.60(4).

136 *Id*. art. 5.60(3). Currency conversion as of February 4, 2017.

B. Japan

1. Japanese Internet Service Provider Liability Law

Unlike Russia, the Twitter removal requests from Japan all relate to defamation.[137] Therefore, the percentage of Japanese removal requests with which Twitter complied should be a good proxy for the efficacy of Japan's Internet laws with respect to defamation.

The Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders ("2001 Provider Liability Limitation Act"), as the name suggests, indemnifies ISPs in certain situations and allows victims to demand identification of the person making defamatory statements.[138] The 2001 Provider Liability Limitation Act defines a "telecommunications service" as one that transmits with the aim of reception by unspecified persons.[139] If an ISP falls under that definition, it shall not be liable for any loss incurred when another's right is infringed unless the ISP sends the infringing information or the ISP knows of the infringing material and did not take feasible measures to prevent such information from being transmitted to unspecified persons.[140]

Additionally, if the ISP has taken measures to block certain content from transmission, they will not be liable for any loss incurred by a sender whose transmission is blocked

137 *Jul. 2014 Removal Requests*, *supra* note 106; *Jan. 2014 Removal Requests*, *supra* note 106; *Jul. 2013 Removal Requests*, *supra* note 106; *Jan. 2013 Removal Requests*, *supra* note 106.

138 Tokutei Denki Tsūshin Ekimu Teikyō-sha no Songai Baishō Sekinin no Seigen Oyobi Hasshinsha Jōhō no Kaiji ni Kansuru Hōritsu [Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders], Law No. 137 of 2001 (Japan).

139 *Id*. art. 2(i).

140 *Id*. art. 3(1).

on reasonable grounds.[141] This provision appears to indemnify ISPs who self-regulate inappropriate content, one of the original purposes of the CDA.

2. Japanese Defamation Law

The Japanese Civil Code addresses defamation in Articles 709, 723, and 724.[142] Article 723 allows a victim of defamation to recover damages and order the person who defamed him to effect appropriate measures to restore the victim's reputation.[143] However, the damages for defamation under civil law are fairly low as compared to those under criminal law.[144] Additionally, police in Japan take libel very seriously, so a victim would have the support of the Japanese police to find and prosecute the perpetrator for criminal defamation.[145]

Under Article 230 of the Japanese Penal Code, a person defames another by alleging facts in public, regardless of whether such facts are true or false.[146] While truth is not a defense to defamation of ordinary people, truth can prevent punishment if the defamation (1) relates to matters of the public interest, (2) has been made solely for the benefit of the public, or (3) has been made about a public officer or candidate for election.[147] Conversely, in the United States, since defamation generally requires a false and defamatory statement, a finding of truth establishes a total defense.[148] In sum, Japan has a fairly strict criminal defamation law because truth does not constitute a defense in defamation actions against most private citizens.

---

141 *Id*. art. 3(2).

142 MINPŌ [MINPŌ] [CIV. C.] 1896, arts. 709; 723; 724 (Japan).

143 *Id*. art. 723.

144 *See Defamation Laws in Japan*, KELLY/WARNER INTERNATIONAL DEFAMATION LAW DATABASE, http://kellywarnerlaw.com/japan-defamation-laws/ [https://perma.cc/9ZY3-VDRD] (last visited Feb. 21, 2017).

145 *Id.*

146 KEIHŌ [PEN. C.] 1907 art. 230 (Japan).

147 *Id*. arts. 230–32.

148 Medenica & Wahab, *supra* note 7, at 240.

C. Netherlands

1. Dutch Internet Service Provider Liability Law

The Netherlands, as a part of the European Union, follows the European Union Directive on Electronic Commerce.[149] The Directive on Electronic Commerce states that information service providers that store information shall not be liable for information stored at the request of a recipient of the service if the provider does not have actual knowledge of illegal information or if the provider acts expeditiously to remove or disable access to information upon obtaining knowledge of its illegality.[150] However, that immunity does not apply if the recipient of the service storing the illegal information acted under the authority or control of the ISP.[151] Additionally, the Directive on Electronic Commerce specifically states that ISPs do not have a general obligation to monitor the information stored or transmitted for circumstances indicating illegal activity.[152]

The Dutch courts, left with the task of applying broad Dutch laws to novel technologies, have ruled in compliance with the Directive on Electronic Commerce. For example, in a suit involving the Church of Scientology, the Dutch court ruled that an ISP does not have liability for illegal or infringing material stored by users if the provider is not aware of the information content.[153] However, once the ISP gains knowledge of the unlawful content, it has a duty to act to remove the material or block its availability to retain the immunity. [154]

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

150 *Id*. art. 14(1).

151 *Id*. art. 14(2).

152 *Id*. art. 15(1).

153 *See* Corien Prins, *Regulating Electronic Commerce in the Netherlands*, ELECTRONIC J. OF COMP. L. 489, 504 (2002).

154 *Id*.

The requirement that an ISP must remove the unlawful material or disable access to it upon knowledge of its illegality echoes the safe harbor provision in the Japanese 2001 Provider Liability Limitation Act, discussed in Section III.B.1, *supra*.

2. Dutch Defamation Law

The Dutch Penal Code discusses defamation in Articles 261–271.[155] Article 262 states that one committing the crime of defamation or libel must know that the fact they alleged is in fact contrary to the truth.[156] Therefore, it appears that not only is truth a defense to defamation, but genuine belief in the veracity of a statement that is in fact false would also insulate a person from liability for defamation. Other articles in the Dutch Penal Code make it a crime to intentionally defame the King,[157] the spouse of the King, the King's heirs, or the Regent,[158] and punishment can be increased for defamation of a ministry official, the public authorities, a public body or institution, and the head or a government official of a friendly state.[159]

The Netherlands has not updated their defamation laws to specifically account for the Internet and other modern technologies. Instead, the Netherlands leaves developments in civil law to the courts, who interpret the broad language of Dutch tort law.[160]

155 Arts. 261–71. SR (Neth.).

156 *Id*. art. 262.

157 *Id*. art. 111.

158 *Id*. art. 112.

159 *Id*. art. 267.

160 Prins, *supra* note 153, at 504.

D. Germany

1. German Internet Service Provider Liability Law

Germany, like the Netherlands, is a part of the European Union, and also follows the European Union Directive on Electronic Commerce. Therefore, ISPs storing unlawful information not posted by persons under the authority or control of the ISP shall not be liable if they do not have actual knowledge and act expeditiously to remove or disable access to information upon obtaining knowledge of its illegality.[161]

Like the CDA, the Directive on Electronic Commerce provides immunity to ISPs for content posted by others. However, unlike the CDA, the Directive on Electronic Commerce requires ISPs to expeditiously remove such content to maintain their immunity. Such a removal requirement sounds similar to the notice and takedown approach in the Digital Millennium Copyright Act, discussed in Section I.C.1, *supra*.

2. German Defamation Law

The German Penal Code defines defamation as a fact related to another person that may negatively affect public opinion about them, unless the fact can be proven to be true.[162] However, Section 193 carves out an exception for critical opinions about scientific, artistic, or commercial achievements in which case defamatory statements only entail liability to the extent that an insult exists from the form of the utterance or the circumstances under which it was made, rather than the content of the opinion.[163] Additionally, the German Penal Code contains specific

161 *See supra* notes 148–51 and accompanying text.

162 STRAFGESETZBUCH [STGB] [PENAL CODE], § 186, *translation* at http://www.gesetze-im-Internet.de/englisch_stgb/index.html [https://perma.cc/5V6M-HPKE] (Ger.).

163 *Id*. § 193.

provisions that outlaw publishing insulting statements about the President,[164] the country, national symbols (e.g., the German flag, colors, coat of arms, national anthem, etc.),[165] representatives of foreign states,[166] or religions.[167]

Interestingly, the German Penal Code sets the statute of limitations at three to five years (depending on whom the defamatory statement was made about) from the end of the year of publication.[168] However, since publication (with respect to the tolling of the statute of limitations) in Germany generally occurs only when, or if, the defamatory material is read, the statute of limitations period can start each time the article is accessed. Therefore, claims in relation to online articles can apparently continue forever if the information is publicly accessible.[169]

E. France

1. French Internet Service Provider Liability Law

France, as a part of the European Union, also follows the European Union Directive on Electronic Commerce. Additionally, France has passed a separate Law on Confidence in the Digital Economy to more concretely implement requirements from Articles 4 through 15 of the Directive on Electronic Commerce.[170] Article 6 of the Law on

164 *Id.* § 90(1).

165 *Id.* § 90a.

166 *Id.* § 103.

167 *Id.* § 166.

168 *Id.* § 78.

169 *Defamation Laws in Germany*, KELLY/WARNER INTERNATIONAL DEFAMATION LAW DATABASE, http://kellywarnerlaw.com/germany-defamation-laws/ [https://perma.cc/4VAV-EX9U] (last visited Feb. 21, 2017).

170 WINSTON MAXWELL, HOGAN & HARTSON, SUMMARY OF FRENCH LAW ON CONFIDENCE IN THE DIGITAL ECONOMY, 21 JUNE 2004 (2005), http://www.hoganlovells.jp/files/Publication/1800aed8-ccd6-4c9f-ab3d-01d5ccbedfeb/Presentation/PublicationAttachment/dc307826-0fbb-40b4-92fa-0568b38da5f3/FrenchLaw_0205.pdf [https://perma.cc/5VN3-AFBR].

Confidence in the Digital Economy states that an Internet host provider may incur liability as a result of storing illegal information if the host knows of the unlawful nature or, once made aware of the unlawful nature, does not take prompt action to remove or disable access to the information.[171] Additionally, an Internet host provider may incur liability if the disputed content is created by a person acting under the provider's control or authority.[172]

Lastly, Article 2.IV(a) of the Law on Confidence in the Digital Economy changes the statute of limitations for Internet causes of action to three months from the date on which the message likely to give rise to an action ceases to be available to the public.[173] Therefore, since disputed content may remain available online through archival websites or search engines even after its editor has deleted the original, claims in relation to online articles can virtually continue forever, like in Germany.

2. French Defamation Law

Defamation in France appears in the Loi du 29 juillet 1881 sur la liberté de la presse ("Press Law").[174] Article 29 of the Press Law defines defamation as any allegation affecting the honor or reputation of the individual against whom it is made.[175] As seen in other countries, France also includes special provisions for defamation of the president, a public officer, a minister of government,[176] an ambassador, and a diplomatic agent,[177] among others.

171 Loi No. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [Law No. 2004-575 of June 21, 2004 on Confidence in the Digital Economy], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 22, 2004, p. 11168 art. 6 I(3).

172 *Id*.

173 *Id*. art. 2 IV(a).

174 Loi du 29 juillet 1881 sur la liberté de la presse [Law on the Freedom of the Press of July 29, 1881].

175 *Id*. art. 29.

176 *Id*. art. 31.

177 *Id*. art. 37.

In France, defamation defendants have two defenses at their disposal: truth (unless the charge concerns an individual's privacy)[178] and good faith.[179] Therefore, since France has no defense for opinion, a defendant would have to instead argue that a statement is made in good faith. Evidence of good faith includes belief in the truth of the statement, the desire to inform the public, and the use of the word "allegedly."[180]

V. PROPOSALS FOR CHANGING THE COMMUNICATIONS DECENCY ACT

An examination of international laws on ISP liability that effectively promote self-regulation of websites, based on the percentage of Twitter removal requests in which Twitter has withheld content, demonstrates that the laws of four of the top five countries are similar. Russia, the one country with substantially differing laws, does not have any withheld content in defamation cases, and therefore is less relevant for the purposes of this Note. Therefore, the United States may want to allow the laws of the other four countries to influence the provisions in the CDA because those laws better promote self-regulation by websites in defamation contexts without chilling speech or website development.

Japan and the countries following the European Union Directive on Electronic Commerce provide immunity to ISPs for illegal content if the ISP does not know of the unlawful content and if the ISP quickly acts to remove or disable access to the unlawful content once made aware of its existence. Additionally, the ISP cannot have had authority or control over the person who posted the illegal content. Such

178 *Id*. art. 35.

179 *Id*. art. 35a.

180 TAYLORWESSIN, DEFAMATION AND PRIVACY LAW AND PROCEDURE IN ENGLAND, GERMANY AND FRANCE 10 (Niri Shan & Timothy Pinto eds., 2006), https://united-kingdom.taylorwessing.com/uploads/tx_siruplawyermanagement/IP_Defamation_and_privacy.en.pdf [https://perma.cc/2HUG-P5XF].

provisions sound similar to the notice and takedown provision of the Digital Millennium Copyright Act, which other legal scholars have suggested should be added to the CDA.[181]

The notice and takedown provision would require ISPs to act rather than sit idly by when unlawful content, such as defamation, has been stored on their servers. Additionally, this provision adds no extra duty to monitor, but merely respond to requests from courts or government entities.

Opponents of the notice and takedown provision being applied to the CDA criticize the chilling of speech that may result from such a requirement.[182] Notably, the removal requests in the Twitter data come from court orders or government agencies (e.g. police).[183] This would require defamation victims to go through some legal process, such as filing a complaint and getting a preliminary injunction, rather than inundating an ISP with phone calls or emails asking for removal. In the United States at least, the requirement of a court or government order would mean ISPs get notice only of legitimate defamatory content, which they must then remove promptly. The application of the notice and takedown provision only to court and government orders should prevent some chilling of speech since the statement would have to be examined by a third party (i.e. not the writer, victim, or ISP) before issuing any removal request.

However, a government that does not like critical speech about itself may issue a request to an ISP that would then have to remove legitimate and not defamatory critical comments from their server to retain immunity. To combat this issue, a safe harbor provision, similar to that of Section 193 of the German Penal Code, should be added to exempt critical opinions about scientific (including political science), artistic, and commercial achievements from the notice and

181 Medenica & Wahab, *supra* note 7, at 265–66.

182 *Id*.

183 *See, e.g.*, *Jan. 2015 Removal Requests*, *supra* note 99.

takedown provision (e.g. potentially defamatory opinions about politicians, artists, corporations and their leaders). Therefore, ISPs could retain their immunity when refusing to comply with removal requests regarding critical opinions about governments and companies. The defense of opinion in defamation causes of action should prevent more chilling of speech.

While the notice and takedown provision does not cure all the problems regarding ISP self-policing, it puts some onus on the ISP to remove content, rather than the current regime which allows ISPs to sit back and do nothing. Therefore, to promote self-policing of defamatory content by ISPs, a notice and takedown provision combined with a critical opinion safe harbor provision should be added to the CDA.

VI. CONCLUSION

The CDA affords ISPs with immunity from liability for defamation, among other crimes, to allow self-policing of websites. However, due to this immunity, websites have insufficient incentive to remove defamatory content, which erodes the entire purpose of the CDA. To improve this statute and promote the removal of defamatory content, this Note proposes that the United States follows in the footsteps of countries with more effective Internet laws. This Note presupposes that a higher percentage of Twitter removal requests in which Twitter has withheld some content indicates a higher efficacy of the Internet laws in those countries. The data published by Twitter shows that France, Germany, Japan, the Netherlands, and Russia are the top five countries in terms of percentage of removal requests with which Twitter has complied. Four of these five countries have laws similar to the notice and takedown provision of the Digital Millennium Copyright Act, which requires an ISP to quickly remove content once made aware of its unlawful nature. Therefore, a notice and takedown provision with a critical opinion safe harbor should be added to the CDA.

APPENDIX 1: TWITTER REMOVAL REQUEST DATA FROM JANUARY 1, 2015 – JUNE 30, 2015[184]

Country	Removal Requests			Withheld		
	Court Orders	Other**	Accounts	Content (%)	Accounts	Tweets
Arg.	-	-	-	-	-	-
Austl.	-	-	-	-	-	-
Brazil	17	4	38%*	38%*	1*	403
Canada	0	1	0	0	0	0
Colombia	-	-	-	-	-	-
Cyprus	-	-	-	-	-	-
Ecuador	-	-	-	-	-	-
France	3	29	7%	7%	0	2
Germany	2	12	86%	86%	10	6
Greece	-	-	-	-	-	-
Hong Kong	-	-	-	-	-	-
India	2	31	0	0	0	0
Indonesia	0	3	0	0	0	0
Iraq	0	1	0	0	0	0
Ireland	-	-	-	-	-	-
Italy	0	2	0	0	0	0
Japan	8	8	56%	56%	0	220
Kaz.	0	1	0	0	0	0
Kenya	-	-	-	-	-	-
Kuwait	-	-	-	-	-	-
Lebanon	-	-	-	-	-	-
Malaysia	0	1	0	0	0	0
Mexico	0	1	0	0	0	0
Mongolia	0	5	0	0	0	0
Netherlands	0	4	0	0	0	0
Norway	-	-	-	-	-	-
Pakistan	0	6	0	0	0	0
Russia	0	68	63%	63%	22	56

184 *Id.*

Singapore	-	-	-	-	-	-
S. Korea	0	40	0	0	0	0
Spain	2	0	0	0	0	0
Switz.	-	-	-	-	-	-
Turkey	408	310	34%*	34%*	125*	1,667*
U.A.E.	-	-	-	-	-	-
U.K.	0	9	0	0	0	0
U.S.	0	25	0	0	0	0
Venezuela	-	-	-	-	-	-
TOTAL	**442**	**561**	**42%**	**42%**	**158***	**2,354***

*Some data was un-withheld
**Government, Agency, Police, Other

APPENDIX 2: TWITTER REMOVAL REQUEST DATA FROM JULY 1, 2014 – DECEMBER 31, 2014[185]

Country	Removal Requests			Withheld		
	Court Orders	Other**	Accounts	Content (%)	Accounts	Tweets
Arg.	0	1	2	0%	0	0
Aust.	-	-	-	-	-	-
Brazil	27	0	191	30%*	5*	101*
Canada	1	4	3	0%	0	0
Colom.	-	-	-	-	-	-
Cyprus	-	-	-	-	-	-
Ecuador	1	0	3	0%	0	0
France	1	34	38	43%	0	15
Ger.	1	42	42	37%	14	6
Greece	0	1	2	0%	0	0
Hong Kong	-	-	-	-	-	-
India	1	14	15	7%	1	0
Indo.	-	-	-	-	-	-
Ireland	-	-	-	-	-	-
Italy	-	-	-	-	-	-
Japan	4	15	26	21%	0	19
Kaz.	0	1	2	0%	0	0
Kenya	0	1	1	0%	0	0
Kuwait	0	2	2	0%	0	0
Mexico	0	2	34	0%	0	0
Neth.	0	14	14	71%	0	12
Norway	-	-	-	-	-	-

185 *Jul. 2014 Removal Requests*, *supra* note 106.

Pakistan	0	4	24	0%	0	0
Russia	2	89	91	13%	3	9
S. Korea	0	2	2	0%	0	0
Spain	0	1	2	0%	0	0
Turkey	328	149	2,642	50%*	62*	1820*
U.A.E.	-	-	-	-	-	-
U.K.	4	18	40	0%	0	0
U.S.	6	26	60	0%	0	0
Venez.	-	-	-	-	-	-
TOTAL	**376**	**420**	**3,236**	**13%**	**85***	**1,982***

*Some data was un-withheld
**Government, Agency, Police, Other

APPENDIX 3: TWITTER REMOVAL REQUEST DATA FROM JANUARY 1, 2014 – JUNE 30, 2014[186]

Country	**Removal Requests**			**Withheld**		
	Court Orders	**Other****	**Accounts**	**Content (%)**	**Accounts**	**Tweets**
Aust.	-	-	-	-	-	-
Brazil	8	0	14	0%	0	0
Canada	0	3	5	0%	0	0
Colom.	0	1	1	0%	0	0
Cyprus	0	1	1	0%	0	0
Ecuador	-	-	-	-	-	-
France	1	107	112	28%	0	30
Ger.	0	2	3	0%	0	0
Greece	0	2	2	0%	0	0
Hong Kong	1	0	1	0%	0	0
India	0	5	9	0%	0	0
Indo.	-	-	-	-	-	-
Ireland	1	1	13	0%	0	0
Italy	-	-	-	-	-	-
Japan	2	6	31	25%	0	24
Kuwait	0	5	7	0%	0	0
Mexico	-	-	-	-	-	-
Neth.	0	3	3	33%	0	1
Norway	1	1	1	0%	0	0
Pak.	0	12	101	0%*	0*	0*
Russia	0	32	34	59%	8	11
S. Korea	-	-	-	-	-	-
Spain	1	1	4	0%	0	0

186 *Jan. 2014 Removal Requests*, *supra* note 106.

Turkey	65	121	304	30%*	17*	183*
U.A.E.	0	1	13	0%	0	0
U.K.	3	14	22	6%	0	2
United States	5	26	42	0%	0	0
Venez.	-	-	-	-	-	-
TOTAL	**88**	**344**	**723**	**9%**	**25**	**251**

*Some data was un-withheld
**Government, Agency, Police, Other

APPENDIX 4: TWITTER REMOVAL REQUEST DATA FROM JULY 1, 2013 – DECEMBER 31, 2013[187]

Country	Removal Requests			Withheld		
	Court Orders	Other**	Accounts	Content (%)	Accounts	Tweets
Aust.	-	-	-	-	-	-
Brazil	11	1	50	33%	2	26
Canada	-	-	-	-	-	-
Ecuador	-	-	-	-	-	-
France	3	306	146	35%	0	133
Ger.	1	1	1	0%	0	0
Greece	0	2	3	0%	0	0
Hong Kong	0	1	1	0%	0	0
India	2	6	54	13%	0	13
Indo.	-	-	-	-	-	-
Ireland	0	1	1	0%	0	0
Italy	0	1	1	0%	0	0
Japan	1	1	1	50%	0	10
Kuwait	0	2	3	0%	0	0
Mexico	0	1	2	0%	0	0
Neth.	-	-	-	-	-	-
Pak.	-	-	-	-	-	-
Russia	0	14	14	64%	1	9
S. Korea	-	-	-	-	-	-
Spain	-	-	-	-	-	-
Turkey	2	0	2	0%	0	0
U.A.E.	1	1	5	0%	0	0
U.K.	1	8	9	0%	0	0
U.S.	2	6	11	0%	0	0

187 *Jul. 2013 Removal Requests*, *supra* note 106.

Venez.	0	1	13	0%	0	0
TOTAL	**24**	**353**	**317**	**11%**	**3**	**191**

*Some data was un-withheld
**Government, Agency, Police, Other

APPENDIX 5: TWITTER REMOVAL REQUEST DATA FROM JANUARY 1, 2013 – JUNE 30, 2013[188]

Country	**Removal Requests**			**Withheld**		
	Court Orders	**Other****	**Accounts**	**Content (%)**	**Accounts**	**Tweets**
Aust.	0	2	2	0%	0	0
Brazil	9	1	11	20%	1	39
Canada	1	0	1	0%	0	0
Ecuador	0	1	1	0%	0	0
France	0	3	14	33%	0	12
Germany	1	3	4	75%	3	0
Greece	-	-	-	-	-	-
India	1	1	2	50%	0	3
Indo.	1	1	2	0%	0	0
Japan	1	1	2	100%	0	6
Neth.	0	2	2	100%	0	5
Pak.	-	-	-	-	-	-
Russia	0	17	17	76%	4*	8
S. Korea	0	1	1	0%	0	0
Spain	0	1	3	0%	0	0
Turkey	3	4	30	0%	0	0
U.K.	1	1	2	0%	0	0
U.S.	2	0	11	0%	0	0
Venez.	1	0	1	0%	0	0
TOTAL	**21**	**39**	**104**	**38%**	**4**	**73**

*Some data was un-withheld
**Government, Agency, Police, Other

188 *Jan. 2013 Removal Requests*, *supra* note 106.

APPENDIX 6: TWITTER REMOVAL REQUEST DATA FROM JULY 1, 2012 – DECEMBER 31, 2012[189]

Country	**Removal Requests**			**Withheld**		
	Court Orders	**Other****	**Content (%)**	**Accounts**	**Accounts**	**Tweets**
Aust.	0	1	0%	1	0	0
Brazil	16	0	0%	22	0	0
Canada	2	0	0%	2	0	0
France	0	1	100%	40	0	44
Germany	0	2	50%	7	1	0
Greece	-	-	-	-	-	-
India	1	1	0%	16	0	0
Japan	0	1	0%	5	0	0
Pak.	-	-	-	-	-	-
Spain	1	0	0%	1	0	0
Turkey	0	6	0%	9	0	0
U.K.	4	2	0%	25	0	0
U.S.	2	2	0%	12	0	0
TOTAL	**26**	**16**	**5%**	**140**	**1**	**44**

**Government, Agency, Police, Other

189 *Jul. 2012 Removal Requests*, *supra* note 107.

APPENDIX 7: TWITTER REMOVAL REQUEST DATA FROM JANUARY 1, 2012 – JUNE 30, 2012[190]

Country	**Removal Requests**			**Accounts Specified**
	Court Orders	**Other****	**Content (%)**	
France	0	1	0%	2
Greece	2	0	0%	2
Pakistan	0	1	0%	1
Turkey	1	0	0%	7
U.K.	0	1	0%	6
TOTAL	**3**	**3**	**0%**	**18**

*Some data was un-withheld
**Government, Agency, Police, Other

190 *Jan. 2012 Removal Requests*, *supra* note 111.