Fairfield UNIVERSITY

North East Journal of Legal Studies

Volume 41 *2021* Article 1

Spring 3-20-2021

Online Defamation Recourse

Bradford H. Buck
University of Hartford

ONLINE DEFAMATION RECOURSE

by

Bradford H. Buck*

I. INTRODUCTION

This article discusses the law of defamation (particularly the form of written defamation known as libel), the various types of online sites where libel could occur and the available recourse or remedies for the person who was libeled online.

II. THE LAW OF DEFAMATION

The Restatement (Second) of Torts, § 558 provides the following elements for defamation: "to create liability for defamation there must be:

> (a) a false and defamatory statement concerning another;
> (b) an unprivileged publication to a third party;
> (c) fault amounting at least to negligence on the part of the publisher; and

---

* Instructor of Business Law at the Barney Business School, University of Hartford

> (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication."[1].

The first element of defamation requires the that the statement must be a statement of fact and not opinion. It can be very difficult to sort out whether a statement is a statement of fact or opinion. "In determining whether a statement is merely an opinion and thus not subject to a cause of action for defamation as a matter of law, courts must take several considerations into account: "whether the statement has a precise and readily understood meaning; whether the statement is verifiable; and whether the statement's literary or social context signals that it has factual content."[2]

The second element of defamation is publication to a third party. In the internet context, this is usually not a problem since the statement is typically published to at least one third person or available for anyone on the internet to see.

The third element of defamation involves the degree of liability. The notes for the Restatement (Second) of Torts Section 558 provides that this was added as a result of the US Supreme Court's constitutional decisions.[3] The most famous case is *New York Times Co. v Sullivan*.[4] In that case, the US Supreme Court held that in defamation actions by a public official, more than negligence is required and the plaintiff must prove actual malice which is that the statement was made with knowledge it is false or with reckless disregard of whether it was false or not.[5] Subsequently, the US Supreme Court extended this protection to "public figures".[6] In addition, there may be public figures for all purposes or public figures for a limited range of issues such a particular newsworthy event.

The fourth requirement element of defamation involves whether damage was proved or is assumed. There are two kinds of defamation: defamation per se; and defamation per quod. “A statement is defamatory *per se* if the resulting harm is apparent and obvious on the face of the statement ….If a statement is defamatory *per se*, the plaintiff is not required to plead actual damage to his reputation ….but, rather, the statement is considered to be so obviously and materially harmful that injury to the plaintiff's reputation is presumed. …. There are five categories of statements that are deemed to be defamation *per se*: (1) words imputing the commission of a criminal offense; (2) words that impute infections with a loathsome communicable disease; (3) words that impute an individual is unable to perform his employment duties or otherwise lacks integrity in performing those duties; (4) words that prejudice an individual in his profession or otherwise impute a lack of ability in his profession; and (5) words that impute an individual has engaged in fornication or adultery.”[7] “Statements are defamatory *per quod* where either: (1) the statement's defamatory character is not apparent on its face so that examining extrinsic circumstances is necessary to show its injurious meaning; or (2) the statement is defamatory on its face but does not fall within the enumerated categories of *per se* actions. Prejudice is not presumed, however, and the plaintiff must plead special damages.”[8] If a statement is not defamatory per se, it is defamatory per quod and the plaintiff must prove actual monetary damages.

The last item to mention is the category of the party who disseminated the defamation. Common law distinguished among three different types of liability regarding defamation: publisher liability, distributor liability, and common carrier liability. “Publishers generally experience the greatest amount of liability, while common carriers experience the least. Publisher liability may be attributed to any entity that exercises a high degree of editorial content control over the dissemination

of defamatory material. …Distributor liability may be attributed to any entity that distributes, but does not exercise editorial control over, defamatory material, such as a news vendor, bookstore, or library. A distributor can be characterized as an entity that transmits or delivers information that is created or published by a third party. Distributors are only held liable if they knew or had reason to know of the defamation. Lastly, common carrier liability applies to any entity that acts as a passive conduit for the transmission of defamatory material. Thus, even if it knew or had reason to know of the defamation, it may escape liability for defamation due to its lack of editorial control over the material."[9]

III. DIFFERENT TYPES OF INTERNET COMMUNICATION

There are many ways in which a person could be defamed in internet communications. Email is the first of those ways. A party would access his or her email through an internet service provider ("ISP"). An email would be sent to at least one other person. In addition, copies of the email could be sent to one or more than one other persons. All these communications should have at least the email address of the sender.

Instant messaging ("IM") is another mode of internet communication. This is similar to an email. Again, the party sending the IM would access go through an ISP or similar carrier. Typically, there may not another person copied on the IM. As with an email, there should be some number identifying the sender.

The third mode of internet communication is a blog, chatroom or forum. Typically, a party would access these forums through an ISP. However, there usually is another party involved in setting up the blog, chatroom or forum. Anyone can contribute to these sites gaining access to them though an ISP. Anyone having access to the blog, chatroom or forum can see the defamatory communication. Many parties may use another name and it may be difficult for anyone reading these comments to identify the contributor without obtaining information from the provider.

Another way to communicate via the internet is through social media. This category has sites such as Facebook, Twitter, Snapchat, LinkedIn and even other rating sites such as Yelp. Just like the previous category, usually someone is the provider and an individual then contributes comments to locations on the site gaining access through an ISP. Some of these such as Facebook and LinkedIn, may identify the person making a communication. Others, such as Yelp, may be like the previous category and it may be hard to identify the contributor.

Lastly, a party may find many sites on the internet by using search engine. There are many search engines such as Google and Bing. These search engines list various sites resulting from the search. There usually are excerpts taken from each actual site listed in the search results. A party would access a search engine through an ISP.

IV. THE COMMUNICATIONS DECENCY ACT AND INTERNET PUBLISHERS AND DISTRIBUTORS

Section 230(c) of the Communications Decency Act of 1996[10] ("CDA") provides as follows:

"(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, 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) [subparagraph (A)]."

Section 230(f) of the CDA provides the following key definitions:

"(2) Interactive computer service. 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.

(3) Information content provider. 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."

The first quoted subsection of 230(c) above provides that a provider or user is not considered to be a publisher for content provided by an information content provider. The second subsection of Section 230(c) above provides that no provider or user of an interactive computer service is liable for restricting access to certain content the provider or user considers objectionable.

There have been numerous actions brought against providers or platforms for online defamation. Many of the providers or platforms who have been sued have raised the defense that Section 230 of the CDA makes them immune from any liability. One of the most famous and early cases was the case of *Zeran v America Online*[11]. The plaintiff Zeran was the victim of a vicious online prank. An unknown person put Zeran's name and telephone number in several notices on the electronic bulletin board of the defendant, America Online ("AOL") advertising T-shirts with slogans glorifying the bombing of the federal building in Oklahoma City. After these were posted, Zeran received numerous troubling and threatening telephone calls. Zeran notified AOL of these posts and demanded their removal. After AOL removed the first posts, other similar posts again appeared, and the process of notice and eventual removal again occurred. Zeran sued AOL claiming AOL was negligent for allowing these notices to remain and reappear. Specifically, Zeran claimed AOL was the distributor of the defamatory material and while publishers are immune under Section 230 of the CDA, distributors are not. The court held that Section 230 of the CDA preempted state law, a distributor is merely a subset of a publisher under that statute and AOL was immune from suit.

Other cases have also held that internet publishers and distributors are not liable. In *Schneider v Amazon.com, Inc.*[12], the plaintiff sued Amazon.com for alleged defamatory

comments posted about the plaintiff's book on Amazon's website. The court held that to have Section 230 immunity, the following three elements are required: the defendant must be a provider or user of an "interactive computer service"; the asserted claims must treat the defendant as the publisher or speaker; and the information must be provided by another "information content provider".[13] If the defendant was the information content provider, then the defendant would not be immune and would be held liable. The court found all three elements were present in that case so Amazon was not liable.

AOL was again sued in *Blumenthal v Drudge*[14]. The Drudge Report, hosted on AOL's website, had alleged defamatory statements about the plaintiff. Even though AOL had given Drudge a license agreement and even though under that license agreement, AOL could remove content that violated AOL's terms of service, the court held that AOL was a publisher, was not the information content provider and therefore was not liable. In yet another case against AOL[15], the court held AOL was not an information content provider for stock quotation information provided by two third parties even though AOL deleted some of the stock symbols.

In *Reit v Yelp!, Inc.*[16], the plaintiff dentist contacted the defendant Yelp to remove a derogatory post about the plaintiff's dental practice. After that contact, the plaintiff alleged that Yelp removed all 10 positive reviews and retained only the negative posting. The court held that if even Yelp's action was true, it did not make Yelp the information content provider and Yelp was immune under Section 230.

In *Klayman v Zuckerberg*[17], the alleged defamatory material was an anti-Semitic post on Facebook. The plaintiff demanded that Facebook remove the page from Facebook which it eventually did. The plaintiff claimed Facebook's conduct did

not arise from its being a publisher but rather from Facebook's contractual obligations in its Statement of Rights and Responsibilities. The court held that under Section 230, Facebook and its founder Mark Zuckerberg were immune.

As a result of Section 230 of the Communications Decency Act as interpreted by all these cases, providers or platforms are not liable for defamatory posts unless the platform itself created the content. It does not matter whether these platforms are publishers or distributors. Therefore, there is a difference between merely hosting a platform and providing content on that platform. Of course, the providers and platforms are known and are the deep pockets to sue for any online defamation. The internet service providers themselves are not liable either.

There are a few cases which hold that Section 230 did not bar recovery where the providers did contribute to the questionable content. In *Carafano v Metrosplash, Inc.*[18], the defendant was an information service that provided or enabled computer access by multiple users to a computer server. Through the internet, thousands of members were able to access and use a searchable database maintained on the service's computer servers. The court held that the service was also an "information content provider," as users of the service's website did not simply post whatever information they desired, but a profile was created from questions asked by the service and the answers provided and therefore, the service was not immune under Section 230. In *Hy Cite Corp. v Badbusinessbureau*[19], the defendant's operators' website allowed users to post and view complaints, so-called "rip-off-reports," about businesses. The plaintiff, among other things, alleged that the website included 35 reports involving its business and those reports contained false and defamatory statements. Among other things, the court held that the

operators were not entitled to immunity under Section 230 of the Communications Decency Act because the manufacturer's allegations (that the operators produced original content contained in the ripoff reports and solicited individuals to submit reports with the promise that they might ultimately be compensated) were sufficient to support a finding that the operators created or developed the wrongful content.

V. OTHER RECOURSE FOR ONLINE DEFAMATION

If the party defamed online cannot sue the provider or platform for the defamatory material, what other remedies does the party have?

Unmasking the Identity of an Anonymous Online Defamer

A party who is defamed has the right to sue the party who posted the defamatory material. With some forms of online communication (such as email, instant messaging, posts on a known person's Facebook page and tweets by a known person) the identity of the party who made the defamatory statement might be known or could be easily identified. However, the identity of a party posting defamatory material on blogs, chatrooms, forums, ratings sites and some social media may not be known. So how does the defamed party find out the identity of the party who posted the defamatory content? Usually, the ISP or the platform that hosted these vehicles probably has some information or can easily find out information about the identity of the defamer.

In the appellate case of *John Doe No.1 v Cahill*[20], the allegedly defamed party sought to obtain the identity of the defamer from the ISP. The appellant (the alleged defamer) , using an alias, had posted two statements on an internet website sponsored by a news agency stating the appellee councilman (the alleged defamed party) was paranoid, full of character flaws and had mental deterioration. The appellee obtained an order requiring the ISP, Comcast, to disclose the identity of the appellant. The appellant appealed from the lower court order. The Supreme Court of Delaware looked at the appropriate standard of proof required in a motion to dismiss the case considering the First Amendment right to speak anonymously. The court adopted the standard of the New Jersey appellate court in *Dendrite Intl., Inc. v Doe*[21]. The court in *Dendrite* put forth a test that had four parts requiring the party seeking disclosure: "(1) to undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for an order of disclosure, and to withhold action to afford the anonymous defendant a reasonable opportunity to file and serve opposition to the application. In the internet context, the plaintiff's efforts should include posting a message of notification of the discovery request to the anonymous defendant on the same message board as the original allegedly defamatory posting; (2) to set forth the exact statements purportedly made by the anonymous poster that the plaintiff alleges constitute defamatory speech; and (3) to satisfy the *prima facie* or "summary judgment standard."[22] After the court concluded a plaintiff has presented a prima facie cause of action, the court must "(4) balance the defendant's *First Amendment* right of anonymous free speech against the strength of the *prima facie* case presented and the necessity for the disclosure of the anonymous defendant's identity in determining whether to allow the plaintiff to properly proceed."[23] The court in *Cahill* held that the second and fourth prongs of the *Dendrite* test were not necessary. Since prong number 1 had occurred, the court looked at prong three of the *Dendrite* test. The court held

that under the summary judgement standard, no reasonable person would believe the appellant's statements had stated facts about the appellee.

The Maryland Court of Appeals in the case of *Independent Newspapers, Inc. v Brodie*[24] applied the *Dendrite* and *Cahill* standards as well as discussing two other cases with different standards. The first other case mentioned in *Brodie* was *Columbia Insurance Company v Seecandy.com*[25], which had the following test: "First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court. This requirement is necessary to ensure that federal requirements of jurisdiction and justiciability can be satisfied. Second, the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants. Third, plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss. A conclusory pleading will never be enough to satisfy this element. Pre-service discovery is akin to the process used during criminal investigations to obtain warrants. The requirement that the government show probable cause is, in part, a protection against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong. A similar requirement is necessary here to prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant. Lastly, the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about

defendant that would make service of process possible."[26] Also, the second other case mentioned in *Brodie* was *In Re Subpoena Duces Tecum to America Online, Inc.*[27], where the Circuit Court of Virginia court put forth the lowest standard which only required that the party seeking the identity have a good faith basis for asserting a cause of action before permitting discovery of identifying information. The court in *Brodie* ended up adopting the *Dendrite* standard and ordered the lower court to grant the protective order/motion to quash preventing disclosure of the identifying information.

The Illinois Appellate Court in *Maxon v Ottawa Publishing Company*[28], discussed *Dendrite* and *Cahill* but came to a different result. In Illinois, Supreme Court Rule 224 provides how a party can determine the identity of a party they may have a claim against. That Rule provides as follows: "(i) a person or entity who wishes to engage in discovery for the sole purpose of ascertaining the identity of one who may be responsible in damages may file an independent action for such discovery. (ii) The action for discovery shall be initiated by the filing of a verified petition in the circuit court of the county in which the action or proceeding might be brought or in which one or more of the persons or entities from whom discovery is sought resides. The petition shall set forth: (A) the reason the proposed discovery is necessary and (B) the nature of the discovery sought and shall ask for an order authorizing the petitioner to obtain such discovery. The order allowing the petition will limit discovery to the identification of responsible persons."[29] The court held that this rule provided the appropriate standard and granted the petition for disclosure.

The Virginia Court of Appeals in *Yelp, Inc. v Hadeed Carpet Cleaning, Inc.*[30] stated that a Virginia has a statute which provides an unmasking standard. That statute provides as follows: "At least thirty days prior to the date on which

disclosure is sought, a party seeking information identifying an anonymous communicator shall file with the appropriate circuit court a complete copy of the subpoena and all items annexed or incorporated therein, along with supporting material showing: a. That one or more communications that are or may be tortious or illegal have been made by the anonymous communicator, or that the party requesting the subpoena has a legitimate, good faith basis to contend that such party is the victim of conduct actionable in the jurisdiction where the suit was filed. A copy of the communications that are the subject of the action or subpoena shall be submitted. b. That other reasonable efforts to identify the anonymous communicator have proven fruitless. c. That the identity of the anonymous communicator …. is …. needed to advance the claim, relates to a core claim or defense, or is directly and materially relevant to that claim or defense. d. That no motion to dismiss, motion for judgment on the pleadings, or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff is pending. The pendency of such a motion may be considered by the court in determining whether to enforce, suspend or strike the proposed disclosure obligation under the subpoena. e. That the individuals or entities to whom the subpoena is addressed are likely to have responsive information."[31] In that case, the appellate court stated there are at least nine standards for unmasking not including the standard in Virginia and including *Columbia Insurance*, *Cahill*, *Brodie* and *Dendrite*. The appellate court also upheld the order of the trial court enforcing a subpoena on Yelp to disclose the identifying information.

In summary, trying to find out the identity of the defamer from ISP's, platforms or providers will depend upon the state in which the party is filing the proceeding. Some states require a much more substantial showing than the other states.

Possible Actions Against the Provider

It is noteworthy that the Digital Millennium Copyright Act[32] does require that if providers or platforms receive a notice from a third party that a user has infringed on its intellectual property, the provider or platform must take action leading to the ultimate removal of the infringing material. Many of the terms and conditions of providers or platforms allow a request to take down material or give the provider or platform the right to remove material that the provider or platform consider to be objectionable. Facebook's terms of service more or less provide a user with the ability to notify Facebook of defamatory material and certainly give Facebook the right to remove objectionable material.[33] If a victim makes such a request of the provider or platform, the provider or platform may agree to remove the defamatory content. However, even if the defamatory post is removed from the site where it appeared, the defamatory post may still show up in internet searches using a search engine. To remove the defamatory material completely, the victim would need to get the search engines, such as Google or Bing, to remove it as well. This could be extremely difficult.

The case of *Barnes v Yahoo!, Inc.*[34] provides a possible recourse concerning a provider's agreement to remove objectionable content and the failure to do so. In that case, a former boyfriend of the plaintiff posted nude photographs and other sexually explicit content on Yahoo. The plaintiff requested Yahoo to remove the content, Yahoo agreed but did not do so. The plaintiff sued Yahoo alleging negligence and promissory estoppel. The court concluded that Section 230 of the Communications Decency Act barred the negligence claim but did not bar the promissory estoppel claim. So, such a claim is a possible recourse against a provider or platform if a defamed

party requests removal, the provider or platform agrees and fails to do so.

Possible Actions Against the Defamer

Some businesses have used a way to combat negative online comments using anti-disparagement clauses in their online agreements. "At present, the agreements take two forms…. In the first format, the customer agrees to a contract that prohibits [the customer] …. from making or posting any negative remarks, criticisms, or comments about a business, its goods or services. The second anti-disparagement clause involves transferring copyright ownership of any online review from the customer to the business."[35] Once this copyright ownership is transferred, the business can demand removal under the Digital Millennium Copyright Act noted above.

The case of *Palmer v Klearegear.com*[36] involved the use of such a disparagement clause. The customer made statements about the defendant's poor-quality customer service practices. The defendant levied a $3,500 fine against the plaintiff. When the plaintiff did not pay the fine, the defendant reported the unpaid fine to the credit bureau. The court found that this clause was unenforceable. Pursuant to the federal Consumer Review Fairness Act[37] and many state laws, including California[38], these clauses are unenforceable.

Another possible course of action is to respond to the content directly. A victim should carefully consider this option. The victim may end up in an online war with the perpetrator. Also, this action could further highlight the defamatory post.

CONCLUSION

Before the advent of the internet, the possibilities of being defamed occurred primarily in print media such as newspapers or magazines, but there were some journalistic standards exercised by the publishers. Now, there are much greater possibilities of being defamed online and there are fewer, if any, journalistic standards.

There are challenges with legal recourse for online defamation. The providers and platforms are mostly immune. Also, it may be difficult to unmask the identity of anonymous defamers through the providers or the ISP. Even if the defamatory content is removed, there still may be references to that content in searches performed by search engines. It is difficult to get those search engines to remove any reference to the content also. Other remedies such as the use of anti-disparagement clauses by online businesses are unenforceable. Even if the defamers are identified and not immune, there can be difficulties proving the required elements of a defamation case. A comment could be deemed to be an unactionable opinion or the defamed party could be a limited public figure and would therefore have to show malice. Also, even if those defamers are unmasked, they may not have sufficient assets to satisfy any judgement.

The best possible outcome would be to amend the Communications Decency Act to have a similar notice and removal provision as the Digital Millennium Copyright Act. Many authors have advocated that very change[39]. While the providers cannot be expected to police every posting on their sites, this notice and removal procedure would take into

account the logistical dilemma of the providers while giving some recourse to the defamed parties as well.

---

[1] Restatement (Second) of Torts, §558 (Am. Law Inst. 1977).
[2] Maxon v Ottawa Publishing, 402 Ill. App. 3d 704, 929 N.E. 2d 666, 2010 Ill. App. LEXIS 505 (2010).
[3] See Restatement, supra note 1 at reporter's notes.
[4] New York Times v Sullivan, 476 U.S. 254 (1964)
[5] *Id* at 279-280.
[6] Gertz v Robert Welch, 418 U.S. 323 (1974).
[7] Stone v Paddock, 961 N.E. 2d 380, 391, 2011 Ill. App. LEXIS 1181 (2011).
[8] *Id* at 393.
[9] Sewali K. Patel, *Note: Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*55 Vand. L. Rev. 647, 651 (2002).
[10] 47 USC Section 230 (2020).
[11] Zeran v America Online, 958 F. Supp. 1124 (E.D. Va., 1997).
[12] Schneider v Amazon.com, Inc., 108 Wn. App. 454, 31 P.3d 37, 2001 Wash. App. LEXIS 2086 (2001).
[13] *Id* at 460.
[14] Blumenthal v Drudge, 992 F. Supp. 44 (D.C., 1998).
[15] Ben Ezra, Weinstein, & Co. v America Online, Inc., 206 F. 3d 980 (10th Cir., 2000).
[16] Reit v Yelp!, Inc., 29 Misc. 3d 713, 907 N.Y.S 2d 411, 2010 N.Y. Misc. LEXIS 4259 (2010).
[17] Klayman v Zuckerberg, 753 F. 3d 1354 (2014).
[18] Carafano v Metrosplash, Inc., 339 F., 3d 1119 (9th Cir. 2002).
[19] Hy Cite, Corp. v Badbusinessbureau, 418 F. Supp. 2d 1142 (D. Az., 2005).
[20] John Doe No. 1 v Cahill, 884 A. 2d 451, 2005 Del. LEXIS 381 (2005).
[21] Dendrite Intl., Inc. v Doe No. 3, 342 N.J. Super. 134, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).
[22] John Doe No. 1, *supra* at 460.
[23] *Id*.
[24] Independent Newspapers, Inc. v Brodie, 407 Md. 415, 966 A.2d 432, 2009 Md. LEXIS 18 (2009).
[25] Columbia Insurance Company v Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).

[26] *Id* at 578-580.
[27] In Re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26 (2000).
[28] Maxon v Ottawa Publishing Company, *supra* at note 2.
[29] *Id* at 710.
[30] Yelp, Inc. v Hadeed Carpet Cleaning, Inc., 62 Va. App. 678, 752 S.E. 2d 554, 2014 Va. App. LEXIS 1 (2014).
[31] *Id* at 698.
[32] 17 U.S.C. Section 512 (2020).
[33] Facebook Terms of Service, https://www.facebook.com/terms.php (last visited July 15, 2020).
[34] Barnes v Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2008).
[35] Ryan Garcia & Thaddeus Hoffmeister, Social Media Law in a Nutshell, (2017).
[36] Palmer v Kleargear.com, no 13-cv-00175 (D. Utah filed Dec. 18, 2013).
[37] 15 U.S.C.. 45b (2020).
[38] California Civil Code § 1670.8 (2014).
[39] Ryan King, *Online Defamation: Bringing the Communications Decency Act of 1996 in Line with Sound Public Policy*, 2003 Duke L. & Tech. Rev. Volume: 2, Issue:1, pages 1-11.