

HOW TO DESTROY A REPUTATION AND GET AWAY WITH IT

THE COMMUNICATION DECENCY ACT EXAMINED: DO THE POLICIES AND STANDARDS SET OUT IN THE DIGITAL MILLENNIUM COPYRIGHT ACT PROVIDE A SOLUTION FOR A PERSON DEFAMED ONLINE?

DAVID E. HALLETT*

INTRODUCTION

Compare and contrast two different scenarios; one situation provides relief while the other does not. In the first scenario, a forty-year-old man, Bob, creates adult copyrighted pictures and sells them online. Bob finds out that an unknown individual is using his pornographic images on a website without his permission. He sends a simple letter to the unknown individual's Internet Service Provider ("ISP"), identifies himself, explains that he is the copyright owner of the pictures, and provides a description and the location of the infringing material. The ISP acts quickly to notify the unknown individual that it is removing the allegedly infringing material and provides

* The author completes his final year at California Western School of Law in April of 2002. He participates in the California Western Law Review/International Law Journal, the National Moot Court Competition, and Advocacy Honors Board oral competitions. The author would like to thank Jaime L. Earnest for her support and Professor Matthew Ritter for his encouragement.

an opportunity for that party to submit a counter notification. The material is removed, the ISP does not receive a counter notification, and Bob goes about his business producing and profiting from adult photographs sold online.

In the second scenario, another forty-year-old man, Paul, owns and runs the “Family Moral Store.” The business thrives through Internet sales and local clientele. An unknown person posts an anonymous statement on an Internet bulletin board exposing Paul as a convicted child molester and thief. Paul, however, has never molested a child nor stolen anything in his life. As a result of these statements, business halts at the “Family Moral Store.” Paul’s local supporters disavow him, and he receives disparaging phone calls at his business every three minutes. He explains the situation to the ISP in a letter asking them to remove the material, but the ISP ignores his request. The “Family Moral Store” is on the verge of bankruptcy and concerned citizens run Paul out of town. Paul sends another explanatory letter to the ISP and they remove the statement. Within one day, however, another message is posted with an even more descriptive account of what Paul did to young children. Paul sends ten more letters to the ISP but his requests are ignored. Paul brings suit. By this time, the “Family Moral Store” has shut down, and Paul is forced to relocate out of fear for his life. Paul loses his case. The court holds that it was not the ISP’s responsibility to remove the defamatory statement.

Is this fair? Do these two scenarios follow our traditional ideas of justice? NO. This is exactly the situation Congress created for defamed plaintiffs. A defamed plaintiff has no recourse except to try and find some unknown party who originated the statement; yet, a porn producer has their monetary interest protected. This is the situation Congress implemented when they enacted the Communication Decency Act (“CDA”) and the Digital Millennium Copyright Act (“DMCA”).

The ramifications of certain provisions of the DMCA and the CDA will be compared and contrasted. The rationale as to why both acts were originally implemented and the purpose and policy behind each will also be addressed. The policy behind the CDA is to promote Internet growth by allowing Internet Service Providers (“ISPs”) to avoid liability. The problem is that the CDA does not provide a remedy for an injured plaintiff. The plaintiff cannot sue the original posting party because that person is usually unknown and cannot be located. As a result, an injured plaintiff cannot seek damages from anybody other than the ISP. The policy behind the CDA is ideal but can be accomplished in a more equitable fashion. Congress should amend the CDA to overcome judicial interpretation by including provisions like those in the DMCA or the courts should change their interpretation of the CDA. Specifically, the CDA needs to include secondary liability

sections like those in the DMCA. These sections require the ISP to take action following notice and such a requirement will foster the original policy concerns of the CDA. Such changes will further promote Internet growth by removing the burden placed on the ISP, avoid lawsuits by limiting liability when certain steps are followed, and most importantly, provide immediate recourse to an injured individual by removing the defamatory material.

First, the provisions of the DMCA, the applicable case law, and aspects of individual provisions are addressed and discussed. Secondly, the CDA is examined and shortcomings fashioned by case law are addressed. The rationale and policy of both the DMCA and the CDA reveals that both acts sought to promote Internet growth by alleviating the burden on ISPs. In conclusion, this article will explain why the provisions of the DMCA provide a feasible solution that will support technological growth as well as provide recourse for a defamed individual.

I. DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

A. Background

The Digital Millennium Copyright Act (“DMCA”) was implemented, in part, to create additions to United States law in order to comply with ratified treaties.¹ In particular, the DMCA, along with several others, was created in furtherance of the World Intellectual Property Organization Copyright Treaties Implementation Act.² In December of 1996 a conference convened in Geneva, Switzerland to negotiate treaties to globally protect copyrighted material in the technical arena.³ Section 512 of the DMCA,⁴ referred to as the On-Line Copyright Infringement Liability Limitation Act (“OCILLA”) provides greater certainty in determining when an ISP will be liable for copyright infringement.⁵

¹ Melville Nimmer & David Nimmer, *Nimmer on Copyright* vol. 10, app. 5, 9 (Matthew Bender & Co., Inc. 2000).

² *Id.*

³ *Id.* The technical arena that was to be protected included, among other things, international protection to performers and producers of phonograms, protection of American records, tapes, and compact discs. *Id.*

⁴ *Limitations on Liability Relating to Material Online*, 17 U.S.C. § 512 (Supp. 1999).

⁵ *Id.* at 11.

B. Copyright in the Digital Medium

Copyright is a property right in an original work fixed in a tangible medium of expression.⁶ “Copyrights protect the expression of ideas and thoughts. Copyrights do not protect ideas or facts.”⁷ Moreover, “[c]opyright protection extends to electronically published works, whether they be completely original, new works, or compilations of existing works, such as databases.”⁸ A copyright violation can occur when pictures or films are modified with digitization, colorization, or other editing, when information is downloaded from one computer to another, or when information, such as messages, are transmitted over an online medium.⁹ These protected works also include compilations, which are creations of an original work that are pieced together from preexisting material or data. Technological innovations make such creations easily accessible, which has in turn increased cases involving copyrighted materials in “derivative works.”¹⁰ Compression and decompression technology is another innovation that is currently reeking havoc on the music and entertainment industry.¹¹ The profound effects of the DMCA in the music arena, however, will not be further addressed.

OCILLA assumes that somebody has violated a copyright. The issue then becomes when and if the ISP will be liable. OCILLA contains different definitions for an ISP. ISP typically refers to a broader definition, which will encompass all providers entailed in the narrower definition. Under the broad definition, a service provider¹² “means a provider of online services or network access, or the operator of facilities . . .”¹³ The narrower definition states that a service provider “means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points *specified by the user, of material of the user’s*

⁶ *Black’s Law Dictionary* 337-38 (Bryan A. Garner ed., 7th ed., West 1999); see also 17 U.S.C. § 102(a) (1994) (providing the prerequisites for obtaining copyright protection).

⁷ Cameron R. Graham & Matt Zinn, *Cable On-Line Services*, 822 (PLI Pat., Copy., Trademarks, & Literary Prop. Course Handbook Series No. G0-00E9, 2000).

⁸ E. Gabriel Perle, John Taylor Williams & Mark A. Fischer, *Electronic Publishing and Software*, Part II, 17 No. 2 Computer L. 15, 17 (2000).

⁹ Graham & Zinn, *supra* n. 7, at 822-23.

¹⁰ Perle, Williams & Fischer, *supra* n. 8, at 17; see also 17 U.S.C. § 101 (1994) (providing the definition of a compilation).

¹¹ *Id.*

¹² Note throughout this paper ISP is used synonymously with “service provider.”

¹³ 17 U.S.C. § 512(k)(1)(B).

choosing, without modification to the content of the material as sent or received.”¹⁴ These definitions differentiate between the liability aspects for direct infringement and those imposed for contributory/secondary infringement. These distinctions will be explored in greater detail below.

C. Section 512 of the DMCA (OCILLA)

Although traditionally copyright infringement is a strict liability standard,¹⁵ the DMCA provides a safe harbor for ISPs under certain circumstances.¹⁶ As discussed above, the DMCA differentiates between direct infringement and contributory infringement.¹⁷

1. Direct Infringement

The narrower definition,¹⁸ under OCILLA, provides the ISP with an absolute bar from liability¹⁹ if:

- (1) a third party initiated transmission of the material;
- (2) this transmission is carried out by an automatic technical process;
- (3) the recipients of the material were not selected by the service provider;
- (4) no copy is maintained by the service provider that is accessible to anyone other than the intended recipients and the copy for the intended recipient is only maintained for a reasonable period of time; and
- (5) the material is transmitted without modification.²⁰

¹⁴ 17 U.S.C. § 512(k)(1)(A) (emphasis added).

¹⁵ Perle, Williams & Fischer, *supra* n. 8, at 19.

¹⁶ *Id.* at 20.

¹⁷ *See generally* 17 U.S.C. § 512.

¹⁸ Direct infringement is the only section of the Act that uses the narrower definition laid out in 17 U.S.C. § 512. *Id.* § 512(k)(1)(a). This narrower definition basically encompasses this section of the act by saying that a service provider is an entity that provides unmodified transmission of material, as specified by the user, to whomever the user requests. *Id.*

¹⁹ This is an absolute bar for monetary damages. *Id.* at § 512(a). In each of the cases discussed, under certain circumstances the party that has been infringed upon may still have injunctive or equitable relief. *Id.*

²⁰ 17 U.S.C. § 512(a). Section (a) entails transmission to recipients at the request of the third party, whereas, § (b) discusses system caching. *Id.* § 512 (a), (b). Under Section

This definition creates an absolute bar from liability if the service provider only provides the service of transferring material at the request of one of its subscribers. In *Playboy Enters., Inc. v. Frena*,²¹ the District Court for the Middle District of Florida held that an ISP could be liable for direct infringement regardless of their knowledge of the infringing activity.²² The District Court for the Northern District of California disagreed in *Religious Tech. Ctr. v. Netcom On-Line Commun. Services, Inc.*²³ In *Netcom*, the court held that direct liability was not the appropriate standard, but that an ISP could be liable for contributory infringement if they had actual or constructive knowledge of the infringing activity.²⁴ *Netcom* ultimately became the standard codified in OCILLA.²⁵ The basis behind making sure an ISP was not considered the publisher and thus creating a “safe harbor” from direct liability was that the ISP, without censoring every single message, would have no idea what the content of the message contained.²⁶ Nor would the ISP provide access to the material for anybody other than the specifically

(b) the bar from liability is exactly the same except this entails transferring the information from an infringing third party or other service provider at the request of the recipient. *Id.* Usually, this also entails maintaining information of the site on their system, essentially a copy to make the material available faster to their users. As long as certain conditions are meant, e.g. no modifications by the ISP and the ISP complies with rules regarding updates and refreshing, etc. the ISP may avoid liability. *Id.* § 512(b)(2). The most important difference is that under Section (b) for the ISP to avoid liability they must remove or disable access to the infringing material, upon notice, if the material had been previously removed/disabled or a Court has ordered that access to the infringing site be barred and the party notifying the ISP of the infringing activity provides a statement that the above has occurred. *Id.* § 512(b)(2)(E). Thus, this section basically is contributory infringement that originates and is requested by third parties and the service provider merely provides access, but only at the request of a third party.

²¹ 839 F. Supp. 1552, 29 U.S.P.Q.2d 1827 (M.D. Fla. 1993).

²² *Id.* at 1556, 29 U.S.P.Q.2d at 1831 (upholding a strict liability standard for direct copyright infringement).

²³ 907 F. Supp 1361, 1370-71, 37 U.S.P.Q.2d 1545, 1552 (N.D. Cal. 1995).

²⁴ *Netcom*, 907 F. Supp. at 1383, 37 U.S.P.Q.2d at 1562 (stating that “the only viable theory of infringement is contributory infringement”); see also Linda A. Goldstein, *Emerging Issues in Online Advertising and Promotion Law*, 855-56 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-0090, 1999) (explaining that *Netcom* essentially changed the scheme from a direct infringement standard to a contributory standard); see also Karen S. Frank, *Cable Online Liability*, 259-61 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-003A, 1999).

²⁵ Nimmer & Nimmer, *supra* n. 1, at 11.

²⁶ *Id.* at 24-25.

requested recipients.²⁷ As the sheer magnitude of monitoring and censoring each and every message on an ISP would be near impossible, the only reasonable solution for infringement of this nature, as discussed in *Netcom*,²⁸ is a contributory liability scheme.²⁹ It is important, however, to note that OCILLA only provides an absolute bar from liability if the ISP does not interject any control of the transmission and selection process.³⁰ *Playboy Enters., Inc. v. Webbworld, Inc.*³¹ and *Playboy Enters., Inc. v. Russ Hardenburgh, Inc.*³² decided prior to the enactment of the DMCA, held that if an ISP took affirmative steps or exercised control over the copyrighted material, then the ISP could be held directly liable.³³

2. Contributory Infringement

Contributory infringement occurs when the ISP has some type of interaction other than transmission.³⁴ In this situation, the ISP maintains information on their systems at the request of a user or provides access to users by referring or linking them to the offensive material.³⁵ Under these

²⁷ *Id.*

²⁸ *Netcom*, 907 F. Supp. at 1373-75, 37 U.S.P.Q.2d at 1554-56.

²⁹ *Id.* at 1383, 37 U.S.P.Q.2d at 1562.

³⁰ 17 U.S.C. § 512(a), (b).

³¹ 991 F. Supp. 543, 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

³² 839 F. Supp. 1552, 29 U.S.P.Q.2d 1827 (M.D. Fla. 1993).

³³ *See Playboy Enters., Inc. v. Webbworld, Inc.*, 991 F. Supp 543, 552, 45 U.S.P.Q.2d 1641, 1647 (N.D. Tex. 1997) (holding that where a company took “affirmative steps to cause the copies to be made” and, in essence, “exercised total dominion [and control] over the content” of their site then they are directly liable); *see also Playboy Enters., Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 512-13 (N.D. Ohio 1997) (holding that encouraging or facilitating activities and setting up a computer bulletin board is not the same as actually infringing but a defendant is directly liable when the defendant encourages the uploading of material, screens that material, selects and moves that material onto their site).

³⁴ *See generally Netcom*, 907 F. Supp. at 1373-75, 37 U.S.P.Q.2d at 1554-56 (discussing ISP’s role and possible contributory infringement status); *see also Nimmer & Nimmer, supra* n. 1, at 24.

³⁵ *See generally* 17 U.S.C. § 512(c), (d). These sections specifically address when information resides on an ISP’s system at the request of a user and when the ISP provides “Information Location Tools”. *Id.*

circumstances the ISP will not be liable for monetary damages³⁶ provided that the ISP:

- (1) does not have knowledge, which can be found in three circumstances:
 - (a) “does not have actual knowledge that the material or activity is infringing,” or
 - (b) “in the absence of ... actual knowledge, is not aware of [any] facts or circumstances from which the infringing activity is apparent”, or
 - (c) upon obtaining such knowledge, acts expeditiously to remove/disable access
- (2) “does not receive a financial benefit directly attributable to the infringing activity, in a case [where the ISP] has the right and ability to control [the] activity,”
- (3) upon notice, acts expeditiously to remove/disable access to the infringing material.³⁷

Thus under the scheme of contributory infringement,³⁸ once an ISP has notice of an infringing act they will be liable unless certain action is taken.

II. NOTICE

To constitute effective notice warranting action by the ISP, the notice must be *written* and *substantially* include:

- (1) the physical or electronic signature of someone authorized to act on behalf of the copyright owner;
- (2) the identification of the copyrighted work or if multiple infringing works a representative list of such works;

³⁶ See *supra* n. 22 (discussing a complete bar for monetary damages, but an injured party may still have equitable relief).

³⁷ 17 U.S.C. § 512(c)(1), (d).

³⁸ See *supra* n. 20. This note describes that system caching fits under the contributory negligence scheme. However, it was discussed under the direct infringement scheme because the main difference is that it originated and was requested by someone other than the ISP. As a result, liability was barred because the ISP only participated in transmission. Section (b) of OCILLA, however, does fit in the contributory infringement scheme because the ISP is providing the access but the bar is higher to find liability because the notice must also show that the material had been previously removed from the original site (only now stored on the ISP’s server) or that a court had ordered removal/disablement of access to the material and/or originating site.

- (3) the identification of the material that is infringing and information that is reasonably sufficient for the ISP to locate that material;
- (4) the information reasonably sufficient to permit the ISP to contact the complaining party;
- (5) a statement that the complaining party believes in good faith that the alleged material is infringing; and
- (6) a statement, under penalty of perjury, that the information provided by the complaining party is accurate.³⁹

For the first time, the Fourth Circuit addressed, in *ALS Scan, Inc. v. Remarq Communities, Inc.*,⁴⁰ whether an ISP can be liable given an imperfect notice.⁴¹ In *ALS Scan*, the appellant alleged that Remarq, an ISP provider, was liable for damages because Remarq failed to remove infringing sites following notification.⁴² The letter sent by ALS Scan to Remarq indicated that two newsgroups, “alt.als” and “alt.binaries.pictures.erotica.als,” were created to infringe on ALS Scan’s pictures, as evidenced by the “.als” in both newsgroups.⁴³ ALS Scan requested that Remarq “cease and desist” use of the two newsgroups.⁴⁴ The court recognized that the contributory infringement sections in OCILLA govern the issue.⁴⁵ Further, the court stated that the primary issue is knowledge of infringement.⁴⁶

There are three ways to establish knowledge: actual, apparent, or becomes aware; following each, the ISP then has to remove.⁴⁷ ALS Scan argued that to require strict compliance to the notice requirements of OCILLA provides an ISP with more protection than granted by Congress.⁴⁸ The Fourth Circuit ultimately held that once an ISP is put on some notice

³⁹ 17 U.S.C. § 512(c)(3)(A).

⁴⁰ 239 F.3d 619, 57 U.S.P.Q.2d 1996 (4th Cir. 2001).

⁴¹ *Id.* at 620, 57 U.S.P.Q.2d at 1997.

⁴² *Id.* at 621, 57 U.S.P.Q.2d at 1998.

⁴³ *Id.* at 620, 57 U.S.P.Q.2d at 1997.

⁴⁴ *Id.* at 620-21, 57 U.S.P.Q.2d at 1997-98.

⁴⁵ This is evident by the *ALS Scan* court stating that this situation is governed by the “broader” definition of a “service provider.” *Id.* at 623, 57 U.S.P.Q.2d at 1999. This broad definition encompasses all of the secondary infringement situations. *Id.* at 623, 57 U.S.P.Q.2d at 1999.

⁴⁶ *Id.* at 622-25, 57 U.S.P.Q.2d at 1999-2001 (discussing that knowledge of infringement is a key element in the safe harbor immunity defense).

⁴⁷ 17 U.S.C. § 512(c)(1).

⁴⁸ *ALS Scan*, 239 F.3d at 622, 57 U.S.P.Q.2d at 1999.

relating to infringing material, the ISP loses its “innocence” and the burden shifts to the ISP to detect and deal with any copyright infringement.⁴⁹ Ultimately, the court decided that the substantial requirements are less stringent when multiple works are being copyrighted and that here the notice was reasonably sufficient to allow the ISP to locate the infringing material.⁵⁰ As such, the court found for ALS Scan, reversing and remanding the case.⁵¹ As a result, according to the Fourth Circuit, the substantial compliance language in OCILLA actually provides for a liberal construction of the language required in a notice. Thus, any notice that makes it reasonable for an ISP to locate any infringing material puts the burden on the ISP to take further action in order to avoid liability.

The Fourth Circuit decision appears to contradict certain provisions in OCILLA. OCILLA specifically states that if notice does not substantially comply with the requirements, then it “*shall not be considered*” on whether the ISP had actual, apparent, or became aware that the activity was infringing which in turn requires the ISP to take action.⁵² It seems that the court may have over shadowed Congress’ intent when saying that notice in *ALS Scan* was sufficient to show that Remarq became aware of the infringement and was required to remove the material. *ALS Scan* was a case of first impression and therefore, a high probability exists that other circuits will disagree with this decision.

A. *No Liability for the ISP for Good Faith Removal*

Generally an ISP will not be liable if it removes access to material that it believes, in good faith, may be infringing, *regardless* of whether it is actually infringing.⁵³ The ISP will be exempt from liability if:

- (1) the ISP takes reasonable steps to notify the alleged infringing party of the removal;
- (2) the ISP receives a counter notification, it informs the original complaining party that it will repost the material in no less than 10 business days and does repost *unless* within the 10 days the

⁴⁹ *Id.* at 625, 57 U.S.P.Q.2d at 2001.

⁵⁰ *Id.* at 625, 57 U.S.P.Q.2d at 2001-02.

⁵¹ *Id.* at 625-26, 57 U.S.P.Q.2d at 2002.

⁵² 17 U.S.C. § 512(c)(3)(B) (emphasis added).

⁵³ 17 U.S.C. § 512(g)(1).

ISP receives notice that the original complaining party has filed an infringing lawsuit related to that material.⁵⁴

The ISP will not be liable for removing any material that they believe in good faith may be infringing. The ISP will avoid liability as long as they attempt to contact the infringing party and do not receive a counter notification.

B. Counter Notification

The ISP must enable access to an allegedly infringing site if the ISP receives a counter notification.⁵⁵ This notification must be in writing and include substantially the following:

- (1) “physical or electronic signature of the subscriber”;
- (2) identification of the removed material and the location prior to removal;
- (3) “a statement under penalty of perjury that the subscriber” believes the information was removed as a result of a mistake; and
- (4) subscriber’s personal information and a location where he will accept service of process.⁵⁶

This counter notification is fairly similar to the requirements of the original notification provided by the complaining party. Courts have not interpreted the “substantial” compliance section of this notice. It would appear that there is a greater necessity for the material to be thorough and accurate because of the likelihood that a lawsuit will result if the material is reposted.

C. Designated Agent

In order for the ISP to avoid liability under the contributory scheme, it must also have a “designated agent” available to obtain the necessary notices.⁵⁷ The ISP must make available, through its website and with the

⁵⁶ 17 U.S.C. § 512(g)(2). This section essentially absolves the ISP from making any legal judgments on the material, it must simply follow a laid out process. It also alleviates First Amendment concerns because it gives immediate recourse to the originating party.

⁵⁵ See generally 17 U.S.C. § 512(g)(3) (1998).

⁵⁶ *Id.*

⁵⁷ 17 U.S.C. § 512(c)(2).

Copyright Office, information regarding the designated agent for the ISP.⁵⁸ This information, accessible to the public, must contain:

- (1) name, address, phone number, and electronic mail address of the agent; and
- (2) any other relevant contact information the Office of Copyright deems important.⁵⁹

Therefore, any complaining party, that is most likely not a subscriber to the service, will have a way to find out how to contact the ISP and complain about an allegedly infringing site.

D. Policy

The legislation specifically states that the OCILLA is not intended to discourage ISPs from monitoring their service for infringing material.⁶⁰ OCILLA is clear that once an ISP becomes aware of an infringing activity, it must take action. The larger policy concerns include implications on the First Amendment and the possibility of hindering Internet growth. First Amendment issues exist when an ISP makes a judgment call to remove allegedly infringing material without any research, this in turn may severely limit an internet communicators right to free speech. If the ISP, however, does the research on each piece of material to find out if it violates a copyright the cost would be enormous and ISPs would no longer be able to operate in a cost efficient fashion.

OCILLA tries to create a balance by allowing the ISP to remove material without liability if they receive notice from someone who alleges infringement. Likewise the original posting party will be able to prevent the item from being removed if they provide a counter notification. As a result, OCILLA specifically creates a balance between the rights of a copyright owner and the posters right to free speech in a fashion that the cost and liability to an ISP are limited. The legislature has done a fairly good job at maintaining this balance in the case of copyright infringement but has failed to exercise the same good judgment in the CDA.

⁵⁸ *Id.*

⁵⁹ 17 U.S.C. § 512(c)(2) (A), (B).

⁶⁰ H.R. Conf. Rep. 105-796 at 72 (October 8, 1998) (reprinted in 1998 U.S.C.C.A.N. 649).

III. THE COMMUNICATION DECENCY ACT

A. Background

Defamation, by definition, is “the act of harming the reputation of another by making a false statement to a third person.”⁶¹ A defamation claim contains the following main elements: “false statement, referring to the plaintiff, published to one or more third parties, [and] causing damage to the plaintiff.”⁶² Section 230 of the Communication Decency Act (“CDA”) was created to limit liability when a third person posted a defamatory message through an Internet Service Provider (“ISP”).⁶³ The two leading Internet defamation cases set the stage for this enactment.⁶⁴ In *Cubby, Inc. v. CompuServe Inc.*,⁶⁵ the District Court for the Southern District of New York held that an ISP could not be considered a “publisher” of material created by a third party⁶⁶ and could only be found to be a “distributor” of the material if it had actual knowledge that the statements were defamatory.⁶⁷ Further in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,⁶⁸ the Supreme Court of New York held that Prodigy, an ISP, was a “publisher” because it portrayed itself as such and actively controlled the content of material posted via an

⁶¹ *Black's Law Dictionary* 427 (Bryan A. Garner ed., 7th ed., West 1999).

⁶² Karen S. Frank, *Cable Online Liability*, 267 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-003A, 1999).

⁶³ *See generally* 47 U.S.C. § 230 (Supp. 1999).

⁶⁴ *See* Jeffrey P. Cunrad et al., *Selected Topics in Internet and E-commerce Law*, 424 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-00BB, 2000); *see also* Frank, *supra* n. 64, at 270-72, *see also* Kenny Silverman, *Defamation on the Internet*, 338-40 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-00DV, 2000); *see also* Barry J. Waldman, *A Unified Approach to Cyber-Libel: Defamation on the Internet, A Suggested Approach*, 6 Rich. J.L. & Tech. 9, 30-42 (1999); *see also* Joseph P. Zammit & Felicia Gross, *Web Site Liability: Risks and Costs of Compliance*, 894-96 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-00D6, 2000).

⁶⁵ 776 F. Supp. 135 (S.D.N.Y. 1991).

⁶⁶ *Id.* at 140 (indicating that the ISP was not a publisher because it was more like a library or book store in that it offers the material but has no editorial control over the material).

⁶⁷ *Id.* at 139-41 (indicating that actual knowledge is required for distributor liability so there is not an impingement of a persons freedom of speech under the First Amendment).

⁶⁸ 1995 N.Y. Misc. LEXIS 229 (1995).

automatic screening program.⁶⁹ These two cases lead to a “bizarre conclusion” because ISPs were provided with a disincentive to remove offensive material from their servers.⁷⁰

Basically without a monitoring process an ISP would not be liable, absent actual knowledge, because it was acting passively, merely as a distributor.⁷¹ On the other hand, an ISP could be liable as a publisher if it took voluntary action to remove harmful and offensive material from its server.⁷² In response to the *Stratton Oakmont* decision, Congress created Section 230 of the CDA to overrule this precedent.⁷³

B. The Act

Section 230(c), labeled the “good Samaritan,” of the CDA states that:

- (1) 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) 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).⁷⁴

⁶⁹ *Id.* at *10. It is interesting to note that the court stated that although this conscious choice of editorial consent created greater liability, this increase in liability would be compensated by the market place where parents would be willing to pay more for a family ISP. *Id.* at *13.

⁷⁰ Kenny Silverman, *Defamation on the Internet*, 338 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-00DV, 2000).

⁷¹ *Id.*

⁷² *Id.*

⁷³ Jeffrey P. Cunard, et al., *Selected Topics in Internet and E-commerce Law*, 425 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-00BB, 2000) (citing H.R. Conf. Rpt. 104-458, at 194 (Jan. 31, 1996)).

⁷⁴ 47 U.S.C. § 230(c) (1996).

According to the CDA, an interactive computer service⁷⁵ is “. . . 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.”⁷⁶

C. Policy

The CDA indicates that the Internet is an excellent medium for intellectual, cultural, technological, and educational advances.⁷⁷ Furthermore, the Internet has benefited all Americans and grown with minimal governmental regulation.⁷⁸ As a result, Section 230 of the CDA was created to support the continued development and growth of the Internet and the development of technological innovations.⁷⁹ Furthermore, in an effort to maximize user control, Congress specifically intended to remove disincentives of technological innovations, which allow parents to restrict access of the Internet and also to support the enforcement of criminal laws that prohibit trafficking of obscene materials.⁸⁰

In essence, the CDA was designed to support the growth of internet technologies by limiting the liability of those who provide access to the Internet.⁸¹ Thus, the legislature wanted to keep costs of the service down⁸² so

⁷⁵ Note throughout the remainder of this paper ISP is used synonymously with “interactive computer service.”

⁷⁶ 47 U.S.C. § 230(f)(2).

⁷⁷ *Id.* § 230(a).

⁷⁸ *Id.* § 230(a)(4).

⁷⁹ *Id.* § 230(b).

⁸⁰ *Id.* § 230 (b)(3)-(5).

⁸¹ See generally 47 U.S.C. § 230; see also *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (stating that “Section 230 was enacted, in part, to maintain the robust nature of internet communication.”); see also David E. Shipley, *Liability Issues Facing Online Businesses*, 36 Ark. L. Rev. 20, 24 (2001) (explaining that although libel on the internet may damage internet users, imposing liability on ISPs would be even more damaging to the Internet and may also result in limiting free speech).

⁸² *Zeran*, 129 F.3d at 330 (indicating that Congress’ intent was “to preserve the vibrant and competitive free market that presently exists for the Internet”—without government intervention.)

that the Internet could continue to expand and become available for all Americans.⁸³

D. Practical Effect

The CDA statutorily limits ISP liability by making it impossible to find an essential element of the claim, publication.⁸⁴ *Zeran v. American Online, Inc.*⁸⁵ established that Section 230 of the CDA provided an absolute bar from liability for both “publisher” and “distributor”⁸⁶ liability.⁸⁷ In *Zeran*, the Fourth Circuit held that the ISP was not even liable after *Zeran* had provided notice to the provider of the defamatory material.⁸⁸ The broad nature of Section 230 as explained in *Zeran* expanded to an even greater limit in *Blumenthal v. Drudge*.⁸⁹ In *Drudge*, the District Court for the District of Columbia held that even though the ISP had a contract for the posting with the originating party, the ISP will not be liable even though the ISP was able to decide whether to publish or alter the material.⁹⁰

⁸³ See generally 47 U.S.C. § 230.

⁸⁴ 47 U.S.C. § 230 (c)(1) (This section essentially states that an ISP will never be considered a publisher or speaker of material that originated from a third party); see also Frank, *supra* n. 62, at 273 (stating that the CDA effectively precludes finding a publication).

⁸⁵ 129 F.3d 327 (4th Cir. 1997).

⁸⁶ Traditionally a distributor, like a newspaper vendor or bookstore, could be held liable if they had actual knowledge of the defamatory material. See *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp 135, 139-42 (S.D.N.Y. 1991).

⁸⁷ *Zeran*, 129 F.3d at 332 (explaining that because “distributor” liability is just a subspecies of publisher liability, that the act, as worded, specifically excludes an ISP from any liability, whether it be distributor or publisher liability).

⁸⁸ *Id.* at 332-33. (explaining that notice based liability would create greater liability for an ISP because any efforts to regulate and monitor offensive material would theoretically give the ISP notice; more importantly, the magnitude of volume on an ISP would create an impossible burden to research each item that someone complained about and also impinge on free speech because an ISP could just remove any complained of material and avoid liability under Section 230 of the CDA).

⁸⁹ See generally 992 F. Supp. 44 (D.D.C. 1998).

⁹⁰ *Id.* at 50-53 (explaining that because the ISP did not provide any editorial comments in the actual writing of the article, it was not liable); see also John F. Delaney & William I. Schwartz, *The Law of the Internet: A Summary of U.S. Internet Case Law and Legal Developments*, 184-85 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-00A2, 2000) (providing a thorough analysis of the *Drudge* case and explaining that the court obviously made a strong policy decision when making the only remedy to an injured plaintiff a suit directly against the originating party.)

The *Zeran* and *Drudge* decisions set a strong precedent for absolving ISPs from any and all liability for defamatory statements regardless of either notice or editorial control.⁹¹ The blanket immunity set out in these two cases, however, is not entirely certain because these are only two jurisdictions.⁹² This bar from liability may still go too far, however, the risks of imposing liability are great because it is difficult to determine the detrimental impact on free speech.⁹³ Thus far, case law interpreting the CDA leaves no deep pockets for injured plaintiffs to sue; they can only sue the, often unknown, originating third party.⁹⁴

IV. RECONCILING THE DIFFERENCES AMONG THE DMCA AND CDA

A. Similarities

Both the Communication Decency Act (“CDA”) and the Digital Millennium Copyright Act (“DMCA”) appear to use broad definitions when referring to “ISPs.”⁹⁵ Although the CDA uses the term “interactive computer service”⁹⁶ and the DMCA uses the term “service providers”⁹⁷ these two terms are used broadly. Congressional intent, in both of these acts, was to use broad definitions when referring to ISPs in order for the statutes to evolve with changing technological developments.⁹⁸ Otherwise, a precise definition would be continually outdated.⁹⁹ As a result, the differences in definitions between the two acts are relatively minor and both encompass a generically defined ISP.

⁹¹ See *Zeran*, *supra* nn. 87-88; see also *Blumenthal*, 992 F. Supp 44 (D.D.C. 1998).

⁹² Linda A. Goldstein, *Emerging Issues in Online Advertising and Promotion Law*, 854 (PLI Pat., Copy., Trademarks & Literary Prop. Course Handbook Series No. G0-0090, 1999).

⁹³ David E. Shipley, *Liability Issues Facing Online Businesses*, 36 Ark. L. Rev. 20, 24 (2001).

⁹⁴ Lyrisa Barnett Lidsky, *Silencing John Doe: Defamation & Disclosure in Cyberspace*, 49 Duke L.J. 855, 871-72 (2000).

⁹⁵ Caitlin Garvey, *The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology*, 25 U. Dayton L. Rev. 133, 144 (1999).

⁹⁶ *Id.* at 138.

⁹⁷ *Id.*

⁹⁸ *Id.* at 144.

⁹⁹ *Id.*

More importantly, however, is that the policy goals and concerns addressed by the CDA and the DMCA are virtually identical.¹⁰⁰ Initially, Congress realized that the Internet was an extremely important medium of communication and the vision was that the Internet would continue to grow and expand in such a way that every American would benefit from the service.¹⁰¹ As a result, Congress intended to limit regulation so that Internet growth was not curtailed.¹⁰² Both the CDA and the DMCA accomplish this goal by limiting ISP liability. Another issue was the effect on the First Amendment, freedom of speech.¹⁰³ If Congress created liability, then ISPs would be forced to remove material that may or may not actually be infringing or defamatory. At the same time, however, Congress did not want to discourage ISPs from monitoring the content on their servers.¹⁰⁴ It is evident that Congress had very similar intentions when creating the CDA and the DMCA. Although the concerns were the same, Congress failed to balance these concerns in the CDA as effectively as it did in the DMCA.

B. Differences

The most important difference between the CDA and the DMCA is that the DMCA requires the ISP to act, in order to avoid liability, once the ISP receives notification of allegedly infringing material.¹⁰⁵ In a case of first impression, the Fourth Circuit recently indicated that the notice requirement need only substantially comply with the requirements of the statute.¹⁰⁶ The CDA requires no such action.¹⁰⁷ In fact, case law regarding the CDA specifically indicates that an ISP is not required to do anything—even after receiving notification.¹⁰⁸ Under the CDA, the ISP has the choice and can

¹⁰⁰ See *supra* Parts II.D, III.C.

¹⁰¹ See *supra* Parts II.D, III.C.

¹⁰² See *supra* Part III.C.

¹⁰³ See *supra* Part II.D.

¹⁰⁴ See *supra* Part II.D.

¹⁰⁵ See generally 17 U.S.C. § 512 (1998).

¹⁰⁶ See *ALS Scan Inc. v. Remarq Communities, Inc.*, 239 F.3d 619, 624-25, 57 U.S.P.Q.2d 1996, 2000-02 (4th Cir. 2001) (holding that a notice requirement lacking an exact description of all the infringing material will be sufficient if it reasonably informs the ISP of the material and its location); see also *supra* Part II.

¹⁰⁷ See generally 47 U.S.C. § 230.

¹⁰⁸ See *Zeran*, 129 F.3d at 332.

either ignore any requests¹⁰⁹ or can remove the material without exposing itself to liability.¹¹⁰

In addition, the DMCA provides for an agent¹¹¹ to receive this material and provides for a counter notification process.¹¹² This counter notification process allows the original posting party to respond to the ISP and explain that the material is non-infringing and at that point, the ISP is able to re-post the material barring notice from the complaining parties that they are going to file suit.¹¹³

C. *Reconciling the Differences*

The CDA does not adequately protect society from would be online defamers. Using the Internet, on-line defamers can continually harass whomever they choose regardless of the consequences to the defamed person. This does not stand up to our ideals of justice and quite simply, is not fair. Online defamation of an individual occurs through the use of an ISP. Without access to the Internet, there would not be such an effective and cost efficient means to create a widely public defamatory message. In order to foster the ideals of tort liability, to return injured plaintiffs to their pre-injury capacity, the CDA must be either judicially or legislatively altered to allow notice based liability.

1. **Judicial Interpretation**

Although the courts in *Zeran*¹¹⁴ and *Blumenthal*¹¹⁵ concluded that Section 230 of the CDA is an absolute bar from liability regardless of whether the ISP is provided with notice¹¹⁶ or had some editorial discretion,¹¹⁷

¹⁰⁹ *Id.*

¹¹⁰ *See generally* 47 U.S.C. § 230(c)(2).

¹¹¹ *See supra* Part II.C.

¹¹² *See supra* Part II.B.

¹¹³ 17 U.S.C. § 512(g)(2)(B)(C) (1998).

¹¹⁴ 129 F.3d 327 (4th Cir. 1997).

¹¹⁵ 992 F. Supp. 44 (D.D.C. 1998).

¹¹⁶ *Zeran*, 129 F.3d at 332-33 (explaining that notice based liability would create greater liability for an ISP because any efforts to regulate and monitor offensive material would theoretically give the ISP notice; more importantly, the sheer magnitude of volume on an ISP would create an impossible burden to research each item that someone complained

these decisions can be judicially changed. In particular, *Zeran* needs to be distinguished and/or disagreed with in other jurisdictions. The Fourth Circuit in *Zeran* stated that an ISP should not be held to notice based liability because it would deter self-regulation, increase litigation,¹¹⁸ and responding to notices would provide an impossible burden¹¹⁹ on the ISP.¹²⁰ Following the creation of the DMCA, none of these contentions have merit.

First, the argument about increased litigation has no real basis. The ISP may be liable given notice but the plaintiff still has the burden of proving the elements of defamation. Furthermore, if the court instructed the ISP to act, in essence, like in the DMCA then no litigation would ensue except from the complaining party against the originating party. That is, if the court were to provide for a notice and counter notification process similar to the DMCA,¹²¹ then the ISP would not be brought into any suits unless it received notification and failed to act. This same rationale alleviates most of the burden on the ISP.

The majority of ISPs will already have a designated agent and procedures to deal with notification and counter notification in order to avoid liability under the DMCA. To apply a similar standard to defamation will not create any additional burden on the ISP. Furthermore, the First Amendment concerns will also be alleviated because the notice and counter notification standard takes the pressure off of the ISP. Once the ISP receives a proper notice, it will remove the defaming material unless it receives a counter notification. As a result, the originating party's speech will only be limited if it is in fact defamatory. Otherwise the originating party can simply provide a counter notification and let the complaining party take it to court to determine whether the statement is defamatory. This situation absolves the

about and also impinge on free speech because an ISP could just remove any complained of material and avoid liability under Section 230 of the CDA); *see also supra* Part IV.D.

¹¹⁷ *Blumenthal*, 992 F. Supp at 50 (explaining that because the ISP did not provide any editorial comments in the actual writing of the article it was not liable); *see also supra* Part IV.D.

¹¹⁸ The court argued that it would increase litigation because a third party could just provide notice whenever it was unhappy with what another party put online and provide itself with a basis for a future suit. *Zeran*, 129 F.3d at 333.

¹¹⁹ *Zeran*, 129 F.3d at 333 (stating the ISP would be put under an impossible burden because it would have to review all of these notices and make a determination on either suppressing controversial free speech or subjecting itself to liability).

¹²⁰ *Id.*

¹²¹ *See supra* Parts I.C, III.B.

ISP from all liability as long as it follows a relatively simple and time efficient process. As a result, the burden on the ISP would be minimal.

Last but not least, allowing this type of system would not affect an ISP's prerogative to self-regulate. Section 230 of the CDA, as written, already provides a complete bar from liability if the ISP chooses to censor its material.¹²² Theoretically, the problem would be that the ISP, rather than going through the notification and counter notification process would just remove the alleged defamatory material.¹²³ Arguably this would automatically shield the ISP from liability because its action would be covered under the "good Samaritan" self-regulation principle laid out in Section 230 of the CDA.

This argument, however, is weak. Section 230 of the CDA requires that the ISP censor and remove the material in "good faith."¹²⁴ This standard will be used in comparison with the ISP's normal operating procedures. If in fact, the ISP has a record of removing similar material from its site, then the ISP will be protected from liability. If, however, the ISP removed this material because it received notice from a complaining party, then removal without going through a counter notification process will not be in good faith. As a result, the ISP by failing to follow the process would subject itself to liability. As discussed above, the "good faith" requirement coupled with the notice and counter notification requirement will limit any prejudicial effect on the originating party's right to free speech. Quite simply, the originating party can provide a counter notification and the item will be re-posted unless the complaining party files suit.

2. Statutory Changes

Another way to bring about reform is for Congress to amend the CDA. Congress could simply change the CDA to encompass all of the notice and counter notification requirements as described in the DMCA. As discussed above, this change would not pose a risk to the success of the Internet, increase litigation or impose an unbearable burden upon the ISP. This method would be more preferable because Congress can specifically

¹²² 47 U.S.C. § 230(c)(2)(A)(B).

¹²³ There would be a greater incentive to just remove alleged defamatory material rather than copyright infringing material because either the ISP or its subscribers are profiting from the use of copyrighted images and it would be worth the time of the ISP to go through the process. The same is not true for defamatory material because it is not usually done to make a profit.

¹²⁴ 47 U.S.C. § 230(c)(2)(A).

layout the process, as detailed in the DMCA, in order to avoid confusion. Specifically, Congress could make a universal decision with a set pattern that the ISP needs to follow in order to avoid liability.

If this is the case, Congress will need to be more specific on what a notice shall contain. Congress should require that any notice be signed under penalty of perjury. Notice should also contain the individuals name and current mailing and e-mail address. In addition, notice *must* contain an *exact* copy of the alleged defamatory material with a *sworn* statement that the material is false. In addition, the complaining party must advise the ISP of the *exact* location of the alleged defamatory material and the date it was viewed. The CDA should specifically require that notice *must* comply with *all* of these requirements. This will avoid the complication and confusion, as addressed under the DMCA in *ALS Scan v. Remarq*,¹²⁵ regarding what type of notice can subject an ISP to liability.

V. RESPONSES TO OTHER SUGGESTIONS AND PROBLEMS

Barry Waldman, author of a recent cyber-libel article, posed an excellent solution. Mr. Waldman proposes that the ISP be liable if it actively edits the defamatory statement that it published.¹²⁶ Holding an ISP liable for active editing is in accordance with the CDA because once the ISP takes an active editing role it becomes the “co-author” and falls outside the CDA protection.¹²⁷ Furthermore, if the ISP takes an active role, then it is no longer acting in “good faith” as required by the statute.¹²⁸ Although the solution is one that will provide liability to an ISP, Mr. Waldman’s solution still will not provide the recourse necessary to protect a defamed individual. The defamed individual needs a way to effectively stop the defaming material; the only effective way to accomplish this is for the ISP to remove the material. The ISP has the ability and control to alleviate the problem. As a result, notice based liability with a counter notification process is the only solution that will overcome First Amendment problems, limit the burden on an ISP, and provide recourse for an injured plaintiff.

¹²⁵ See generally *ALS Scan*, 239 F.3d 619, 57 U.S.P.Q.2d 1996.

¹²⁶ Barry J. Waldman, *A Unified Approach to Cyber-libel: Defamation on the Internet, A Suggested Approach*, 6 Rich. J.L. & Tech. 9, 54 (1999).

¹²⁷ *Id.* at 54-55.

¹²⁸ *Id.* at 55.

The strongest argument against ISP liability is based on the sheer number of postings.¹²⁹ Thus, the number of postings makes it impossible for the ISP to investigate and make a legal judgment on each “notice” that it receives.¹³⁰ If the ISP were required to make a legal judgment, subjecting the ISP to liability, then there is no question that this would be an impossible burden on the ISP. As a result of Congress’ creative and innovative thinking in the DMCA, however, this is simply no longer the case.

The notice and counter notification process alleviates this responsibility from the ISP. The ISP would no longer have to make a legal judgment; it would simply follow the process laid out. The ISP would advise the originating parties of the removal and provide them the opportunity to provide a counter notification, upon receipt of a counter notification the ISP would simply advise the complaining party and re-post unless suit was filed. This simple process would require nothing more than a technical and repetitive response. All of the burden will be placed on the parties involved. Even with the commencement of court proceedings, the ISP will be absolved from all liability unless it chooses not to follow the notice and counter notification process.

CONCLUSION

Creating ISP liability hinders the growth of an important interactive tool. As a result, Congress created a way for ISP’s to avoid liability, yet, provide protection for a copyright owner. Congress was very successful in its endeavors demonstrated by the increase in ISPs. In fact, “[t]he total number of entities under the encompassing heading of “ISP” has grown from about 1500 in 1996 to more than 6500, and it is estimated that the number of ISPs will rise five-fold in five years.”¹³¹

The DMCA was created several years after the CDA, after Congress was able to appreciate the best way to limit the burden on an ISP and provide protection to those harmed. As a result, either Congress or the courts need to

¹²⁹ Mary K. Finn et al., *Policies Underlying Congressional Approval of Criminal and Civil Immunity for Interactive Computer Service Providers Under Provisions of the Communications Decency Act of 1996—Should E-Buyers Beware?*, 31 U. Toledo L. Rev. 347, 368 (2000).

¹³⁰ *Id.*

¹³¹ Caitlin Garvey, *The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology*, 25 U. Dayton L. Rev. 133, 137 (1999) (citing Seth Lubove & Anne Linsmayer, *Mom and Pops Thrive . . .*, *Forbes*, at 120 (Feb. 22, 1999)).

further examine Section 230 of the CDA and implement changes that will afford similar protection to a defamed individual.

Paul, the “Family Moral Store” owner, deserves the same right as Bob, the porn producer, to be protected from illegal online attacks. Legislative or judicial reforms need to re-evaluate the provisions of the CDA so that Paul can be protected from a vicious online attack that could possibly ruin his business and reputation. Congress already addressed the answer in the DMCA, now all that needs to be done is simply to apply these same principles to afford protection for a defamed individual.