

## I. INTRODUCTION

### I(a). BRIEF STATEMENT ABOUT THE STATE OF THE INTERNET AND INTERNET BUSINESS TODAY

“The Internet has given people the power to transmit and reproduce vast amounts of information, including copyrighted [material].”<sup>1</sup> For example, the ability of Internet users to automatically reproduce information through a network of interlinked computers has led to easy and inexpensive copyright infringement on a global scale.<sup>2</sup> In response, law making bodies and courts throughout the world are reevaluating laws and policies regarding all areas of law.<sup>3</sup> As a further complication, the global reach of the Internet has led to a myriad of laws and regulations, which lack consistency and provide little guidance for Internet Service Providers (ISPs) to prevent against defamation, censorship, intellectual property infringement, and crime detection.<sup>4</sup> Consequently, ISPs are faced with the enormous and impractical task of monitoring their subscribers’ activities, despite the immense amount of online traffic.<sup>5</sup> ISPs successfully argued that if they were held strictly liable for their subscribers’ online infringements, higher access fees would be placed on the subscribers to deflect the cost of liability.<sup>6</sup>

---

<sup>1</sup> Heidi Pearlman Salow, *Liability Immunity for Internet Service Providers—How Is It Working?*, 6 J. TECH. L. & POL’Y 1 (2001).

<sup>2</sup> *Id.*

<sup>3</sup> Michael Deturbide, *Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses*, J. INFO. L. TECH. Oct. 31, 2000 at [www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000\\_3/deturbide](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/deturbide).

<sup>4</sup> Posting of Manon Ress, [mress@essential.org](mailto:mress@essential.org), at <http://lists.essential.org/pipermail/hague-jur-commercial-law/2002-May/000605.html> (May 9, 2002).

<sup>5</sup> Salow, *supra* note 1; see also, Michelle A. Ravn, Note, *Navigating Terra Incognita: Why the Digital Millennium Copyright Act Was Needed to Chart the Course of Online Service Provider Liability for Copyright Infringement*, 60 OHIO ST. L.J. 755, 778 (1999).

<sup>6</sup> Salow, *supra* note 1; see also, On-Line Copyright Liability Limitation Act and WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2280 and H.R. 2281 Before the House Judiciary Committee, Courts and Intellectual Property Subcommittee, 105th Cong. (1997) (statement of Edward Black, President, Computer and Communications Industry Association) (“[s]ervice providers do not know, nor would we be capable of knowing, the billions of bits of information that we are transmitting over tens of thousands of lines.”).

## **I(b). DEFINITION OF INTERNET SERVICE PROVIDER**

“Internet Service Providers . . . provide Internet access service[s] to customers in exchange for a fee.”<sup>7</sup> Additionally, they provide a variety of services, including, inter alia, data-storage for their customers on newsgroup servers or World Wide Web servers.<sup>8</sup>

Traditionally, courts took the position that an Internet Service Provider was the equivalent of a “traditional telecommunications carrier.”<sup>9</sup> As a telecommunications carrier, ISPs were viewed as inactive conduits that allowed the transmission of information; because of the ISPs’ passive activity, they were not deemed to be responsible for the content of the transmitted data.<sup>10</sup> Therefore, courts reasoned that requiring ISPs to monitor every service provided to protect against criminal activity would not be justified, reasonable, or practical.<sup>11</sup> Courts often argued that placing such a large burden on ISPs “would adversely affect the free flowing nature of the Internet.”<sup>12</sup> More recently however, the ISPs’ “conduit immunity” has been attacked and chipped away by the courts.<sup>13</sup> The main reasoning behind this movement is the simple understanding that ISPs are the gateway to the Internet super highway; they are, therefore, in the best position to detect, block, and remove offensive or infringing material.<sup>14</sup> ISPs often find themselves liable for the activities of their customers when they have knowledge of their illegal activities.<sup>15</sup> Courts are reluctant to hold ISPs liable when their customers’ illegal activity is

---

<sup>7</sup> Brad Bolin & Daniel A. Tysver, *ISP Liability*, at <http://www.bitlaw.com/internet/isp.html> (last visited Jan. 17, 2004).

<sup>8</sup> *Id.*

<sup>9</sup> Martin J. Hayes, *Internet Service Provider Liability*, at [http://www.jisc.ac.uk/legal/index.cfm?name=lis\\_isp](http://www.jisc.ac.uk/legal/index.cfm?name=lis_isp) (last visited Jan. 24, 2004).

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> Hayes, *supra* note 9.

<sup>15</sup> Bolin & Tysver, *supra* note 7.

unknown.<sup>16</sup> However, once an ISP becomes aware, or should have become aware of its customers' activities, courts will then hold an ISP liable.<sup>17</sup>

Increasingly, ISPs find themselves named as defendants where customers have misused an ISPs' services because "of their visibility in the Internet scheme."<sup>18</sup> Several reasons exist why ISPs are often the defendant in defamation claims, most of which deal with high litigation costs.<sup>19</sup> Guilty customers or parties are often located outside the plaintiff's jurisdiction, thus, including the ISP as a party in the claim is one method of obtaining jurisdiction if the ISP is incorporated within the plaintiff's jurisdiction.<sup>20</sup> Generally, ISPs are readily identifiable and easily located, whereas guilty parties are often difficult to locate because determining the author of a particular message is practically unfeasible.<sup>21</sup> Even if the author is found, he or she may be "judgment proof" because the plaintiff will likely seek the deeper pockets of the ISP.<sup>22</sup>

### I(c). OVERVIEW

This note's objective is to provide insight into the liability that Internet Service Providers (ISPs) face in the ever-changing world of the Internet. This note will first focus on the four main areas of liability for ISPs: (1) copyright infringement, (2) defamation (including "cybersmear"), (3) objectionable content, and (4) crime/terrorism detection and prevention. It will provide an overview of the major cases and laws that restrict, guide, and even those that protect ISPs' interactions with their customers. Finally, this note will address the general methods and steps

---

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> SUGARMAN, ROGERS, BARSHAK & COHEN, P.C., *Internet Service Providers and Webmasters*, Netlitigation.com, Internet Law: News, Suits, and Discussions, at <http://www.netlitigation.com/netlitigation/isp.htm> (last visited Jan. 24, 2004) [hereinafter SUGARMAN].

<sup>19</sup> Deturbide, *supra* note 3.

<sup>20</sup> *Id.*

<sup>21</sup> SUGARMAN, *supra* note 18.

<sup>22</sup> Deturbide, *supra* note 3.

that allow ISPs to protect their own interests. In order to better illustrate these points, this note will provide a boilerplate contract for use by ISPs in their web hosting businesses. This contract will incorporate many of the protection measures that derive from the major laws and rulings of the following cases discussed herein.

## II. COPYRIGHT AND TRADEMARK INFRINGEMENT

### II(a). DEFINITIONS

The reality that any person across the globe with a computer can inexpensively and effortlessly access copyrighted works, coupled with the automatic reproduction ability of the Internet's networked computers, has increased copyright infringement to an unimaginable scale.<sup>23</sup> In order to make copyrighted materials available globally, ISPs will often provide the necessary access and channels to their customers.<sup>24</sup> It has been said that every time an ISP's subscriber accesses copyrighted material (i.e. uploading or downloading) without permission, the ISP is infringing on the exclusive rights of reproduction and distribution.<sup>25</sup>

Individual customers are guilty of copyright infringement when they violate an exclusive right held by the copyright owner under the Copyright Act.<sup>26</sup> These six rights include:

- (1) the right to reproduce the copyrighted work;
- (2) the right to prepare derivative works based upon the work;
- (3) the right to distribute copies of the work to the public;
- (4) the right to perform the copyrighted work publicly;
- (5) the right to display the copyrighted work publicly; and
- (6) the right "to perform the copyrighted work publicly by means of digital audio transmission."<sup>27</sup>

---

<sup>23</sup> Salow, *supra* note 1.

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> Bolin & Tysver, *supra* note 7.

<sup>27</sup> Copyright Act, 17 U.S.C. § 106 (2000); *see also*, Daniel A. Tysver, *Rights Granted Under Copyright Law*, at <http://www.bitlaw.com/copyright/scope.html> (last visited Nov. 14, 2003).

An ISP will be liable for an act of copyright infringement if it is found to be directly involved in the copying of protected material.<sup>28</sup> Therefore, an ISP would be guilty of infringement if it placed a copy of either a best-selling novel or computer program on its site.<sup>29</sup>

Other common lawsuits brought against ISPs are those related to trademark infringement. Such claims are becoming more and more common in the wireless universe,<sup>30</sup> because many website owners and designers are not familiar with the laws regulating trademarks. To prevail on a trademark infringement claim, the plaintiff has the burden of proving that the defendant created confusion, mistake, and/or deception in its use of a similar mark.<sup>31</sup> The alleged confusion can be shown by demonstrating the defendant held out his product as being the same as or affiliated with the plaintiff's products or company.<sup>32</sup>

When one of an ISP's customers infringes or misuses another's trademark, that ISP may be prosecuted for liability under the "theory of contributory trademark infringement."<sup>33</sup> This type of liability exists when an ISP knowingly causes or contributes to the infringement.<sup>34</sup>

## **II(b). CASES OF COPYRIGHT INFRINGEMENT AND TRADEMARK INFRINGEMENT**

There are numerous cases addressing an Internet Service Provider's liability stemming from copyright and trademark infringement. However, the main focus of this note is not to comment on these two infringements alone, but rather to focus on the different forms of liability

---

<sup>28</sup> Bolin & Tysver, *supra* note 7.

<sup>29</sup> *Id.*

<sup>30</sup> Daniel A. Tysver, *Trademark Infringement*, at <http://www.bitlaw.com/trademark/infringe.html> (last visited Nov. 14, 2003).

<sup>31</sup> Tysver, *supra* note 30.

<sup>32</sup> *Id.*

<sup>33</sup> Bolin & Tysver, *supra* note 7.

<sup>34</sup> *Id.*

ISPs face and the steps they can take to prevent that liability. Therefore, the major cases and their importance for the future business of ISPs will be briefly discussed.

**II(b)(1). *Playboy Enterprises, Inc. v. Frena***

Frena operated a pay-based computer bulletin board service (“BBS”) that distributed unauthorized copies of Playboy’s copyrighted photographs containing the trademarks “PLAYBOY” and “PLAYMATE.” After Playboy commenced an action against Frena, the defendant removed the photographs and began monitoring the BBS to prevent subscribers from uploading additional photographs belonging to the plaintiff.<sup>35</sup>

The court found the BBS operator liable for direct copyright infringement because although he did not make infringing copies, his product contained unauthorized copies.<sup>36</sup>

**II(b)(2). *Religious Technology Center v. Netcom On-Line Communications Services, Inc.***

Religious Technology Center (“RTC”) brought a copyright infringement action against the defendants, an on-line BBS and Netcom On-Line Communications, Inc. (“Netcom”), an ISP.<sup>37</sup> RTC held copyrights in the works of its founder, and the defendant BBS posted messages on the Internet using portions of those works.<sup>38</sup> RTC asked both defendants to deny access to the individual involved and to remove all documents containing church materials from the servers they controlled.<sup>39</sup> When both the BBS and Netcom refused, the plaintiff brought the case to court.<sup>40</sup>

---

<sup>35</sup> *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993).

<sup>36</sup> *Id.* at 1556.

<sup>37</sup> *Religious Tech. Center v. Netcom On-Line Communications Servs., Inc.*, 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995).

<sup>38</sup> *Id.* at 1366.

<sup>39</sup> *Id.*

<sup>40</sup> *Bolin & Tysver, supra* note 7.

The court rejected the notion that either the BBS operator or Netcom was directly liable for the third party infringement.<sup>41</sup> The court held that it did not make sense to adopt a rule that would impose liability on numerous parties who held no role in the infringement aside from forming and operating system programs on the Internet.<sup>42</sup>

**II(b)(3).      *Sega Enterprises, Ltd. v. MAPHIA***

Sega Enterprises, Ltd. filed suit for copyright infringement (17 U.S.C. §101) and federal trademark infringement (15 U.S.C. §1051) against the defendant, MAPHIA, as owners and operators of Internet bulletin boards. Sega complained that MAPHIA made Sega's video games available over the Internet without making customers pay.<sup>43</sup>

“[T]he court stressed that the BBS operator did not upload or download the infringing files himself and thus did not directly cause the copying.”<sup>44</sup> The court's rationale was that whether or not the BBS operator knew of or encouraged its users' infringement had no bearing on a BBS operator's direct acts causing infringement.<sup>45</sup> The BBS operator was not liable for direct infringement because Sega was unable to show that they directly caused the copying.<sup>46</sup>

**II(b)(4).      *Gucci America, Inc. v. Hall & Associates***

Gucci America, Inc. owns the trademark and trade name “GUCCI.” Mindspring, an Internet Service Provider, provides Web page hosting services to Hall & Associates (“Hall”). Gucci notified Mindspring that Hall was using Mindspring's services to aid in acts of trademark infringement and unfair competition, including the advertising of jewelry on the Goldhaus website which bore (and infringed) the Gucci Trademark. Despite the e-mails, Mindspring continued to permit Hall to use Mindspring's Internet services to infringe the plaintiff's

---

<sup>41</sup> *Religious Tech. Center*, 907 F. Supp. at 1372.

<sup>42</sup> *Id.*

<sup>43</sup> *Sega Enters., Ltd. v. MAPHIA*, 948 F. Supp. 923 (N.D. Cal. 1996).

<sup>44</sup> Salow, *supra* note 1.

<sup>45</sup> *Id.*

<sup>46</sup> *Id.*

trademark rights, with actual knowledge of, or in reckless disregard of, the plaintiff's rights and Hall's infringement.<sup>47</sup>

The court held that the Telecommunications Act of 1996 did not shield the defendant corporation from liability for information posted on a website by the defendant individual.<sup>48</sup> The court reasoned that based upon the doctrine of contributory infringement, a manufacturer or distributor can be held liable when a manufacturer or distributor continuously supplies products to one it knows, or has reason to know, is committing trademark infringement.<sup>49</sup>

### **II(b)(5).      *A&M Records, Inc. v. Napster, Inc.***

Napster, Inc. ("Napster") produced software that allowed its Internet users to search for, request, download, and play music files free of charge by exchanging the files with other users. A&M Records, Inc. ("A&M") sued, alleging the defendant's users infringed on its copyrighted music. Napster filed a motion for summary judgment, arguing that the safe harbor provision of the Digital Millennium Copyright Act, 17 U.S.C.S. §512(a), protected it from liability.<sup>50</sup>

The court denied Napster's motion. First, the court reasoned that the section 512(a) protection could not be extended to Napster's role in the transmission of MP3 files because no transmission went through Napster.<sup>51</sup> Second, Napster did not reasonably implement a repeat offender policy required by section 512(i)(A).<sup>52</sup>

After the trial, the District Court's injunction was temporarily stayed pending a hearing on the merits.<sup>53</sup> The Court of Appeals for the Ninth Circuit remanded the case to the District Court, stating that an injunction was warranted, not just required.<sup>54</sup>

---

<sup>47</sup> *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 410-11 (S.D.N.Y. 2001).

<sup>48</sup> *Id.* at 412.

<sup>49</sup> *Gucci Am.* 135 F. Supp. 2d at 413 (quoting *Inwood Labs., Inc. v. Ives Labs., Inc.* 456 U.S. 844, 854 (1982)).

<sup>50</sup> *A&M Records, Inc. v. Napster, Inc.*, 2000 U.S. Dist. LEXIS 6243 (N.D. Cal. 2000).

<sup>51</sup> Salow, *supra* note 1 (emphasis in original).

<sup>52</sup> *A&M Records*, 2000 U.S. Dist. LEXIS 6243, at \*28 (emphasis in original).

<sup>53</sup> Salow, *supra* note 1.

## **II(c). STATUTES/LAWS**

### **II(c)(1). DIGITAL MILLENNIUM COPYRIGHT ACT**

#### **II(c)(1)(A). GENERAL APPLICATION TO ISPs**

The Digital Millennium Copyright Act<sup>55</sup> [hereinafter DMCA] addresses the issue of an ISP's copyright liability.<sup>56</sup> Generally, an ISP is not liable for providing or facilitating access to infringing material.<sup>57</sup> When an ISP acts as a "passive conduit," it is almost automatically protected from liability claims.<sup>58</sup> In contrast, an ISP must follow a notice and take-down procedure when it provides storage on the Internet through the use of web hosting, hyperlinking or caching.<sup>59</sup> Thus, the Act is, in part, favorable to ISPs, and was supported by a strong ISP lobby which successfully argued that the great quantity of information and traffic on ISPs' sites and the Internet made it impossible to monitor ISPs' subscribers' activities.<sup>60</sup> Congress agreed with the ISPs. If ISPs were held strictly liable for the actions of their subscribers, the cost of the Internet would become excessive because ISPs would pass their liability on to customers in the form of higher fees.<sup>61</sup>

#### **II(c)(1)(B). NOTICE AND REMOVAL**

The DMCA sets out a "clearly defined notice and take down time table."<sup>62</sup> As a preventative measure to any infringement action, an ISP must have in place, on every one of its hosted sites, information that will allow customers to notify the Register of copyrights and an

---

<sup>54</sup> *Id.*

<sup>55</sup> Digital Millennium Copyright Act, 17 U.S.C. § 512 (2000).

<sup>56</sup> Hayes, *supra* note 9.

<sup>57</sup> *Id.*

<sup>58</sup> Salow, *supra* note 1.

<sup>59</sup> *Id.*

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

agent of the ISP, of any alleged infringement(s).<sup>63</sup> Initially, the ISP is to be “notified in writing that copyright infringing material [is] available through its service,” and must then “act expediently to remove or disable access to the offending material.”<sup>64</sup> Next, the ISP must notify the alleged infringer that the material will be removed from its site within ten working days of the notification.<sup>65</sup>

An alleged infringer is not without rights under the Act; he or she may file a counter-notification.<sup>66</sup> If a counter-notification is filed and received by the ISP, it is the ISP’s responsibility to “pass it along to the copyright owner who initiated the dispute.”<sup>67</sup> The copyright owner must, within a ten day period from the date of the notification, seek an injunction to restrain the alleged infringer from continuing to engage in the alleged infringing activity.<sup>68</sup> If the party seeking the infringement claim does not do this within ten days, the ISP can put the material back up on the hosted site.<sup>69</sup> However, if no counter-notification is provided, the ISP must take down the allegedly infringing material.<sup>70</sup> These procedures strike a balance between the alleged infringer’s First Amendment rights and the copyright owner’s intellectual property rights.<sup>71</sup>

### **II(c)(1)(C). AVAILABLE SAFE HARBORS**

The DMCA provides several safe harbors to ISPs for allegedly infringing actions committed by their users or customers.<sup>72</sup> These safe harbors are used to provide protection in

---

<sup>63</sup> SUGARMAN, *supra* note 18.

<sup>64</sup> Salow, *supra* note 1.

<sup>65</sup> *Id.*

<sup>66</sup> SUGARMAN, *supra* note 18.

<sup>67</sup> *Id.*

<sup>68</sup> Hayes, *supra* note 9.

<sup>69</sup> *Id.*

<sup>70</sup> SUGARMAN, *supra* note 18.

<sup>71</sup> Hayes, *supra* note 9.

<sup>72</sup> Joseph A. Sifferd, Note, *The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology*, 4 VAND. J. ENT. L. & PRAC. 93, 97 (2002).

instances where ISPs are passively storing infringing material on their systems, or where they have merely directed “users to infringing material on other sites, by providing ‘information location tools,’ such as directories, indexes, search engines, or simple hypertext links.”<sup>73</sup> These safe harbors do not insulate ISPs from their own actions of direct infringement, but rather are in place only for protection against liability for contributory or vicarious infringement.<sup>74</sup>

The safe harbors apply to ISPs when:

- (1) The ISP acts merely as a conduit, unknowingly transferring infringing materials;
- (2) The ISP temporarily stores infringing materials for the users' convenience;
- (3) The ISP acts as storage for infringing material, except when “the ISP knows or should know, or financially benefits from, the infringing material”; or
- (4) The ISP uses information location tools (“ILTs”), such as hyperlinks, to find infringing materials unless the ISP has actual knowledge or received notice of the infringing materials.<sup>75</sup>

The previous cases and the DMCA set up some basic guidelines that ISPs should follow. Internet Service Providers should not provide a product or service that contains unauthorized reproductions of a copyrighted work.<sup>76</sup> Additionally, ISPs should not make the means available to allow copyrighted material to be copied.<sup>77</sup> Finally, if an ISP knows the material is protected by a copyright or trademark, it should, in accordance with the DMCA where applicable, take that material down.<sup>78</sup>

---

<sup>73</sup> SUGARMAN, *supra* note 18.

<sup>74</sup> Sifferd, *supra* note 72, at 97.

<sup>75</sup> Kevin Michael Lemley, Comment, Protecting Consumers From Themselves: Alleviating the Market Inequalities Created by Online Copyright Infringement in the Entertainment Industry, 13 ALB. L.J. SCI. & TECH. 613, 620 (2003) (citing 17 U.S.C. 512(a)-(d)).

<sup>76</sup> *Playboy Enters.*, 839 F. Supp. at 1559.

<sup>77</sup> *A&M Records*, 2000 U.S. Dist. LEXIS 6243, at \*29; *Sega Enters.*, 948 F. Supp. at 945.

<sup>78</sup> *Gucci Am.*, 135 F. Supp. 2d at 413.

### III. DEFAMATION

#### III(a). DEFINITIONS OF DEFAMATION AND “CORPORATE CYBERSMEAR”

Defamation is defined as “a false written or oral statement that damages another’s reputation.”<sup>79</sup> Included in this definition is what has been termed “corporate cybersmear.” “Corporate cybersmear” is the “the posting of demonstrably false statements to online message boards in an effort to drive down the price of a company’s stock.”<sup>80</sup>

#### III(b). DIFFERENCE BETWEEN “PUBLISHER” AND “DISTRIBUTOR”

A common problem that arises when lawsuits are brought on grounds of defamation is that a court must decide whether or not an ISP should be considered a “publisher” or a “distributor.” “Publishers’, such as newspapers, which traditionally exerted editorial control over content, are generally liable for the defamatory statements that they publish. ‘Distributors’, such as bookstores or newsstands, exert very little if any editorial control, and have the benefit of the ‘innocent disseminator’ defence.”<sup>81</sup> So under which category do ISPs fall? The prevailing view suggests that ISPs do not typically impose editorial filters on content, which distinguishes them from their print and broadcast counterparts.<sup>82</sup> Therefore, ISPs operate as distributors (“innocent disseminators”) and are not held liable for defamatory statements placed on the ISPs’ websites by customers unless they knew, or ought to have known, of the existence of the defamatory statement.<sup>83</sup>

#### III(c). CASES OF DEFAMATION AND CORPORATE CYBERSMEAR

##### III(c)(1). *Cubby, Inc. v. CompuServe, Inc.*

---

<sup>79</sup> BLACK’S LAW DICTIONARY 427 (7th ed. 1999).

<sup>80</sup> Ress, *supra* note 4.

<sup>81</sup> Deturbide, *supra* note 3.

<sup>82</sup> *Id.*

<sup>83</sup> Deturbide, *supra* note 3.

The plaintiffs, a computerized database operator, Cubby, Inc., and its developer, Robert Blanchard, brought a diversity action against a competing database owner, CompuServe, for libel, business disparagement, and unfair competition which arose when the defendant's database displayed a publication containing defamatory statements about Cubby.<sup>84</sup>

The court found that CompuServe had acted as a distributor, not a publisher, of the statements.<sup>85</sup> The court stated the rule that “New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.”<sup>86</sup> The court likened CompuServe to public libraries, book stores, and newsstands, noting that all had comparable levels of editorial control over publications; consequently, it would not be feasible for any of these entities to examine each publication for defamatory content.<sup>87</sup> Based on the preceding rule and facts of the case, the court allowed CompuServe to escape liability because it neither knew of, nor had any reason to know about the defamatory statement.<sup>88</sup>

### **III(c)(2). *Stratton Oakmont, Inc. v. Prodigy Services Co.***

Stratton Oakmont, a securities investment-banking firm, sued Prodigy Services Company (“Prodigy”), an online service provider.<sup>89</sup> The suit was brought after a defamatory comment was posted by an anonymous party on Prodigy's “Money Talk” bulletin board—a financial information board that boasted a widespread readership across the United States.<sup>90</sup> The posting

---

<sup>84</sup> Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

<sup>85</sup> *Id.* at 141.

<sup>86</sup> *Id.* at 139 (quoting Lerman v. Chuckleberry Publ'g. Inc., 521 F. Supp. 228, 235 (S.D.N.Y. 1981)).

<sup>87</sup> *Id.* at 140.

<sup>88</sup> Bolin & Tysver, *supra* note 7.

<sup>89</sup> Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995), *superseded by statute as stated in* Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1999).

<sup>90</sup> Deturbide, *supra* note 3.

alleged the plaintiff “had committed fraudulent acts in connection with an initial public offering, and further derogatory characterizations of the company and its employees.”<sup>91</sup>

The court found that Prodigy could not be considered a “distributor” because Prodigy “used a software screening program that automatically removed offensive language, issued guidelines that indicated offensive posts would be removed, and hired bulletin board ‘leaders’ to enforce the guidelines.”<sup>92</sup> According to the court, Prodigy engaged in editorial control by “making content decisions and establishing a system to monitor content.”<sup>93</sup> The court further held that Prodigy was considered a publisher, thus potentially liable for defamation, because of Prodigy’s widely publicized forum monitoring and censoring policies.<sup>94</sup>

### **III(c)(3).      *Zeran v. America Online, Inc.***

In 1995, an anonymous person placed an advertisement on America Online (AOL) promoting the sale of t-shirts that depicted offensive sayings related to the Oklahoma City bombing.<sup>95</sup> The phone number listed in the advertisement belonged to the plaintiff, Kenneth Zeran, who had no knowledge of the incident.<sup>96</sup> As a result of the prank, Zeran received many phone calls, some of which threatened his life.<sup>97</sup> Zeran was reluctant to change his phone number because he used it for his personal business, so he contacted AOL to rectify the problem.<sup>98</sup> Though the original posting was removed, new postings subsequently surfaced.<sup>99</sup> After numerous calls to AOL, Zeran was informed the account would be closed, but as before,

---

<sup>91</sup> *Id.*

<sup>92</sup> *Id.*

<sup>93</sup> *Id.*

<sup>94</sup> Bolin & Tysver, *supra* note 7.

<sup>95</sup> *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 329 (4th Cir. 1999).

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> *Id.*

new postings soon appeared on AOL.<sup>100</sup> A local radio show host even encouraged his listeners to phone Zeran to convey their indignation.<sup>101</sup> Thereafter, Zeran required protective police surveillance because he was flooded with calls and death threats which did not stop until the Oklahoma City newspaper ran a story which revealed the postings were a hoax.<sup>102</sup> Zeran sued AOL based on the traditional test for liability for distributors—that a distributor has a duty to remove material if the distributor knows, or had reason to know of the material’s defamatory character.<sup>103</sup>

The Zeran court upheld the “CDA’s [Communications Decency Act of 1996] limitations on the liability of ISPs for messages posted by subscribers or others.”<sup>104</sup> The court granted AOL immunity because under the CDA, an ISP could not be liable for defamation originating from a third party’s use of AOL’s Internet services.<sup>105</sup> The court ruled in favor of AOL. In addition to the near impossibility of requiring ISPs to screen millions of postings daily, the court felt there should be minimal government interference with Internet communication.<sup>106</sup>

### **III(c)(4). *Blumenthal v. Drudge***

In his online column entitled the *Drudge Report*, gossip columnist Matt Drudge alleged White House aide Sidney Blumenthal was a spousal abuser.<sup>107</sup> Blumenthal sued both Drudge and AOL for defamation.<sup>108</sup> Though it was acknowledged that AOL had received advance notice of the *Report*, the court held that the *Zeran* court’s interpretation of section 230 protected

---

<sup>100</sup> *Id.*

<sup>101</sup> *Id.*

<sup>102</sup> *Id.*

<sup>103</sup> *Id.* at 328.

<sup>104</sup> SUGARMAN, *supra* note 18.

<sup>105</sup> *Zeran*, 129 F.3d at 331-32.

<sup>106</sup> *Id.* at 330.

<sup>107</sup> *Blumenthal v. Drudge*, 992 F. Supp. 44, 46 (D.C. Cir. 1998).

<sup>108</sup> *Id.*

AOL from liability.<sup>109</sup> Despite AOL’s retention of some editorial control over forum postings, the courts decision in *Blumenthal* reaffirmed the CDA’s extension of absolute immunity for ISPs regarding third party postings.<sup>110</sup>

### **III(d). STATUTES/LAWS**

#### **III(d)(1). COMMUNICATION DECENCY ACT OF 1996 (“CDA”)**

In 1996, Congress enacted the Telecommunications Act of 1996,<sup>111</sup> which amended the Communications Act of 1934.<sup>112</sup> Title V of the Telecommunications Act is known as the Communications Decency Act of 1996.<sup>113</sup> Section 230 of the CDA shields ISPs from liability for defamation. “The underlying principle of the section is that ‘Good Samaritans’ who undertake editorial duties to remove offensive content should not be penalized for their efforts by being treated as publishers, and hence be subject to liability for defamation or other causes of action.”<sup>114</sup> Pursuant to section 230(c)(1), an ISP will not be treated as a publisher of online material posted by a third party.<sup>115</sup> Furthermore, “section 230(c)(2) states that no provider or user of an interactive computer service can be held liable for voluntarily restricting access to or availability of objectionable material, or for making available the technical means to restrict access to such material.”<sup>116</sup> The purpose of the section is to prevent lawsuits against ISPs, such as in *Prodigy*, where the ISP had undertaken editorial functions.<sup>117</sup>

The previous cases and the CDA set up some basic guidelines that ISPs should follow. If an ISP uses no, or some amount of, editorial control, courts consider them to be mere

---

<sup>109</sup> *Id.* at 52-53.

<sup>110</sup> SUGARMAN, *supra* note 18.

<sup>111</sup> Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

<sup>112</sup> Communications Act of 1934, 47 U.S.C. § 609 (2000).

<sup>113</sup> Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (1996).

<sup>114</sup> Deturbide, *supra* note 3.

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

“distributors” who are not subject to liability; however, if they exercise too much control, ISPs are considered to be “publishers,” and thus subject to liability.<sup>118</sup> Courts are reluctant to hold ISPs liable when they are acting as “Good Samaritans” for editorializing offensive content or making the means available to restrict access to offensive material.<sup>119</sup>

#### **IV. OBJECTIONABLE CONTENT**

##### **IV(a). DEFINITION OF OBJECTIONABLE CONTENT**

There seems to be no bright-line definition of objectionable content. Perhaps it is best described in the words of Supreme Court Justice Potter Stewart, who remarked in his concurring opinion in *Jacobellis v. Ohio*, “I know it when I see it.”<sup>120</sup> Simply stated, if you have to ask, then you already know the answer.

##### **IV(b). CASES OF OBJECTIONABLE CONTENT**

###### **IV(b)(1). *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme***

In France, it is a violation of the Penal Code to display objects connoting racial symbolism. When Nazi memorabilia was sold over the Internet via a server located in the United States that was accessible to French users, the *Yahoo!* Case ensued.<sup>121</sup> Yahoo! appealed an order by a French court that ordered Yahoo! to bar French citizens’ access to the auctions in question.<sup>122</sup>

The Northern District of California ruled that Yahoo! was not obligated to follow the French court’s ruling.<sup>123</sup> In arriving at this decision, Judge Fogel acknowledged that while “France has the sovereign right to regulate what speech is permissible in France, this Court may

---

<sup>118</sup> *Cubby*, 776 F. Supp. at 140; Deturbide, *supra* note 3.

<sup>119</sup> Deturbide, *supra* note 3.

<sup>120</sup> 378 U.S. 184, 197 (1964).

<sup>121</sup> *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181, 1184 (N.D. Cal.), *rev'd on juris. grounds*, 379 F.3d 1120 (9th Cir. 2004), *reh'g on juris. grounds*, 2005 U.S. App. LEXIS 2166 (9th Cir. 2005).

<sup>122</sup> *Id.* at 1185.

<sup>123</sup> *Id.* at 1194.

not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders.”<sup>124</sup>

**IV(b)(2). *Doe v. America Online, Inc.***

The plaintiff filed charges against America Online (“AOL”) claiming that a man who sexually molested her son and created videos and photographs of the acts used AOL’s chat rooms to market and sell the items.<sup>125</sup> The case was dismissed because the plaintiff was not able to “overcome section 230 immunity.”<sup>126</sup>

*Doe*’s ruling demonstrated the expansiveness of section 230 and its interpretation; in fact it may be the case that “all tort-based claims against ISPs for material originating with a third party are barred because of section 230.”<sup>127</sup>

**IV(c). STATUTES/LAWS**

**IV(c)(1). 47 U.S.C. § 231**

In 1998, section 231 was amended to permit criminal and civil penalties against a person who “makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors.”<sup>128</sup> Section 231 creates an affirmative defense for ISPs, provided that they restrict access to harmful material through any number of age verification measures.<sup>129</sup>

The previous cases and section 231 provide some examples where ISPs will not be held liable for the actions of third parties who use an ISP’s services. Section 231 enables ISPs to use editorial functions such as age verification software or software that allows the ISP to monitor online forms for offensive links, pictures, words, and more.

---

<sup>124</sup> *Yahoo!*, 169 F. Supp. 2d at 1192.

<sup>125</sup> *Doe v. Am. Online, Inc.*, 718 So. 2d 385, 386 (Fla. Dist. Ct. App. 1998).

<sup>126</sup> *Id.* at 389.

<sup>127</sup> *Deturbide*, *supra* note 3.

<sup>128</sup> 47 U.S.C. § 231(a)(1) (2000).

<sup>129</sup> *Id.* § 231(c)(1).

## **V. CRIME AND TERRORISM DETECTION**

### **V(a). GENERAL INTRODUCTION TO CRIME AND TERRORISM DETECTION**

While crime detection and anti-terrorism are not new ideas to the twenty-first century, there have been significant increases in the ability to track would-be criminals and terrorists using the resources of the World Wide Web. In response to the September 11 terrorist attacks, there has been a worldwide call by politicians for ISPs to store user information and activity logs in case of a police investigation.<sup>130</sup> While speaking before the House Judiciary Committee's Subcommittee on Crime, Clint Smith, President of the United States Internet Service Providers Association, described how crime, terrorism, the government, and ISPs should interact. He stated that "[t]he successful investigation and prosecution of crime on the Internet requires a legal framework that balances the powers of law enforcement, the privacy rights of individuals, and the responsibilities and liabilities of service providers."<sup>131</sup> Considering the rapid rate at which the Internet and technology are increasing, society, and especially ISPs, will be in a far better position to help prevent future crime and acts of terrorism. However, to make the previous statement a reality, Congress needs to pass laws that aid and protect ISPs with their online monitoring.

### **V(b). STATUTES/LAWS**

#### **V(b)(1). USA PATRIOT ACT**

One such law, the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001),<sup>132</sup> was signed into law by President George W. Bush on October 26, 2001, in response to the direct acts

---

<sup>130</sup> Ress, *supra* note 4.

<sup>131</sup> *The Cyber Security Enhancement Act of 2001: Hearing on H.R. 3482 Before the Subcomm. on Crime of the House Comm. on the Judiciary*, 107th Cong. 38 (2002) (statement of Clint N. Smith, President, United States Internet Service Providers Association).

<sup>132</sup> Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

of terrorism on American soil. This Act is designed to “deter and punish terrorist acts in the United States and around the world,” and “to enhance law enforcement investigatory tools.”<sup>133</sup> The Act “allows authorities to search educational, library and medical data, as well as travel, credit and immigration records. The act expands the use of wiretapping and Internet monitoring permitted by the Combating Terrorism Act, giving the government access to personal data records and allowing for secret searches.”<sup>134</sup> Generally, section 212 of the USA PATRIOT Act gives teeth to ISPs because it allows an ISP’s disclosure to governmental entities if the ISP has a reasonable belief that there is an emergency involving immediate death or serious physical injury.<sup>135</sup>

However, the USA PATRIOT Act does “not explicitly grant ISPs immunity from liability in all cases for their role in”<sup>136</sup> fighting terrorism. To deal with this problem, Congress has proposed the Cyber Security Enhancement Act of 2001.<sup>137</sup> This proposed act would “encourage ISPs to promptly report threats of death or personal injury to law enforcement”<sup>138</sup> because it would remove “the requirement that the danger be ‘immediate’ and allows ISPs to act on a ‘good faith’ belief rather than the higher standard of a ‘reasonable’ belief.”<sup>139</sup> The Cyber Security Enhancement Act of 2001 clarifies that ISPs are immune from liability when acting in good faith in two situations—turning over information to law enforcement personnel in emergencies, and inviting law enforcement to monitor the communications of computer trespassers.<sup>140</sup>

The USA PATRIOT Act has laid the foundation for protecting ISPs from liability for disclosing records to the government under certain circumstances. With proposed laws, such as

---

<sup>133</sup> *Id.*

<sup>134</sup> Ress, *supra* note 4.

<sup>135</sup> 18 U.S.C. § 2702.

<sup>136</sup> Smith statement, *supra* note 131, at 41.

<sup>137</sup> The Cyber Security Enhancement Act of 2001, H.R. 3482, 107 Cong. (2001).

<sup>138</sup> Smith statement, *supra* note 131, at 41.

<sup>139</sup> Smith statement, *supra* note 131, at 41.

<sup>140</sup> *Id.*

The Cyber Security Enhancement Act of 2001, ISPs will be presented with more protection from liability. This is a necessity in the fast-paced and ever-changing world. ISPs are the gateway to endless information, and should be afforded the full backing of our government to help protect America.

## VI. Conclusion

It is evident that ISPs face a great deal of uncertainty and risk in their daily businesses. This note has set forth some of the general ways in which an ISP can protect itself against liability, keeping in mind its role as the gateway to the Internet super highway, and the one in the best position to detect, block, and remove offensive or infringing material.<sup>141</sup> However, the question of “how much protection is enough” still remains uncertain. It is clear that all ISPs must have measures in place that comply with Federal laws and statutes. ISPs must have measures for notice and removal under the DMCA, must comply with orders from governmental agencies under the USA PATRIOT Act, and must have age verification measures in place under section 231 to protect minors from offensive material. Conversely, the CDA is not as clear in regards to the editorial duties ISPs must take. Problems arise when an ISP uses no, or some amount of editorial control; in these instances, the courts consider ISPs mere “distributors” who are not subject to liability. However, if an ISP exercises too much control, it is considered to be a “publisher,” and thus subject to liability for defamation or infringement.<sup>142</sup> It is not clear which measures are “too much” and which measures are “too little.” When exercising editorial control, ISPs should comply with the requirements of all federal laws and statutes, and follow the general reasoning reached in *United States v. Carroll Towing*.<sup>143</sup>

---

<sup>141</sup> Hayes, *supra* note 9.

<sup>142</sup> *Cubby*, 776 F. Supp. at 140; Deturbide, *supra* note 3.

<sup>143</sup> *United States v. Carroll Towing*, 159 F.2d 169 (2d Cir. 1947).

In *Carroll Towing*, a United States barge named the “Anna C” sank when it broke free from its moorings, traveled down stream, and struck a tanker’s propeller.<sup>144</sup> Judge Learned Hand set out a three-part test for determining an owner’s duty to provide against injury. Hand’s formula placed liability on an owner where the burden of preventing harm was less than the probability of the event occurring multiplied by the amount of the injury caused.<sup>145</sup> How does this classic torts case analogize to an ISP’s liability? *Carroll Towing* anchors a guideline for ISPs to take appropriate precautions that are reasonable and foreseeable on a case-by-case basis. As business owners, ISPs know the difference between creating and hosting a site for their local Catholic grade school or for “Triple X Entrepreneurs, Inc.,” and should act accordingly.

#### **VI(a). BOILERPLATE CONTRACT**

The following boilerplate contract incorporates many of the protective measures that derive from the major laws, statutes, and rulings of the cases previously discussed. This contract is in no way a complete business contract covering every liability an ISP may face. Its main purpose is to better illustrate this note’s objective of protecting ISPs.

#### **WEB SITE HOSTING AGREEMENT**

“This Agreement is entered into on \_\_\_\_\_ [date], (the “Effective Date”) by and between \_\_\_\_\_ [name of customer] (“Customer”) and \_\_\_\_\_ [name of host] (“Host”). Customer and Host are sometimes referred to collectively in this Agreement as the “Parties.”

Customer desires to engage Host for the purpose of storing Customer’s site on the World Wide Web (the “Web Site”) and making it available for browsing on the Internet.

To carry out these purposes, the Parties have agreed to the following.”<sup>146</sup>

The Host will make available the means necessary to prevent the access of obscene material by minors. At no point will the Customer have the ability to remove these programs or links making these programs available.

---

<sup>144</sup> *Id.* at 171.

<sup>145</sup> *Id.* at 173.

<sup>146</sup> *Website Hosting Agreement*, N.Y. FORMS LEGAL & BUS. §15A:35 (2003).

In accordance with the Digital Millennium Copyright Act (“DMCA”), the Host will have in place procedures for the notification of alleged copyright infringement. At no point will the Customer have the ability to remove these programs or links making these programs available. The Customer will be provided with a copy of the procedures under the DMCA and the Host will maintain at all times a link to these procedures.

The Customer agrees that the Host is not responsible for the accuracy of out-of-date material contained on the Customer’s site. Host “neither endorses nor is responsible for the accuracy or reliability of any opinion, advice or statement made on the Services by anyone other than authorized Host employee spokespersons while acting in their official capacities.”<sup>147</sup>

The Host will have in place procedures for the notification of alleged obscenity, defamation, trademark infringement, criminal activity and terrorism. At no point will the Customer have the ability to remove these programs or links making these programs available. The Customer will be provided with a copy of the procedures and the Host will maintain at all times a link to these procedures.

The Host agrees to provide limited monitoring functions on its hosted sites of any and all traffic which utilize the Host’s services. “This monitoring may include public as well as private communications and data transfers from our Customers and to our Customers as well as any and all communications and data transfers to and from any other Internet sites.”<sup>148</sup> However, the Customer agrees to remain primarily responsible, to the fullest extent permitted by law, for the content on their site and the control of their site.<sup>149</sup> Host “is a distributor (and not a publisher) of Content supplied by third parties and Customers. Accordingly, Host has no more editorial control over such Content than does a public library, bookstore or newsstand. Any opinions, advice, statements, services, offers or other information or Content expressed or made available by third parties are those of the respective author(s) or distributor(s) and not of the Host.”<sup>150</sup>

Content. “Any copyrighted Content submitted with the consent of the owner should contain a phrase such as “Copyright owned by \_\_\_\_\_ [insert name of Customer]; Used by Permission.” The unauthorized submission of copyrighted or other proprietary Content constitutes a breach of this Agreement and could subject you to criminal prosecution as well as personal liability for damages in a civil suit. The Customer, not Host or its employees or independent contractors, are liable for all damages arising from such submission.”<sup>151</sup>

“Online Conduct. Customer agrees to use the Services solely for lawful purposes. Customer is prohibited from posting on or transmitting through the Services any unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, profane, hateful, racially, ethnically or otherwise objectionable material of any kind, including but not limited to, any material which encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable local, state, national or international law. Host reserves the

---

<sup>147</sup> *Internet Network Access and Service Agreement* 6 FLA. JUR. FORMS LEGAL & BUS. § 20B:33(2.7) (Dec. 2003).

<sup>148</sup> *Id.* § 20B:33(4.1).

<sup>149</sup> *World Wide Web Site Design, Storage and Promotion Agreement*, 6 FLA. JUR. FORMS LEGAL & BUS. § 20B:34(6)(B)(i) (Dec. 2003).

<sup>150</sup> 6 FLA. JUR. FORMS LEGAL & BUS. § 20B:33(2.7).

<sup>151</sup> *Id.* § 20B:33(2.6).

right to suspend or terminate any Customer whose actions are in violation of acceptable on-line conduct, the determination of which resides in Host's sole discretion."<sup>152</sup>

"Right to Monitor and Remove Unacceptable Sites. Host has the right, but not the duty, to review and monitor all content submitted for or included on the Web Site, and in its sole discretion to remove any content that Host finds objectionable for any reason, without prior notice to Customer."<sup>153</sup>

"Indemnity. Customer is solely responsible for any liability arising out of or related to the Web Site. Customer agrees to indemnify and hold Host harmless from and against any and all liabilities, losses, damages, costs, and expenses, including reasonable attorney's fees and experts' fees, associated with any claim or action brought against Host related to or arising out of the Web Site or Customer's breach of its warranties under this Agreement."<sup>154</sup> With the exception of Host Material, the Customer agrees to indemnify the Host against the actions of the Customer or Third Party and against claims by any "Third Party relating to the Web Site Material. This indemnification agreement will survive termination of this Agreement."<sup>155</sup>

"Validity of Agreement. If any term, provision, covenant, or condition of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the rest of the Agreement will remain in full force and effect and will in no way be affected or invalidated."<sup>156</sup>

[Printed Name of Host]

[Title]

[Signature]

[Printed Name of Customer]

[Title]

[Signature]

Dated \_\_\_\_\_

<sup>152</sup> *Id.* § 20B:33(2.5).

<sup>153</sup> *Website Hosting Agreement*, N.Y. FORMS LEGAL & BUS. §15A:35(6) (Sept. 2003).

<sup>154</sup> *Id.* §15A:35(7).

<sup>155</sup> *Id.*

<sup>156</sup> *Website Design Agreement*, N.Y. FORMS LEGAL & BUS. §15A:29(16) (Sept. 2003).