THE SUPERHIGHWAY TO JERICHO: GOOD SAMARITAN PROVISIONS

by Jonathan Band[1]

The New Testament Book of *Luke* tells the parable of the Good Samaritan. A man traveling from Jerusalem to Jericho was attacked by robbers, who beat him, stripped his clothes, and left him half dead on the side of the road. A priest passed by and did not stop to help. A Levite passed by and also didn't stop to help. Finally, a man from Samaria came by, and stopped to help the injured traveler. The Samaritan bandaged his wounds, took him to an inn, and paid the innkeeper to continue caring for the traveler. After telling the parable, Jesus urged his disciples to behave like the Samaritan, suggesting that that was the way to inherit eternal life.

In the United States, Good Samaritan laws refer to provisions which hold people harmless for injuries they may cause when doing good deeds they have no legal obligation to perform. The policy rationale for such laws is, quite simply, to encourage people to perform good deeds. This article argues that the Internet regulations which are proliferating at the federal and state level should include Good Samaritan provisions for Internet Service Providers (ISPs). While such provisions may not ensure eternal life for the ISPs, they might contribute to the safety of the Internet.

I. Introduction

Congress and the state legislatures recognize that the Internet has great potential to promote commerce and communication. At the same time,

[1] Jonathan Band is partner in the Washington, D.C. office of Morrison & Foerster. He is grateful for the assistance of Shahzad Bhatti in the preparation of this article.

legislators appear to believe that the Internet may threaten the policy rationales underlying existing laws, including regulation pertaining to securities, copyright, defamation, firearms, pharmaceuticals, indecency, privacy and gambling. Accordingly, legislatures are considering new Internet-related legislation at both the federal state levels.

In formulating these regulations, legislatures typically have fashioned "safe harbors" for the ISPs, absolving them of liability for unlawful conduct occurring on their service if the ISPs have no affirmative knowledge of the illegal activity nor derive any benefit therefrom. However, once they become aware of the unlawful activity, the ISPs typically have to respond appropriately. The rationale for the safe harbors is that given the volume of traffic, the ISPs can not effectively prevent the unlawful activity; and if the ISPs were held liable, valuable resources would be diverted away from expanding the Internet. Thus, imposing liability on the ISPs would not deter the unlawful conduct, but it would retard the growth of the Internet.

In creating the safe harbors, the legislatures generally have chosen not to place any affirmative duty on the ISPs to monitor their sites for unlawful activity. This is motivated by the realization that monitoring would be extremely costly, would probably slow the flow of information on the Internet, and ultimately may well be ineffective. Additionally, privacy advocates have opposed requirements which would in effect require ISPs to "snoop" on their subscribers. Moreover, civil liberties groups are uncomfortable with ISPs acting as the enforcer of laws.

In some cases, legislatures have chosen to include "Good Samaritan" provisions. Although the ISPs are not required to monitor their service for

unlawful activity, these provisions protect the ISPs from incurring liability in the event they, on their own initiative, engage in good-faith monitoring of their servers for illegal activity. In other cases, however, the legislatures have failed to adopt Good Samaritan provisions.

This omission of Good Samaritan provisions should be corrected. Although ISPs should not be required to monitor their services for the reason stated above, they should not be *discouraged* from doing so. In certain instances, due to their technological proximity to their subscribers' conduct, the ISP may be the party best situated to detect and eliminate the unlawful material.

The ISPs may be reluctant to engage in this voluntary monitoring, however, if they felt it would expose them to liability. This liability could come from three different directions. First, if the ISP incorrectly removed lawful material because of a mistaken belief that it was unlawful, the ISP could be liable to the subscriber. Second, if the ISP became aware of the unlawful material during the course of its voluntary monitoring, but failed to remove it, the ISP could be liable to the person harmed by the material. Third, and most ominous, through voluntary monitoring the ISP could acquire knowledge that arguably would satisfy the scienter requirement of a criminal statute. Legislatures can eliminate these disincentives to voluntary monitoring by enacting Good Samaritan provisions.

Without Good Samaritan provisions, ISPs are discouraged from taking proactive measures to prevent unlawful activity; instead, the statutory safe harbor regime forces them, as a practical matter, to wait passively until they have received appropriate notice from injured parties or law enforcement authorities.

This article first reviews the existing Internet-related Good Samaritan provisions. The article then suggests several statutes which could be improved substantially by the addition of Good Samaritan provisions. Finally, the article explores concerns which have been raised about Good Samaritan provisions.

II. EXISTING GOOD SAMARITAN LEGISLATION

A. Section 230(c) of the Communications Decency Act.

The broadest Internet-related Good Samaritan provision finds its genesis in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710, 1995 N.Y. Misc. LEXIS 229 (Sup. Ct. Nassau Cty. May 24, 1995). The plaintiff, Stratton Oakmont, Inc., an investment bank, was the subject of allegedly defamatory statements posted by an unidentified individual on Prodigy's "Money Talk" computer bulletin board. The board carried messages that, in connection with an initial public offering of stock, Stratton-Oakmont and its President had committed "major criminal fraud" and "100% criminal fraud." Stratton-Oakmont brought suit, alleging that the material constituted libel *per se*, that Prodigy was not merely the distributor but rather the publisher of the material, and that the "Board Leader" for "Money Talk" acted as Prodigy's agent.

On plaintiff's motion for partial summary judgment, the court imposed liability on Prodigy. The court ruled that having held itself out as a "family oriented computer network" that monitored the content of bulletin board postings for conformity with standards of taste set forth in its "content guidelines," Prodigy was not a mere distributor but rather a publisher, subject to liability for the defamatory content of the materials it carried. According to the court, Prodigy

had "arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards." *Id*. at *10.

Congress quickly recognized that the court's reasoning led to a peculiar result. If an ISP made no effort whatsoever to regulate the postings of its subscribers, it likely would be treated as a "distributor" and therefore would not incur defamation liability. On the other hand, if the ISP attempted to keep its service free of defamatory material, it would be treated as a "publisher," and would incur liability for any defamatory material that it failed to edit. Accordingly, Congress included Section 230(c) in the Communications Decency Act of 1996.[2] Although much of the Communications Decency Act was struck down as unconstitutional by the Supreme Court in *ACLU v. Reno*[3], Section 230(c) survived.

> Section 230(c) provides, in relevant part, 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).
>
> *Id.*

[2] Pub. L. No. 104-104, 110 Stat. 56, 138 (1996).

[3] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

Section 230(c)(1) protects an ISP from liability for defamatory statements posted by third parties, even if the ISP monitors its service and exercises "editorial" control by removing what it considers to be defamatory material. This provision, therefore, reverses the result in *Stratton-Oakmon*t.

Further, Section 230(c)(2) protects the ISP from liability for any action taken in good faith to restrict a user's access to material the user or the ISP believes to be obscene, lewd, violent, harassing, or otherwise objectionable, even if the material is constitutionally protected. The provision also frees the ISP from liability for making available the technical means of restricting access to this material. It is unclear how far the "otherwise objectionable" language reaches. Although it appears intended to apply to pornography or hate speech, a court could decide to stretch it to any material the ISP believes, rightly or wrongly, to be unlawful, e.g., fraudulent advertising.

Section 230(c)(1) has been the subject of a fair amount of litigation. *Zerun v. America Online, Inc.,* 958 F. Supp. 1124 (E.D. Va. 1997), 129 F.3d 327 (4th Cir.), *cert. denied*, 118 S. Ct. 2341 (1998) concerned a notice on an America Online ("AOL") bulletin board advertising the sale of offensive t-shirts relating to the Oklahoma City bombing and falsely identifying the plaintiff as the seller. After receiving death threats, the plaintiff complained to AOL. AOL removed the offending message, but similar messages appeared on AOL bulletin boards several times thereafter, each time leading to a flood of angry phone calls to the plaintiff. The plaintiff sued AOL for negligence under state law, contending that AOL should have removed the notices more promptly and should have taken

measures to prevent their reposting. AOL responded that plaintiff's causes of action were preempted by Section 230(c)(1).

The trial court agreed with AOL, and granted AOL's motion to dismiss. The court noted that allowing plaintiff's cause of action would conflict with one of the goals of the Communications Decency Act, *i.e.*, to encourage Internet service providers to self-censor material by not holding them liable for any defamatory material they failed to censor. *Id*. at 1134-35. On appeal, the Fourth Circuit affirmed the trial court's findings. Although the courts properly applied Section 230(c)(1) to the facts of this case, it does not appear that AOL did in fact take any proactive measures to eliminate the offensive material; it simply responded when notified of specific postings. In other words, AOL *did not* act as a Good Samaritan.

Another prominent case relating to Section 230(c)(1) is *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998). In *Drudge,* AOL had a contractual relationship with gossip columnist Matt Drudge whereby AOL would pay a flat monthly fee for the column which it made available to AOL subscribers. White House advisor Sidney Blumenthal brought an action for defamation against the gossip columnist and AOL claiming that they both should be held liable for defamatory statements found in the column. The District Court disagreed with the plaintiffs, holding that Section 230(c)(1) protected a service provider from any potential liability stemming from making a gossip column available to its subscribers. Despite AOL's contractual relationship with the columnist, the court held that AOL could not be held responsible because it had played no role in the actual writing, editing, checking, verifying or supervising of the column. Here,

too, AOL benefited from Section 230(c)(1) even though it did not act as a Good Samaritan.

B. Section 230 Outside the Defamation Context.

Section 230(c)(1) has also been invoked in cases not involving defamation. In *Doe v. America Online, Inc.*, 718 So.2d 385 (Fla. Dist. Ct. App. 1998), *review granted*, 1999 Fla. LEXIS 712 (Fla. April 12, 1999), a woman brought an action against AOL and an AOL subscriber for the sale via an AOL bulletin board of videotapes of the woman's eleven year old son engaged in sexual acts. The mother argued that AOL had violated Florida's statutes concerning obscenity and child pornography. AOL responded that it was protected by Section 230 of the CDA. A Florida state trial court agreed with AOL, and the appeals court affirmed, relying heavily on the Fourth Circuit's opinion in *Zeran*.

Another Florida court is currently deliberating the merits of extending Section 230(c)(1) to the issue of privacy. In *Aware Woman Center for Choice v. CompuServe, Inc.*, No. 99CV0005 (M.D. Fla. filed January 4, 1999), a Florida abortion clinic has brought an action against CompuServe for allegedly violating its rights to privacy. The abortion clinic has argued that CompuServe failed in its duties to protect the privacy of its employees and patients by allowing anti-abortion activists to post their state motor vehicle records online. CompuServe, Inc. has responded by invoking Section 230 as a defense to this action.

C. Child Online Protection Act

Subsequent to the Supreme Court's striking down much of the Communications Decency Act, Congress responded by enacting the Child

Online Protection Act ("COPA").[4] COPA attempts to correct the constitutional infirmities the Supreme Court identified in the CDA's prohibition on the distribution of material harmful to minors. COPA contains a specific safe harbor for ISPs:

> … a person shall not be considered to be engaged in making communications for commercial purposes to the extent that such person is-
>
> (1) a telecommunications carrier engaged in the provision of a telecommunications service;
>
> (2) a person engaged in the business of providing an Internet access service;
>
> (3) a person engaged in the business of providing an Internet information location tool; or
>
> (4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with … section 230 shall not constitute such selection or alteration of the content of the communication.

Id. at 112 Stat. 2681-737.

Subsection (4) of the safe harbor contains a Good Samaritan provision. Subsection (4) generally provides that an ISP which hosts a website which in turn violates the statute (i.e., it communicates to minors for commercial purposes material which is harmful to minors) is not liable to the extent the ISP does not select or alter the material. Significantly, the subsection adds that deletion of material does not constitute selection or alteration. In other words, if an ISP undertakes a monitoring program, and discovers material harmful to

[4] Pub. L. No. 105-277, 112 Stat. 2681-736 (1998).

minors, it can remove that material without fear that it will be considered to have "selected" the material that it failed to delete.

Shortly after its enactment, COPA was found unconstitutional by a district court. *American Civil Liberties Union v. Reno*, 31 F. Supp.2d 473 (E.D. Pa. 1999). COPA is currently under review by higher federal courts. Even if the Supreme Court once again invalidates Congress' effort to restrict distribution of harmful content to minors via the Internet, Congress likely will come back with yet another prohibition. Presumably the prohibition will provide a safe harbor for ISPs, and presumably the safe harbor will contain a Good Samaritan clause like COPA's.

D. Anti-Spam Legislation

Two anti-Spam measures introduced this Congress contain Good Samaritan provisions. In H.R. 2162, the Can Spam Act, a person may not use the equipment of an electronic mail service provider for the transmission of unsolicited commercial mail in violation of a posted policy of such provider. The bill does not require the e-mail service provider to adopt an anti-Spam policy, but shields it from liability if it does. Specifically, the adoption of an anti-Spam policy will not cause an ISP to lose its protections under Section 230 (c)(1) of the CDA. Moreover, the bill does not restrict the exercise of an editorial function by a service provider, nor limit an ISP's decision to restrict use of its equipment.

H.R. 1685, the Internet Growth and Development Act of 1999, contains a similar provision. However, two anti-Spam bills introduced in the Senate, S. 759 and S. 1910, do not contain Good Samaritan provisions.

E. Legislation at the State Level

State legislatures have also begun to regulate the Internet. Some of these regulations include Good Samaritan provisions. For example, California's anti-Spam legislation, Section 17538.45 of the Business and Professions Code, is very similar to the proposed federal anti-Spam bills discussed above, H.R. 2162 and 1685. Likewise, Washington House Bill 2752 (1998) prohibits the sending of an e-mail that uses an Internet domain name without authorization, or that contains false or misleading information in the subject line. The bill specifically provides that an interactive computer service may, upon its own initiative, block the receipt or transmission of commercial email it reasonably believes to violate the statute. Further, the bill states that no interactive computer service may be held liable for any such action taken on its own initiative.[5]

III. INTERNET REGULATIONS LACKING GOOD SAMARITAN PROVISIONS

Despite inclusion of Good Samaritan provisions in the statutes discussed above, Congress failed to insert such provisions in important pending and enacted Internet- related legislation.

A. Digital Millennium Copyright Act

In October 1998, Congress enacted the Digital Millennium Copyright Act ("DMCA").[6] Title II of the DMCA establishes a very elaborate set of safe harbors for four separate ISP functions: "mere conduit" services; automatic caching; hosting; and linking through information location tools. With respect to hosting

[5] H.B. 2752, 55th Leg., Regular Sess., at § 6(1) and (2) (Wa. 1998).

[6] Pub. L. No. 105-304, 112 Stat. 2860 (1998).

and linking, the ISP is free from liability unless it has: 1) actual knowledge of infringing activity; 2) awareness of facts and circumstances from which infringing activity is apparent; or 3) received a financial benefit directly attributable to the infringing activity in a case where it has "the right and ability to control" the activity. 17 U.S.C. 512. Further, to qualify for the safe harbor, the ISP must comply with a detailed "notice and takedown" regime. The DMCA clearly provides that the ISP has no duty to monitor its service in order to receive the safe harbor's protections.

While the DMCA's safe harbor framework is clearly good policy which will facilitate the growth of the Internet, it fails to provide ISPs with any sort of Good Samaritan provision encouraging proactive monitoring. Without Good Samaritan protections, ISPs are encouraged to remain passive until informed of infringement by third-parties.

For example, if the ISP chooses to monitor its service, uncovers what it believes to be infringing material, and removes it, the ISP could face liability to the subscriber. Under the DMCA, the ISP is sheltered from liability to the subscriber only if it removes material pursuant to proper notice from the content provider. Similarly, if the ISP voluntarily monitors its service, uncovers infringing material, and mistakenly fails to remove it, it might face liability to the content provider because it arguably had gained knowledge or awareness of the infringing activity. Moreover, the mere fact that a service provider engages in a monitoring program could lend weight to a content provider's argument that the ISP had the "right and ability to control" the infringing activity. Accordingly, the

ISP's most prudent course of action would be to engage in no monitoring, and instead wait until it receives notices from content providers.

The DMCA's disincentive to proactivity was pointed out to Congress while it is was drafting the DMCA, and Congress responded by including the following language in the Conference Report: "This legislation is not intended to discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program."[7]

This language does seem to make clear that monitoring should not lead a court to conclude that the ISP has "the right and ability to control the infringing activity," and therefore fall out of the safe harbor. At the same time, it is not clear how far this language will go. Will it protect an ISP which uncovers infringing material and mistakenly fails to remove it? Only a statutory Good Samaritan provision could truly eliminate the disincentives to proactivity built into the DMCA.

B. Securities Fraud

Another legal regime where Good Samaritan provisions would prove beneficial is securities fraud. S. 1015, the Online Investor Protection Act of 1999, introduced in May, 1999, doubles the penalties for violations of the federal securities laws if the Internet or other interactive computer service is used as part of the unlawful act or omission. The bill does not include any safe harbors for ISPs nor a Good Samaritan provision. Given the frequent use of the Internet for

[7] H. Rep. No. 105-796, at 73 (1998), *reprinted in* 1998 U.S.C.C.A.N. 639, 649.

a wide range of unlawful securities related activities, the aid of the ISPs should be enlisted through Good Samaritan provisions.

C. Internet Gambling

Due to concerns about web-sites circumventing federal gambling regulations, Senator Kyl introduced a bill which would prohibit engaging in gambling business over the Internet.[8] The bill contains a safe harbor for ISP. Among other exceptions, an ISP will not be liable for hosting or linking to a site where gambling is occurring, provided that 1) "the material or activity was initiated by or at the direction of a person other than the provider"; 2) the ISP has not knowingly permitted its service to be used to engage in gambling activity the ISP knows is unlawful; and 3) the ISP complies with the specified "notice and takedown" regime. *Id.* at § 1085(d).

Unfortunately, the Kyl bill's safe harbor does not include a Good Samaritan provision. Such a provision would enable an ISP to monitor its service without fear that the monitoring might provide it with the knowledge that would cause it to fall out of the safe harbor. Further, a Good Samaritan provision would make it clear that the ISP did not "initiate" any material or activity that it failed to remove.

IV. CONCERNS REGARDING GOOD SAMARITAN PROVISIONS

Critics of Good Samaritan provisions raise several concerns about the implications of enacting such provisions. One is that allowing ISPs to engage in monitoring of their servers will result in a chilling effect on First Amendment rights of free speech. Overly-enthusiastic ISPs may selectively monitor against

[8] S. 692, Internet Gambling Prohibition Act of 1999, 106th Cong. (1999), sponsored by Senator Jon Kyl.

particular types of content harming particular groups or viewpoints. In addition, ISPs, perhaps due to their lack of legal training, may be overly broad in what they determine to be illegal, thus hindering the Internet's use as a forum for ideas and informational exchange.

What these concerns fail to note is that counter-notification provisions, such as those in place in the DMCA, can provide a legislative safeguard for individuals whose content is wrongly removed from the Internet. *See* 17 U.S.C. 512(g) (1998). Even if content is mistakenly removed, the owner of the web-site would have the opportunity to respond in a timely manner to show that the removal was mistaken. Concerns about the over-zealousness of a particular monitoring program should also be tempered by the commercial reality that ISPs who are too swift to remove materials will likely suffer in profitability as potential customers take their business to competitors.

Another concern is that ISPs may abuse Good Samaritan provisions in the other direction; that is, use the provisions to justify inaction. The Good Samaritan provision contained in Section 230(c)(1) of the CDA has been cited as an example of this, particularly with respect to the *Drudge* case.

Regardless of whether one agrees with the result in *Drudge*, the result is not a function of the Good Samaritan principle. AOL, after all, was not acting as a Good Samaritan in the *Drudge* case. Rather, the result in *Drudge* is a function of the breadth of Section 230(c)(1)'s safe harbor for ISPs. Importantly, the safe harbors adopted by Congress since the CDA are significantly narrower than Section 230(c)(1). A Good Samaritan provision within a narrowly crafted ISP safe harbor is not prone to abuse.

V. CONCLUSION

There may well be certain circumstances when a Good Samaritan provision is inappropriate -- where the cost to society outweighs the benefit. However, as laws regulating the Internet multiply, the general rule should be to include Good Samaritan provisions, and to omit them only for good reason. The ISP often is the entity best placed to stop the unlawful conduct, particularly if it is working cooperatively with law enforcement authorities or the aggrieved party. Although *requiring* ISPs to monitor their services would be extremely burdensome and likely would adversely affect the growth of the Internet, ISPs should not be discouraged from voluntarily implementing monitoring or screen programs appropriate to their service. Legislatures should remove legal impediments to proactive measures by ISPs to prevent harmful activities on the Internet.