5-1-2014

Protecting The Victims Of Child Pornography: An Analysis Of The Current State Of The Law, With A View Towards Amending The CDA 230 Safe Harbor

William Evans Wells

PROTECTING THE VICTIMS OF CHILD PORNOGRAPHY: AN ANALYSIS OF THE CURRENT STATE OF THE LAW, WITH A VIEW TOWARDS AMENDING THE CDA 230 SAFE HARBOR

By: William Wells[1]

"It has become appallingly obvious that our technology has exceeded our humanity." Albert Einstein

This century old quote, spoken by the great inventor in reference to the atomic bomb age, tends to resonate loudly after a simple perusal of today's Internet. The Internet, a tool of such immense value, can and oftentimes does; reveal the very depth of human depravity. Nowhere is this depravation more exemplified than in the ever-expanding world of Internet child pornography. Despite its egregious nature, Internet child pornography continues to flourish, due to the difficulty of regulation in a technologically evolving medium and a disjointed regulatory scheme. Most shockingly, is the shelter provided to Internet service providers ("ISPs"), who

[1] The impetus for this paper was established during my time at the Ocean County, NJ Prosecutor's Office. While there, I worked in child sex crimes, where the gross injustice of the current state of child pornography laws came to light. This paper will explore the current state of those laws, with a view towards holding Internet Service Providers liable when they turn a blind eye to child pornography hosted or transmitted on their services.

escape liability arising out of the harm caused by child pornography hosted by or transmitted through their services.

The purpose of this paper is to further explore the relationship between child pornography, the Internet, and the ISPs, with an overarching focus on bringing closure to the victims of Internet hosted child pornography. More specifically, in Part I, this paper will focus on clarifying the murkiness surrounding child pornography and the Internet; Part II, will examine the pre-existing law and its effectiveness in helping victims of child pornography hold negligent ISPs responsible for knowingly hosting illegal material; and Part III, will argue that similar to Copyright Law, the safe harbor provision of Section 230 ("§ 230") of the Communications Decency Act ("CDA"), should be amended to hold ISPs accountable when they have actual knowledge that one of their websites is hosting child pornography.

PART I. THE STATE OF CHILD PORNOGRAPHY IN A TWENTY-FIRST CENTURY WORLD

a. *RELEVANT DEFINITIONS*

Traditional Child Pornography

Defining child pornography is not black and white. Audiovisual works, depicting real children engaged in sexual acts, is unambiguous and self-identifying.[2] Yet on the other end of the spectrum, still photographs of fully or mostly clothed teenagers who are posed in stances or contexts that strike some observers as sexualized may or may not constitute child pornography.[3] For the purpose of this paper, the term traditional child pornography includes this full range of examples, from the most egregious to the relatively benign.

[2] *See* New York v. Ferber, 458 U.S. 747 (1998) (referring to audiovisual works depicting real prepubescent children clearly engaged in sexual acts).
[3] Ann Bartow, *Copyright Law and Pornography*, 91 Or. L. Rev. 1, 40 (2012).

Self-Produced Child Pornography

In addition to traditional child pornography this paper, at times, will distinguish the relatively new concept of self-produced child pornography or underage sexting from traditional child pornography.[4] Loosely defined, self-produced child pornography is the modern term given to "the practice of sending or posting sexually suggestive text messages and images, including nude or semi-nude photographs, via cellular phone or over the Internet."[5] Naturally, to qualify as self-produced child pornography, the actor must be under the age of eighteen.[6]

ISPs

ISPs, as "gatekeepers to the Internet," play an integral role in this paper.[7] By definition, an ISP is a business or corporation that provides users access to the Internet.[8] Similarly, included categorically under the heading of ISP for the purpose of this paper, are online service providers ("OSPs").[9] Under Federal Law, ISPs and OSPs are given a broad definition and include any entity who "transmits, routs or provides connections for online communications," or "provides online services and/or network access" to Internet users.[10]

b. *THE HARMS OF CHILD PORNOGRAPHY*

[4] *See infra* p. 8, (Arguing that victims of self-produced child pornography are copyright holders.).
[5] JoAnne Sweeny, *Do Sexting Prosecutions Violate Teenagers' Constitutional Rights?*, 48 San Diego L. Rev. 951, 952 (2011) (defining sexting).
[6] 18 U.S.C. § 2256
[7] (The phrase, "gatekeepers to the Internet," has been coined by the author to capture the unique position occupied by ISPs in the world of the Internet.).
[8] Wikipedia, http://en.wikipedia.org/wiki/Internet_service_provider (last visited Dec. 2 2013).
[9] *See* Wikipedia, http://en.wikipedia.org/wiki/Online_service_provider (last visited Dec. 2, 2013) (noting that OSPs can be an ISP, email provider, news provider (press), entertainment provider (music, movies), search, e-shopping site (online stores), e-finance or e-banking site, e-health site, e-government site, etc.).
[10] 17 U.S.C. § 512 (k)(1)

The harm inherent in traditional child pornography has been well articulated by Congress, but bears repeating.[11] Similarly, The United States Supreme Court has highlighted the harm child pornography inflicts on its victims and the repeated exacerbation of this harm that occurs when the pornography is circulated.[12]

What is not well articulated is the harm caused by self-produced child pornography. It is quite clear that the same depth of research does not exist for child sexting as it does for traditional child pornography.[13] Often, this lack of comprehensive research leads to a wrongful focus on the lack of physical harm to the child in the production of a sext. In fact, some commentators argue that the harm of creating traditional child pornography through sexual abuse far outweighs the harm, if any, associated with voluntary self-production of child pornography.[14]

---

[11] *See* 18 U.S.C. § 2251, Sexual Exploitation of Children, The findings were:

> (1) the use of children in the production of sexually explicit material, including photographs, films, videos, computer images, and other visual depictions, is a form of sexual abuse which can result in physical or psychological harm, or both, to the children involved;
>
> (2) where children are used in its production, child pornography permanently records the victim's abuse, and its continued existence causes the child victims of sexual abuse continuing harm by haunting those children in future years;
>
> (3) child pornography is often used as part of a method of seducing other children into sexual activity; a child who is reluctant to engage in sexual activity with an adult, or to pose for sexually explicit photographs, can sometimes be convinced by viewing depictions of other children "having fun" participating in such activity;
> (4) child pornography is often used by pedophiles and child sexual abusers to stimulate and whet their own sexual appetites, and as a model for sexual acting out with children; such use of child pornography can desensitize the viewer to the pathology of sexual abuse or exploitation of children, so that it can become acceptable to and even preferred by the viewer;
> (5) new photographic and computer imaging technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from unretouched photographic images of actual children engaging in sexually explicit conduct…; *And see infra*, note 22.

[12] *See* Ferber, 458 U.S. at 759 (noting that "the materials produced [child pornography] are a permanent record of the children's participation and the harm to the child is exacerbated by their circulation").
[13] Susan H. Duncan, *A Legal Response Is Necessary For Self-Produced Child Pornography: A Legislator's Checklist For Drafting The Bill*, 89 Or. L. Rev. 645, 654-663 (2010).
[14] Id.

This comparison of the physical harm of self-produced child pornography and traditional child pornography is wrong because it does not account for the mental harms that often accompany an ill-advised 'sext.'[15] The permanent mental harm caused by sexting is exemplified by the tragic story of Jessica Logan, an eighteen year old who committed suicide after she sent a nude picture of herself to her boyfriend that was later spread throughout her Cincinnati-area high school.[16] Commenting on the mental abuse Jessica suffered, MSNBC.COM reported, "[t]he girls were harassing her, calling her a slut and a whore. She was miserable and depressed, afraid even to go to school."[17]

c. *THE PREVALENCE OF CHILD PORNOGRAPHY*

It is difficult to ascertain, with any degree of certainty, a consistent estimation regarding the amount of traditional child pornography available throughout the world. For instance, in 1996, one commentator noted that there was a vast, worldwide, commercial five billion dollar child pornography industry.[18] Other estimations place child pornography as a one billion dollar industry, exploiting about 1.5 million children.[19] Yet there are others who inexplicably deny the existence of commercial child pornography in the United States.[20] If we disregard the seemingly absurd contention of those who deny the existence of child pornography, and adopt a

[15] *See* Id. at 658 (noting readily identifiable harms from self-produced child pornography, [which] include: "mental anguish, harassment, economic harm, and social stigma").
[16] Clay Calvert, *Sex Cell Phones, Privacy, And The First Amendment: When Children Become Child Pornographers And The Lolita Effect Undermines The Law*, 18 CommLaw Conspectus 1, 3 (2009).
[17] Id.
[18] Amy Adler, *The Perverse Law of Child Pornography*, 101 Colum. L. Rev. 209, 232 (2001).
[19] Id.
[20] Id.

conservative estimate of the prevalence of child pornography, the numbers and prevalence remain alarming.[21]

Estimates regarding the prevalence of underage sexting are also hard to obtain. In a 2009 Associated Press-MTV poll, more than a quarter of the 1247 participants (ages fourteen to twenty-four) surveyed had been involved in some type of "naked sexting."[22] Critics may disregard the results of this survey because the participants did not constitute a random sampling of society, nor were they all underage. Regardless of this criticism, it's apparent that although not rising to epidemic levels, underage sexting is common.

d. THE INTERNET'S PROLIFERATION OF CHILD PORNOGRAPHY

The Internet has had a major impact on child pornography. By the mid 1980's, circulation of child pornography in the United States had waned drastically.[23] Since the advent of the Internet, what was once almost domestically obsolete has been dramatically spread and exploited. As Congress recognized, with ever-increasing technological capability at their fingertips, including peer-to-peer file sharing and encrypted IP addresses, pedophiles can stay one step ahead of law enforcement experts as they peddle child pornography.[24] It is safe to say,

---

[21] *See e.g.* New York Daily News, http://www.nydailynews.com/2.1353/child-porn-pervasive-catching-offenders-shooting-fish-barrel-article-1.380910 (last visited Dec. 2, 2013) (comparing the catching of online child pornography users to "catching fish in a barrel").

[22] Duncan, *supra* note 11, at 652.

[23] Adler, *supra* note 18, at 231.

[24] *See* 18 U.S.C. 2251, Sexual Exploitation of Children, Additional findings were:

> (6) computers and computer imaging technology can be used to --
>
> > (A) alter sexually explicit photographs, films, and videos in such a way as to make it virtually impossible for unsuspecting viewers to identify individuals, or to determine if the offending material was produced using children;
> >
> > (B) produce visual depictions of child sexual activity designed to satisfy the preferences of individual child molesters, pedophiles, and pornography collectors; and
> >
> > (C) alter innocent pictures of children to create visual depictions of those children engaging in sexual conduct;

that as the technological world has advanced to the twenty-first century, we have now entered "the golden age of child pornography."[25]

PART II: AN EXAMINATION OF THE PRE-EXISTING LAW AND ITS EFFECTIVENESS IN HELPING VICTIMS OF CHILD PORNOGRAPHY HOLD NEGLIGENT ISPS RESPONSIBLE FOR KNOWINGLY HOSTING ILLEGAL MATERIAL

a. *COPYRIGHT LAW*

---

(7) the creation or distribution of child pornography which includes an image of a recognizable minor invades the child's privacy and reputational interests, since images that are created showing a child's face or other identifiable feature on a body engaging in sexually explicit conduct can haunt the minor for years to come;

(8) the effect of visual depictions of child sexual activity on a child molester or pedophile using that material to stimulate or whet his own sexual appetites, or on a child where the material is being used as a means of seducing or breaking down the child's inhibitions to sexual abuse or exploitation, is the same whether the child pornography consists of photographic depictions of actual children or visual depictions produced wholly or in part by electronic, mechanical, or other means, including by computer, which are virtually indistinguishable to the unsuspecting viewer from photographic images of actual children;

(9) the danger to children who are seduced and molested with the aid of child sex pictures is just as great when the child pornographer or child molester uses visual depictions of child sexual activity produced wholly or in part by electronic, mechanical, or other means, including by computer, as when the material consists of unretouched photographic images of actual children engaging in sexually explicit conduct;

(10) (A) the existence of and traffic in child pornographic images creates the potential for many types of harm in the community and presents a clear and present danger to all children; and

(B) it inflames the desires of child molesters, pedophiles, and child pornographers who prey on children, thereby increasing the creation and distribution of child pornography and the sexual abuse and exploitation of actual children who are victimized as a result of the existence and use of these materials;

(11) (A) the sexualization and eroticization of minors through any form of child pornographic images has a deleterious effect on all children by encouraging a societal perception of children as sexual objects and leading to further sexual abuse and exploitation of them; and

(B) this sexualization of minors creates an unwholesome environment which affects the psychological, mental and emotional development of children and undermines the efforts of parents and families to encourage the sound mental, moral and emotional development of children;

(12) prohibiting the possession and viewing of child pornography will encourage the possessors of such material to rid themselves of or destroy the material, thereby helping to protect the victims of child pornography and to eliminate the market for the sexual exploitative use of children; and

(13) the elimination of child pornography and the protection of children from sexual exploitation provide a compelling governmental interest for prohibiting the production, distribution, possession, sale, or viewing of visual depictions of children engaging in sexually explicit conduct, including both photographic images of actual children engaging in such conduct and depictions produced by computer or other means which are virtually indistinguishable to the unsuspecting viewer from photographic images of actual children engaging in such conduct.; *And see supra*, note 9.

[25] Adler, *supra* note 18, at 231.

In certain situations, copyright law may afford victims of child pornography civil redress against ISPS. As way of background, at the most basic level, it is well understood that to qualify for copyright protection, a work must be original to the author.[26] Original, as the term is used in copyright, means only that the work is independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity.[27] The level of creativity required is extremely low, and work satisfies that requirement as long as it possesses some creative spark, no matter how crude, humble or obvious it might be.[28]

Historically, Congress' power to enact copyright laws is found in the Intellectual Property Clause of the United States Constitution, which authorizes Congress to "secur[e] for limited times to authors and inventors… the exclusive right to their respective writings and discoveries."[29] Although the original goal of the clause was to protect the progress of science, the protections have been expanded and applied to the arts, including photography and videography.[30]

A repeated victim of evolution, copyright law has long struggled to stay abreast of perpetually modernizing technology, which over time has made copyright infringement easy and commonplace.[31] Nowhere is this struggle more evident than in the provisions of Title 17 of the *United States Code* ("Title 17"), colloquially known as the Copyright Law of 1976.[32] Particularly demonstrative of this inability to adapt to technology is the Digital Millennium

[26] Feist Publications Inc. v. Rural Telephone Service Company, Inc., 499 U.S. 340, 345 (1991).
[27] Id.
[28] Id.
[29] U.S. Const. art. I, § 8, cl. 8.
[30] Id.
[31] *See* Wikipedia, http://en.wikipedia.org/wiki/Copyright_law_of_the_United_States (last visited Dec. 2, 2013) (noting the multiple instances of updated Copyright Law in the United States).
[32] *See* Copyright Law of the United States, http://www.copyright.gov/title17/circ92.pdf (last visited Dec. 2, 2013) (demonstrating the extent of the Copyright Law of 1976).

Copyright Act ("DMCA"), adopted as part of Title 17 in 1998.[33] The DMCA was promulgated in an attempt to keep pace with the Internet, "a technology that made copying and disseminating works around the world incredibly easy, on a scale previously unimaginable."[34] In assessing the effectiveness of copyright law as a tool of civil redress against ISPs, we need to examine the DMCA's most impactful provision, 17 USC § 512, which applies to virtually all commercial websites [ISPs] in the U.S. dealing with third-party content.[35]

The Profound Impact Of OCILLA's Nuanced Safe Harbors

The Online Copyright Infringement Liability Limitation Act ("OCILLA"), 17 U.S.C. § 512, provides four mutually exclusive safe harbors, insulating ISPs from liability in certain copyright infringement actions.[36] The impetus for establishing OCILLA was provided by the powerful ISPs who were concerned about their potential liability in the constantly fluctuating legal world of online copyright infringement.[37] The ISPs were bolstered by the Legislature, who feared that in the absence of clear legislation, ISPs who faced the possibility of primary or secondary liability in infringement actions would be hesitant to invest in Internet services and technologies.[38]

Eligibility under OCILLA

At the outset, to be eligible for one of OCILLA's four specified safe harbors, ISPs must adopt and reasonably implement a policy that addresses and terminates the accounts of repeat

[33] *See* The Digital Millennium Copyright Act of 1998, http://www.copyright.gov/legislation/dmca.pdf (last visited Dec. 2, 2013) (outlining the varying provisions of the DMCA).
[34] Edward Lee, *Decoding the DMCA Safe Harbors*, 32 Colum. J. L. & Arts 233, 233 (2009).
[35] *See* Id. (noting that virtually every ISP including, "Amazon, AOL, CNN, eBay, Facebook, Google, MySpace and YouTube," fall under the purview of the DMCA safe harbors).
[36] Steven Halpern, note, *New Protections For Internet Service Providers: An Analysis Of "The Online Copyright Infringement Liability Limitation Act"*, 23 Seton Hall Legis. J. 359, 387 (1999); *And* see 17 U.S.C.A. § 512 (a)-(d).
[37] Id. at 376.
[38] Id. at 378.

infringers, and must accommodate and not interfere with standard technical procedures for eliminating copyright infringement.[39] These eligibility requirements further reinforce the idea that ISPs, as "gatekeepers of the Internet," are uniquely positioned to combat and prevent illegal online activity. [40]

First Safe Harbor

First, an eligible ISP will not be held liable when infringing material is transmitted by a third party through a "system or network controlled or operated by the service provider."[41]

Second Safe Harbor

[39] 17 U.S.C.A. §§ 512 (i)(1)(A) and (i)(1)(B) provide:

> (i) Conditions for eligibility.--
>
> > (1) Accommodation of technology.--The limitations on liability established by this section shall apply to a service provider only if the service provider--
> >
> > > (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and
> > >
> > > (B) accommodates and does not interfere with standard technical measures.

[40] *See supra* p. 4.

[41] 17 U.S.C.A. § 512 (a) provides:

> (a) Transitory digital network communications.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if--
>
> > (1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
> >
> > (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
> >
> > (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
> >
> > (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
> >
> > (5) the material is transmitted through the system or network without modification of its content.

Second, the ISP will not be held liable in certain instances of system caching, where "acts of intermediate and temporary storage, [are] carried out through an automatic technical process for the purpose of making the material available to subscribers who subsequently request it."[42] System caching is the process of retaining unauthorized copies for limited times so that material may be made available for transmission to a subscriber at the discretion of the service provider.[43]

Third Safe Harbor

Third, most pertinent to the victims of child pornography, is OCILLA's limitation on liability for "information residing on the service provider's systems or networks at direction of the users." [44] Such limitation applies directly to chatrooms, websites, and other forum in which

[42] *See* 17 U.S.C.A. § 512 (b).
[43] Halpern, *supra note* 36 at 391.
[44] 17 U.S.C.A. § 512 (c) comprehensively provides:

> (c) Information residing on systems or networks at direction of users.--
>
> (1) In general.--A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider--
>
> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.
>
> (2) Designated agent.--The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:
>
> (A) the name, address, phone number, and electronic mail address of the agent.
>
> (B) other contact information which the Register of Copyrights may deem appropriate.
>
> The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

users post information; areas of the Internet that often give rise to trading in child pornography.[45] To take advantage of the safe harbor, the ISP must satisfy three criteria.[46]

First, the ISP must not have actual knowledge of the infringing material or activity conducted by the Internet user.[47] This requirement insulates the ISP from actively policing their

---

(3) Elements of notification.--

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B) (i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

[45] *See* Halpern *supra note* 36 at 393 (supporting the inference that an eligible ISP will be insulated from copyright liability in most child pornography cases because of the provisions of 17 U.S.C. § 512 (c), and the fact that most pedophiles participate in the child pornography trade in these type of forums).

[46] *See e.g.* 17 U.S.C. § 512 (c)(1).

[47] 17 U.S.C. A. § 512 (c)(1)(A)(i).

services for infringing material and prevents them from being held strictly liable for the actions of their users. Actual knowledge is established by the victim filing a takedown notice under the provisions of the DMCA, which must take the form of a written notice to the service provider.[48]

Second, the ISP must not have profited from the infringing activity if the service provider has the ability and right to control the activity.[49] In determining whether a service provider has profited from infringing activity, courts should look to see if the value of services provided subsisted in "providing access to infringing material."[50] An argument that the ISP has not profited from the infringing activity is hard to make in today's online environment, as almost every model of service contains a profit making mechanism.[51]

Finally, the ISP must have a reporting mechanism in place, and upon notice of infringing activity, expeditiously remove access to the infringing activity.[52] Generally, reporting mechanisms are hosted internally by the ISP, and are easily accessible to the users.[53]

Fourth Safe Harbor

Lastly, OCILLA provides limitation on liability for ISP is linking or referring users to an Internet location, which contains infringing material or infringing activity.[54] To qualify for this provision, such linking must be accomplished by the use of "information location tools," including a reference, index, directory, hypertext link, or pointer.[55] Under certain circumstances,

[48] *See infra* ps. 14-15.
[49] 17 U.S.C.A. § 512 (c)(1)(B).
[50] H.R. Rep. No. 105-551. Pt. 2 at 54 (1998).
[51] *See* Forbes, http://www.forbes.com/sites/quora/2013/02/26/how-do-free-services-on-the-web-make-money/ (last visited Dec. 2, 2013) (demonstrating the various money making models followed by most ISPs).
[52] 17 U.S.C.A. § 512 (c)(1)(C).
[53] *See* Google, http://support.google.com/legal/troubleshooter/1114905?hl=en (last visited Dec. 2, 2013) (demonstrating Google's current reporting mechanism).
[54] 17 U.S.C.A. § 512 (d).
[55] H.R. Rep. No. 105-551, Pt. 2, at 56 (1998).

ISPs engaging in these activities may avail themselves of OCILLA's limitations on liability, including: (1) when the ISP did not have actual knowledge of the infringing activity and (2) when the ISP takes steps to expeditiously remove the link to the infringing material.[56]

Takedown Notice

Under OCILLA, to be viable, the takedown notice must comply with the Act's requirements. For instance, the takedown notice must be in writing and delivered to the service providers designated agent.[57] In addition, the notice must substantially comply with six additional requirements; the absence of one or several in certain circumstances, not necessarily being fatal to the copyright holder's infringement claims against the ISP.[58] Once the ISP is provided with actual notice of the infringing material, the ISP is deemed to have actual knowledge of the infringement, and must notify the alleged third party infringer of the action.[59] The ISP must also take steps to expediently remove or disable access to the infringing material.[60]

[56] Halpern, *supra note* 36 at 396.
[57] Id.
[58] 17 U.S.C.A. § 512 (c)(3)(a)(i)-(vi) requires the following:

> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
> (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

[59] 17 U.S.C.A. § 512 (g)(2)(A).
[60] 17 U.S.C.A. § 512 (c)(1)(C).

Remedies

Injunctive relief is the primary remedy available to copyright holders under the provisions of OCILLA.[61] Courts must consider four enumerated factors when deciding whether to grant injunctive relief; and upon deciding to grant an injunction, will craft relief that is consistent with those promulgated by OCILLA.[62] For instance, when the service provider is a passive conduit for the infringing conduct, (1) the court may order the service provider to terminate the accounts or subscriptions of those who are using the service provider's system to engage in infringing activities, (2) or the court may order the service provider to take reasonable steps to block access to identified and specific locations outside the United States.[63] When the service provider is acting in the capacity of either a system cache, an information location tool, or a network hosting information at the direction of the user, (1) the court may enjoin the service provider from providing access to the infringing material, whether the material or activity is occurring at a particular online site or on the service provider's own network, (2) the court may order the service provider to terminate accounts or subscriptions it has with the entities engaging in infringing activities, (3) or the court may issue any injunctive relief that it believes is necessary to restrain or prevent infringement.[64]

---

[61] *See* 17 U.S.C.A. § 512 (j).

[62] 17 U.S.C.A. § 512 (j)(2) requires the following considerations:

> (A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;
>
> (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;
>
> (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and
>
> (D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

[63] 17 U.S.C.A. §§ 512 (j)(1)(B)(1) and (j)(1)(B)(2).

[64] 17 U.S.C.A. §§§ 512 (j)(1)(A)(i), (j)(1)(A)(ii) and (j)(1)(A)(iii).

The Application of Copyright Law to Traditional Legal Pornography

It has become increasingly clear that traditional legal pornography is copyrightable. In 1979, the Fifth Circuit held that obscenity was not a defense to copyright infringement of pornographic materials because nothing in the Copyright Act of 1909 precluded the copyright of obscene.[65] In that seminal case, the Fifth Circuit concluded that holding obscene materials copyrightable furthered the pro-creativity purposes of the Copyright Act and of congressional copyright power generally.[66]

Most courts are willing to accept the idea that legal pornography is afforded copyright protections.[67] Nearly three years later, the Ninth Circuit adopted the Fifth Circuit's position on the copyright of obscene materials.[68] Similarly in 2004, a third court decided to follow Mitchell Brothers decision.[69]

The Application of Copyright Law to Child Pornography

At first glance, it is quite clear that child pornography falls outside the protections of copyright law, as it is "non-progressive" and "non-useful."[70] Undoubtedly, such a conclusion arises when one considers the ongoing harm inherent in the production and dissemination of child pornography.[71] But if we dig a little deeper, it becomes obvious that an argument can be

[65] Mitchell Bros. Film Group and Jartech, Inc. v. Cinema Adult Theater, 604 F. 2d 852 (5th Cir. 1979).
[66] *See* Id.
[67] *But see* Devils Films, Inc. v. Nectar Video, 29 F. Supp. 2d 174, 175-77 (S.D.N.Y. 1998) (the District Court holding that the pornographic films were "obscene," and not afforded copyright protections from infringement).
[68] *See* Jartech, Inc. v. Clancy, 666 F. 2d 403, 406 (9th Cir. 1982) (remarking that "the leading treatise on copyright has called the Fifth Circuit's Mitchell Brothers case 'the most thoughtful and comprehensive analysis on the issue '"[the application of copyright to traditional legal pornography]).
[69] Bartow, *supra note* 2 at 36, *citing* Nova Products, Inc. v. Kisma Video, Inc., 2004 U.S. Dist. LEXIS 24171, at *10 (S.D.N.Y. Nov. 30, 2004) (describing the Mitchell Brothers decision as "well-reasoned and scholarly").
[70] Bartow, *supra note* 3.
[71] *See supra* ps. 4-5.

made that victims of self-produced child pornography may, in certain situations, have a copyright claim against ISPs.[72]

Under the tenets of traditional copyright law, victims of self-produced child pornography are creators as they produce the images or video themselves, and should be able to claim a copyright interest in the work.[73] As copyright holders, victims of self-produced child pornography have the power to serve a takedown notice to the ISP who is providing access to the pornographic material.[74] This power gives the victim, as copyright holder; leverage to force the ISP to take action in removing or preventing access to the infringing pornographic material. If the ISP fails to comply with the takedown notice, the victim can seek injunctive relief through the courts.

The ongoing case of texxxan.com is instructive in illustrating the potential remedial power copyright law gives to victims of self-produced child pornography. In this case, the website specialized in the particularly evil practice of "revenge porn," where individuals posted self-produced images of former girlfriends or wives, out of spite.[75] The victims, including two who are underage, brought a class action lawsuit against the website and the ISP seeking damages.[76] Although, the victims did not need to assert a copyright action in this particular case, as the website was shut down after public outcry, in the future, similarly situated victims can

[72] It becomes critical at this juncture of the analysis to recall the definition of self-produced child pornography; *See supra* p. 3-4.
[73] *But see* supra p. 3 (By definition, victims of traditional child pornography do not have remedies based in copyright law because they are not considered creators under the law.).
[74] *See* 17 U.S.C.A. § 201
[75] Jolt Digest, http://jolt.law.harvard.edu/digest/privacy/unwanted-exposure-civil-and-criminal-liability-for-revenge-porn-hosts-and-posters (last visited Dec. 2, 2013).
[76] BetaBeat, http://betabeat.com/2013/02/two-alleged-underage-victims-sign-onto-revenge-porn-lawsuit-against-texxxan-com-and-godaddy/ (last visited Dec. 2, 2013) (noting that two underage victims have joined the lawsuit against texxxan.com and GoDaddy).

assert a copyright action to compel the ISP to take corrective measures and eliminate or block access to the infringing material.

b. COMMUNICATIONS DECENCY ACT ("CDA," "ACT," or "§ 230")

The safe harbor provision of the CDA represents another Congressional attempt to regulate the Internet, and perhaps, a potential avenue of recourse against negligent ISPs for victims of child pornography.[77] The impetus for CDA § 230 was provided by a 1995 court decision, which held an ISP liable for defamation when the ISP exercised editorial control over content provided by a third party.[78] In that case, the defendant, an ISP who hosted an online message board, was compared to a newspaper editor; in the way it removed obscene material from board.[79] The Court opined that under the CDA, the ISP's actions were equivalent to those of a publisher, and therefore, the ISP was liable for the defamatory remarks posted on the message board.[80]

Congress, concerned that the Stratton decision would prevent ISPs from policing their own content, amended the existing CDA by adding § 230. As evidenced by Senator James Eton's introduction to the CDA, the Act was established with the dual intent of promoting free speech on the Internet, while allowing ISPs to self-regulate without fear of liability.[81] In light of these intentions, once passed, § 230 had two effects: (1) it regulated harassment, indecency, and obscenity online and (2) it determined that operators of online services would not be held liable

[77] *See* 47 U.S.C. § 230.
[78] KrisAnn Norby-Jahner, *"Minor" Online Sexual Harassment And The CDA § 230 Defense: New Directions For Internet Service Provider Liability*, 32 Hamline L. Rev. 207 (2009).
[79] *See* Id. *citing* Stratton Oakmont v. Prodigy Serv., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, 12-13 (N.Y. Sup. Ct. May 25, 1995).
[80] Id.
[81] Id.

for illegal conduct in the process of self-regulation.[82] At controversy, and most relevant to this paper, is the far-reaching ramifications of the latter effect, which has been interpreted to provide a virtually per se safe harbor to ISPs.[83]

The CDA's safe harbor is established by § 230 (c), which indicates that ISPs will not be "treated as the publisher or speaker of any information provided by another information content provider."[84] More specifically, to gain the benefit of the safe harbor, the ISP must satisfy three criteria. First, the defendant must be a "provider or user" of an "interactive computer service."[85] Second, the Plaintiff's cause of action must treat the service provider as the "publisher or speaker" of the harmful information at issue.[86] Finally, the harmful information must be provided by a third party, colloquially known as the "information content provider."[87] Given the function of the typical ISP, as a passive conduit for the posting and sharing of content online, most, if not all ISPs, will be able to escape liability under this safe harbor provision.

Several courts have interpreted the CDA's safe harbor provision as providing complete immunity to ISPs from liability stemming from cyber tort actions.[88] At the outset, courts were willing to extend complete immunity in cases of defamation. In Zeran v. America Online, Inc., the Fourth Circuit held that § 230 "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of

[82] Id.
[83] (This answers in the negative, the original question of whether the CDA provides an avenue of civil recourse for victims of child pornography against the ISPs.).
[84] 17 U.S.C.A. § 230 (c)(1).
[85] Id. at (c)(1)(2).
[86] Id. at (c).
[87] Id. at (c)(1).
[88] Wikipedia, http://en.wikipedia.org/wiki/Section_230_of_the_Communications_Decency_Act#Limits (last visited Dec. 2, 2013)

the service."[89] In that case, the plaintiff was allegedly defamed by an unidentified user of America Online's ("AOL") bulletin board service, but was unable to bring claims against the poster because of missing records.[90] The Fourth Circuit's holding, left the ISP judgment proof, even when the ISP may have had actual knowledge of the tort, and had the ultimate effect of preempting all state tort law claims against ISPs.[91]

The Application of § 230 to Child Pornography

Alarmingly, the broad immunity exemplified by the *Zeran* Court's decision, has been extended beyond defamation cases, and has touched the realm of child pornography.[92] For the first time, in 1998, a Court addressed the intersection of child pornography and CDA Section 230.[93] The victim, an eleven-year-old boy, was sexually assaulted by the defendant, his schoolteacher.[94] The encounter was videotaped, and the defendant proceeded to discuss the attack and make arrangements to sell the tape in an AOL chatroom.[95] The victim's mother sued AOL for negligence, claiming that AOL knew or should have known, that the defendant and others like him used the service to market and distribute child pornographic materials, that it should have used reasonable care in its operation, that it breached its duty, and that the damages were reasonably foreseeable as a result of AOL's breach.[96] Citing § 230, the Court dismissed

[89] 129 F.3d 327, 330 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998).
[90] Id.
[91] *See* Id. at 331 (Plaintiff is contending that "he provided AOL with sufficient notice of the defamatory statements appearing on the company's bulletin board.").
[92] Doe v. America Online Inc., 718 So. 2d 385 (Fla. Dist. Ct. App. 1998); Doe v. Myspace, 528 F.3d 413 (5th Cir. 2008).
[93] American Online, Inc., 718 So. 2d.
[94] Id. at 386
[95] Id.
[96] Id.

the case, holding that AOL was not liable because it did not edit or withdraw the posting.[97]

Similarly, in 2007, the United States District Court for the Eastern District of Texas extended complete immunity in a case arising out of the trading of child pornography in a Yahoo! hosted e-group, aptly named the Candyman group.[98] Here, Plaintiffs, the parents of the victim, sought to hold Yahoo! civilly liable for profiting from the trade of child pornography. [99] To circumvent the safe harbor provision of the CDA, Plaintiffs argued that Yahoo! had actual knowledge of the illegal conduct, and did nothing to rectify the situation.[100] In upholding Yahoo!'s motion to dismiss, the District Court emphasized the holding in Zeran, and found that the CDA's safe harbor extends to situations where the service provider has actual knowledge of the illegal activity. [101]

These two cases exemplify the problem with § 230 as applied to the issue of child pornography. Quite ironically, the CDA, an act that was originally established to protect children has paradoxically gone the other way, giving ISPs a license to completely ignore the problem of child pornography on their websites, by preempting all state tort law claims.[102]

Why § 230 should be Amended

[97] Id.
[98] 2006 WL 3813758
[99] Id.
[100] Id. at 6.
[101] *See* Id. at 22 (Noting that this case be dismissed with prejudice for the defendants.).
[102] Devon I. Peterson, *Child Pornography on the Internet: The Effect of Section 230 of the Communications Decency Act on Tort Recovery for Victims against Internet Service Providers*, 24 Haw. L. Rev. 763, 768 (2002), *citing* Michelle J. Kane, *Internet Service Provider Liability: Blumenthal v. Drudge*, 14 Berkeley Tech. L. J. 483, 501 (1999) (noting that "while Congress and the court certainly acted admirably in attempting to encourage the development of the Internet, both erred in excusing [ISPs] from [their] duty under the common law to guard against the damage to others' reputations. A more cautious approach to regulation on the Internet, and more restraint in interpreting such regulations, would allow the Internet to develop as a forum of free speech while continuing to offer legal protection to those who may be damaged by careless citizens of cyberspace.").

As highlighted by the three aforementioned cases, the judicially broadened § 230 should be amended for three primary reasons: 1) the broadened view of § 230 is contrary to the Legislative history of the Act; 2) the broadened view of § 230 provides no incentive to the ISPs to police child pornography on their websites; and 3) under the current interpretation of § 230, victims of child pornography are denied recovery, which cuts deeply against established public policy concerns.[103] I will discuss each reason in turn.

The True Legislative Purpose of § 230

The legislative history of § 230 does not support a broadened interpretation of the safe harbor provisions. Although the history is devoid of any specific debate on the issue of providing complete immunity to ISPs from suits under state tort law for hosting third party content, there is clear indication that such an interpretation is not justified.[104] But what is quite clear from the legislative history is that the Legislature's *only* purpose in establishing § 230 was to "reverse the preposterous result in Stratton."[105] Thus, the broadened judicial interpretation of § 230 is not explicitly or implicitly supported by the legislative history of the Act, and has gone so far beyond the protections that the Legislature intended to grant to ISPs, that states are now severely limited in their ability to protect victims of child pornography.[106]

---

[104] Id. at 782, *citing* Jonathan A. Friedman & Francis M. Buono, *Limiting Tort Liability for Online Third-party Content Under Section 230 of the Communications Act*, 52 Fed. Comm. L. J. 647, 652 (2000) ("[C]ritics point to the plain language and legislative history of section 230 to support the view that Congress enacted section 230 to immunize [ISPs] only from publisher, not distributor, liability.").

[105] Id.

[106] Id., *And see* 17 U.S.C.A. § 230 (b) providing that, it is the policy of the United States:

> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

The Need to Incentivize ISPs

Following naturally from the Legislature's purpose of reversing the Stratton decision, was a strong desire to remove any disincentive for self-regulation on behalf of the ISPs.[107] Yet, instead of spurring more regulatory action, the Act has created complete immunity from state tort liability, and ironically, incentivized Service providers to do nothing.[108] This paradoxical result is not wasted on the most skeptical of legal scholars, indeed even some courts seem frustrated with outcome, referring to the Zeran outcome, the District Court for the District of Columbia noted that; "it appears to this court that AOL in this case has taken advantage of all the benefits conferred by Congress in the Communications Decency Act, and then some, without accepting any of the burdens that Congress intended."[109]

Given the ISP's unique position as gatekeepers to the Internet, it is crucially important to amend the Act to incentivize self-regulation of content hosted on their websites, including child pornography.[110] Recently, we have seen a shining example of the viability of ISP self-regulation in the realm of child pornography.[111] Pressured by a large upwelling of public outcry in the

---

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking schools who use the Internet and other interactive computer services;

(5) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(6) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

[107] Id. at 788.

[108] *See supra* ps. 21-22, (Noting complete inaction on behalf of ISPs to regulate child pornography on their websites, even when they allegedly have knowledge of the illegal material.).

[109] Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998).

[110] *See supra* p. 4, (As I analogize ISPs to "gatekeepers.").

[111] DailyMail, http://www.dailymail.co.uk/news/article-2509036/Google-blocks-child-porn-Internet-giant-axes-links-sex-abuse-websites.html (last visited Dec. 2, 2013).

United Kingdom, Google and Microsoft, two of the largest ISPs, have integrated technology into their popular search engines that is designed to prevent over 100,000 search terms that are calculated to lead to images or videos of child pornography.[112] The establishment of this screening program represents a stunning U-turn in the position of these two ISPs, who only a short time ago were arguing that the self-regulation of child pornography shouldn't be done.[113] If the public's outcry can so effectively incentivize service providers to regulate child pornography, it seems intuitive that § 230 should be amended to serve this end as well.

The Need to Allow Recovery for Victims of Child Pornography

The most persuasive reason for narrowing the § 230 safe harbor is to allow recovery for victims of child pornography who have suffered because of the actions or inactions of the ISPs. As noted earlier, when the Internet is used to distribute obscene and illegal material, the injury to the victim is real, continual and unending.[114] For example, although both child pornography cases cited in this note were dismissed prior to a jury trial, and thus, we don't know the full extent of the evidence, it seems readily apparent that the inaction of both AOL and Yahoo! played an integral role in the harm.[115] If these ISPs were indeed on notice of the illegal material, their negligence in removing it should be punishable, as they are best positioned to eviscerate the problem and failure to do so further exacerbates the harm.[116] This position of action on behalf of the ISPs, is further necessitated if we consider the general evasiveness of the modern day pedophile, and the likelihood that the actual perpetrator is rarely, if ever identifiable to be named

[112] Id.
[113] *See* Id., (Noting that the ISPs argument against self-regulation was not that it "couldn't be done," but that it "shouldn't be done.").
[114] *See supra* ps. 4-5.
[115] *See supra* ps. 21-22.
[116] (Especially given the ISPs position as "gatekeepers to the Internet.").

as a defendant by the victim.[117] As it currently stands, § 230 removes any option of redress for the victim, as it completely insulates the ISPs from liability, even if the ISP has actual knowledge of the situation. In order to protect children, § 230 needs to be amended, to allow victims of child pornography a course of redress against negligent ISPs who have actual knowledge of illegal content and refuse to remove the material.[118]

PART III. SIMILAR TO COPYRIGHT LAW, § 230 SHOULD BE AMENDED TO HOLD ISPS LIABLE WHEN THEY HAVE ACTUAL KNOWLEDGE THAT ONE OF THEIR SERVICES IS HOSTING CHILD PORNOGRAPHY.

a. SOLUTION

In searching for a narrowing solution to § 230, it is instructive to juxtapose the Act with copyright law provisions discussed, supra.[119] Fundamentally, OCILLA's greatest attribute is the consummate balance it strikes between protecting the interests of the ISPs and the victims of self-produced child pornography, by promoting the continuing growth of the Internet, while still imposing self-regulatory action on ISPs.[120] The key to facilitating this balance is the actual knowledge requirement of the provision, which does not trigger the possibility of liability until the ISP is placed on actual notice of the infringing material.[121]

An amendment to § 230 that reflects the safe harbor provisions of OCILLA, will successfully strike a balance between the Legislative policies, which constitute the underpinnings of § 230, including the policies that call for promotion and continued development of the Internet

[117] *See supra* ps. 6-7, (Noting that in today's age of technology, pedophiles have more resources at their fingertips to participate in trading child pornography.).
[118] (This cry for a narrowing of § 230 cannot be viewed as controversial or novel, in light of the strong public interest to protect children and eliminate child pornography from circulation.).
[119] 17 U.S.C.A. § 512.
[120] *See supra* ps. 8-18, (Highlighting the self-evident regulatory action of the ISPs, incentivized by the possibility of liability in situations where the ISP fails to expeditiously remove or prevent access to the infringing material.).
[121] *See* 17 U.S.C. A. § 512 (c), (Actual knowledge provision.).

and the protection of children.[122] Accordingly, § 230 should be amended to reflect the actual knowledge and takedown notice requirements of OCILLA.[123]

On a practical level, this amendment will work as follows. Similar to the requirements of OCILLA, ISPs will be required to designate an agent who will receive complaints regarding illegal content hosted or transmitted on their services.[124] Upon receipt of a takedown notice regarding child pornography, the ISP will have a reasonable amount of time to remove or prevent access to the content.[125] Failure to take action will open the ISP up to state tort liability and provide the victim with the right to pursue civil damages against the ISP.

b. CONCLUSION

I am not that naïve to believe that an amendment to § 230, which provides virtually similar provisions to that of OCILLA, will have a major impact on eradicating the circulation of child pornography. Yet, I think such an amendment will have the desirable effect of narrowing § 230's safe harbor, and facilitating some form of regulatory action on behalf of the ISPs. The time has come to hold the gatekeepers to the Internet responsible, when they knowingly ignore child pornography hosted or transmitted through their services.

[122] *See* 17 U.S.C.A. §§ 230 (b)(1) and (b)(5).
[123] *See* 17 U.S.C.A. § 512.
[124] *See* Id., (As in copyright law, the designation of an agent prevents both the ISP and the victim from being burdened with the cost of initiating litigation.).
[125] Id.