STANFORD
LAW & POLICY REVIEW

SHOOTING THE MESSENGER: AN ANALYSIS OF THEORIES OF CRIMINAL LIABILITY USED AGAINST ADULT-THEMED ONLINE SERVICE PROVIDERS

Lawrence G. Walters

VOLUME 23 2012 ISSUE 1

23 Stan. L. & Pol'y Rev. 171

Stanford Law and Policy Review
2012

Symposium: Adult Entertainment

SHOOTING THE MESSENGER: AN ANALYSIS OF THEORIES OF CRIMINAL LIABILITY USED AGAINST ADULT-THEMED ONLINE SERVICE PROVIDERS

Lawrence G. Walters [a1]

Introduction

Since the inception of the Internet, Congress has attempted to keep pace with technological developments in cyberspace, and the unique legal issues they spawn. Occasionally, lawmakers demonstrate a flash of competence, but U.S. law is infamous for its tendency to lag behind technology at a seemingly embarrassing pace. The potential criminal exposure facing providers of online services is one of the areas that have received a startling lack of attention from legislators or the courts, despite the gargantuan stakes facing this industry, and the increasing popularity of social networking websites that allow third-party users to upload content. Intellectual property issues impacting Internet communications are being hashed out at a rapid pace, as evidenced by the recent filing of a slew of copyright infringement cases-- particularly by the producers of adult-oriented content. [1] In fact, the adult entertainment industry has taken the lead in exploring the contours of "end user" copyright infringement liability, [2] and use of fingerprinting technology designed to ***172** identify infringing material on the Internet. [3] One online adult entertainment company is even suing its own members for copyright infringement, after tracking their alleged activity in illegally sharing content they had accessed as members. [4] Using these and other methods, the adult industry hopes to stamp out online piracy by 2012. [5] Since the adult industry has historically taken the lead in pushing the development of new technology, [6] it is not surprising that legal disputes involving erotic material are driving the development of Internet law in general.

Issues relating to the civil liability of so-called "online service providers" (OSPs), such as "tube sites"--based on user-generated material--are also percolating in the lower courts, with the Viacom v. YouTube case expected to be the one that reaches the U.S. Supreme Court. [7] But starkly absent from the current spate of litigation involving website operators' liability for online activity is any substantial case law or legislation detailing the contours of potential criminal liability facing OSPs, based on the acts of third parties such as their customers or end users. Little has been written on the subject from an academic perspective, either. Exacerbating the lack of legal guidance on this issue are the incredibly harsh potential criminal sanctions facing any OSP targeted by state or federal law enforcement authorities under these circumstances. Criminal laws, including vague accomplice liability statutes, [8] can result in draconian legal penalties being imposed on website operators having only tangential involvement in the alleged illegal conduct. Such penalties can include years in prison for the responsible individuals, seizure of all business assets, and millions of dollars in fines. [9] Yet those companies that provide Internet-based services to third parties, such as hosts, search engines, tube sites, and online dating sites, remain largely in the dark when it comes to their responsibilities and liabilities relating to compliance with criminal laws.

As explained more fully below, those OSPs engaged in the controversial ***173** realm of providing access to adult-themed material fall into a 'gray' area of the law, and are potentially subject to targeting by law enforcement authorities based on the

type of material uploaded by their customers--much more so than their mainstream OSP counterparts. Such disparate treatment of adult-oriented OSPs, based on the content of the speech flowing through their networks, raises substantial First Amendment concerns relating to viewpoint discrimination. [10] Irrespective of the eventual constitutional defenses that might ultimately be available to the OSP, the danger of prosecution persists. The potential for getting caught up in a criminal indictment based on the actions of third-party Internet users has historically been seen as a cost of doing business, even as the OSP industry continues to blossom in recent times with the infusion of social networking and user-generated content sites. Nevertheless, today the line between legal protection and serious criminal liability for OSPs is difficult to discern, especially for operators who invite, or focus on, adult-themed materials originating from their subscribers. While some support for a claim of immunity can be found in federal statutes--at least with respect to the application of state criminal laws--the contours of such protection have not been well defined, and prosecution for federal criminal offenses remains a substantial concern. As a result, the affected businesses remain wholly uncertain of both their exposure and the compliance obligations expected of them by law enforcement authorities.

This article seeks to explore the relatively unmapped territory of potential criminal liability for OSPs providing online access to adult content submitted by their third-party users. Part I examines the evolution of service provider liability beginning with the first criminal prosecution against an OSP and the subsequent proliferation of user-generated content websites. Part II details the recent criminal actions against OSPs by state and federal authorities, and illustrates the legal challenges facing these companies. Part III discusses the existing legislative protections provided to OSPs, primarily in the context of civil liability. Part IV addresses potential criminal charges facing OSPs under various state and federal statutes. Finally, Part V looks at the existing state of affairs and explores the need for new federal legislation clarifying the status of service provider liability in the criminal context for the future.

I. The Evolution of Online Service Provider Liability

The Internet, if not by choice then most certainly by default, has become the preferred venue for disseminating speech. Megaphones and telephones have given way to keyboards and forum boards--the World Wide Web has changed the flavor of public discourse forever. Because of the web's popular perception as the ultimate public forum for free expression, it may be easy to overlook the ***174** fact that private entities are responsible for enabling such a forum. From website hosts to forum board operators to social networking sites, the free flow of end-user communication online depends on the willingness of a private entity to enable these services. Any such business must evaluate and manage its potential legal exposure--from both civil and criminal perspectives. Utilizing a simple cost-benefit analysis, OSPs will be inclined to cease offering a forum for communication if the risks are too high to justify the anticipated profit. The forum of communication will then cease to exist. While no cognizable First Amendment claims can be asserted against an OSP based on a pure business decision to cease operating based on liability concerns, given the lack of governmental attention to this problem, free speech interests are implicated if this popular venue for modern speech begins to disappear as a direct result of uncertain or intolerable legal exposure. [11] Where certain risks cannot be reasonably quantified, responsible business entrepreneurs simply pass on the opportunity to provide the service, or find another jurisdiction in which to operate where the risks are more manageable. Online services can be provided from just about any location that has reliable, established bandwidth resources. Numerous developing countries are increasingly capable of serving the bandwidth needs of OSPs. [12] Accordingly, OSPs are not hesitant to relocate to foreign jurisdictions if the legal risks in the United States become untenable.

A. BuffNET--The First Service Provider Prosecution

In 1998, the New York State Attorney General's Office began what appears to be the first reported criminal investigation of an OSP based on user-generated material. The initial target was an online newsgroup (“Pedo University”), which accessed the Internet utilizing a regional Internet service provider, BuffNET.com, to exchange child pornography among members. [13] Law enforcement, as well as several customers, notified BuffNET about the illegal content sharing, but the Internet service provider apparently took no ***175** action on the matter. [14] After the successful prosecutions of several of Pedo University's

members, law enforcement turned its focus from the users of the group to BuffNET itself, based on its role in making the illegal images available online. [15] Ultimately BuffNET pled guilty to knowingly providing access to child pornography, essentially acknowledging an obligation to eliminate illegal content appearing on its network. [16] Prior to this case, prosecutions of this nature typically only involved the user actually possessing and distributing the illegal materials, as opposed to the OSP that provided the technological means of publication. In effect, BuffNET opened the door to imposing liability on an OSP under the theory that it merely provided the electronic method and/or opportunity for a third-party to commit a criminal act. Law enforcement would call this "facilitating" or "aiding and abetting" illegal activity. Following the BuffNET approach, if an OSP has knowledge of any illegal behavior by its customers but declines to take swift action against the users after notification, the provider could face criminal liability. And although BuffNET remains the earliest example of criminal prosecution against an OSP, its theory of liability--i.e., knowledge coupled with the failure to act after notification--remains the presumptive, customary standard for imposing criminal liability on OSPs even today.

B. The Emergence of User-Generated Content Sites

In recent years, user-generated content sites like YouTube.com, Myspace.com, and Facebook.com have fueled the development of "Web 2.0." These sites have captured the imagination of a new generation of web users and have generated huge profits for their operators. But this new business model highlighted a decade-old problem: Is the operator criminally responsible for illegal material or activity originating from its users?

The legal protections carved out by lawmakers for OSPs thus far have focused on protection from civil monetary liability. They have traditionally been designed to benefit web hosts, Internet service providers (ISPs), and search engines. Much of the existing jurisprudence surrounding OSP liability emanates from cases interpreting 47 U.S.C. § 230, an immunity provision of the Communications Decency Act (CDA) giving legal protection to those entities providing access to third-party generated or "user generated" content. In the statute, an "interactive computer service" (ICS) [17] is defined as "any information service, system, or access software provider [18] that provides or ***176** enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." [19] An ICS is entitled to assert § 230 immunity in response to any claims arising from its involvement with content posted by third parties. Courts have insisted that the scope of those covered by the immunity be "broadly construed" [20] to include a "wide range of cyberspace services." [21] Given its expansive definition, essentially any online intermediary supplying a service to web users may be deemed an ICS. For example, courts have accorded § 230 protection to online dating sites and classified sites advertising escorts, deeming them ICSs. [22] The legal protections carved out by lawmakers for OSPs thus far have focused on protection from civil monetary liability. They have traditionally been designed to benefit web hosts, Internet service providers (ISPs), and search engines. These OSPs have become fairly comfortable in their legal position, given the broad immunity provided by § 230, as discussed infra. But in recent years, the Internet has experienced an influx of a new breed of OSP: social networking sites, allowing subscribers or members to upload content on their own to the OSPs' servers--known as user-generated content (UGC). [23] UGC sites thus provide an online forum, or web space, for third parties to communicate--thereby allowing them to fall into this ICS category--even though their existence may never have been contemplated by Congress when crafting § 230 immunity.

Liability concerns, particularly criminal issues, constantly plague all UGC sites regardless of their subject matter or focus: getting hit with a six-figure civil judgment and filing for bankruptcy is one thing, but going to jail is quite another. Accordingly, UGC sites have tried over the years to get a handle on ***177** where the legal line might be drawn when it comes to being held criminally responsible for a user's conduct or content. Again, the UGC sites that concentrate on more controversial subject matter, like erotic material, pharmaceuticals, or gambling, face the most legal uncertainty. This article focuses on the concerns facing OSPs that operate in the adult entertainment space--or "sex business" for want of a better term. These adult-themed OSPs operate in a legal void of sorts, given the stunted development of the law in this area. Yet given the numerous state and

federal statutes that are uniquely applicable to adult-oriented content producers, publishers, and distributors, these OSPs face the most significant and realistic potential for criminal liability. Each day, thousands of erotic-themed forums, hosts, adult dating sites, adult-oriented "tube" sites, online escort classified sites, and adult-content review sites are essentially forced to operate in fear that a SWAT team might at any moment descend on their corporate headquarters, or that the Department of Justice might seize their assets, including their domain name(s), based on the uncertain legal issues pertaining to criminal liability for content generated by third parties. The author routinely advises these UGC sites in their quest to quantify the legal risks of doing business as an OSP. Unfortunately, as discussed below, the legal issues relating to criminal liability are far from settled, and this increasingly popular new online business model is fraught with legal instability. Despite the existence of this uncertainty for almost two decades, Congress has failed to act, while the problem grows larger by the day.

C. Recent Criminal Actions Against OSPs

With BuffNET occurring over a decade ago, it was easy for OSPs to let caution fall by the wayside. The criminal exposure was lurking, but was not of immediate concern due to lack of enforcement. This inactivity lasted until just a few short years ago when a provider of online classified space, Craigslist.org, found itself targeted by law enforcement on account of its "adult personals" ad category. Ads in this type of category are often placed by escorts advertising companionship services. The ads thus qualify as a form of adult-themed UGC.

Believing that the existence of the adult personals category facilitated acts of prostitution, a team of state Attorneys General sprang into action, with public demands that the entire ad category be removed, under the penalty of criminal prosecution. [24] One Attorney General in particular, South Carolina's Henry McMaster, penned a letter chastising Craigslist for having yet to "install sufficient safeguards" on its site as the company had promised to do approximately six months earlier and threatened to file criminal charges against ***178** the company if all offending material was not removed before May 15, 2009. [25] Within days of McMaster's public reprimand, Craigslist replaced its controversial section with a closely-monitored "adult" section, in the hopes of diffusing the controversy. [26] But that action did not satisfy McMaster, who ultimately demanded that Craigslist "block everything (sexually explicit) in South Carolina." [27] Realizing the futility of further negotiations with McMaster, Craigslist sued in federal court, seeking to stop the attempted censorship of its user-generated advertising. [28] After some skirmishes in court, where Craigslist seemed to be winning, the site pulled an about-face, and completely abandoned its U.S. based erotic services category [29] in apparent response to the intense public pressure and threats of criminal prosecution. [30]

The issues with online escort advertising sites really started to heat up in February 2010, when the U.S. Senate Committee on the Judiciary commenced hearings entitled In Our Own Backyard: Child Prostitution and Sex Trafficking in the United States. In his opening remarks, the Honorable Richard J. Durbin noted: "President Obama has called human trafficking 'a debasement of our own common humanity.'" [31] This political rhetoric fueled the fire started by the gang of state Attorneys General, who, after adding a few more states to their ***179** group, then turned their sights on the next most popular escort ad destination: Backpage.com. Not surprisingly, the law enforcement action against Craigslist had not resulted in the immediate demise of the escort industry--instead the escorts just moved their advertising to Backpage.com. Twenty-one Attorneys General across the country then teamed up and wrote a letter to Backpage, demanding that the site immediately censor its online advertising of "adult services" or face potential criminal charges and other law enforcement action [32] --a dangerous threat, especially during election season. Connecticut's Attorney General, Richard Blumenthal, called the demands for censorship "common-sense steps toward protecting women and children." [33] The fact that the site had been sued by a fifteen-year-old female victim of sex trafficking for allegedly turning a blind eye to illegal activity presumably provided additional ammunition to the law enforcement demands. [34] Backpage initially fought back with the unveiling of its opposition blog, [35] but eventually compromised to a degree, in announcing new 'security measures' associated with future adult personal ads. At the same time,

it sought to diffuse the public attention on its website by calling on its 'industry brethren' to form a "National Task Force" to study ways to prevent misuse of online escort advertising venues for illicit purposes. [36]

Backpage's purported gesture of goodwill--in calling out other escort advertising sites--ultimately resulted in investigation of, and prosecutorial threats pertaining to, the business practices of several of the identified sites by a variety of state and local authorities. For example, law enforcement officials from Montgomery County, Maryland, went so far as to accuse one of the websites 'outed' by Backpage as the "primary internet advertiser of human trafficking." [37]

***180** Within weeks of Backpage's call to action, over one hundred federal law enforcement agents raided the corporate offices of another popular online escort advertising site, Escorts.com, seizing substantial business and personal assets. [38] Although unconfirmed at the time, initial media speculation aptly suggested that the seizure was based upon claims that the site facilitated prostitution in violation of state and federal law. [39] The raid ratcheted up pressure in the industry, as no adult OSP wanted to be the next to be subjected to this sort of intimidating muscle flexing by the Department of Justice or state law enforcement agency. However, OSP's were forced to wait and see, for several months, whether any prostitution charges would be filed against Escorts.com based on the content of their customer's ads. Then, after more than six months of virtual silence on the issue, on June 21, 2011, Escorts.com quietly shut down its website without explanation. [40] Some sort of criminal charges seemed inevitable.

In July 2011, the campaign against Backpage took on new life, as Seattle's Mayor, Mike McGinn, ordered all city departments to halt any advertising business with the Seattle Weekly, a subsidiary of the company that owns Backpage (Village Voice Media). This action was taken in response to a letter sent by the National Organization of Women, a few days before, which demanded that McGinn support a boycott of Village Voice Media. The war against OSPs heated up again in August 2011, when, in a public display reminiscent of that waged against Craigslist, forty-six state Attorneys General sent a letter to Backpage accusing the site of knowingly profiting from advertisements related to illegal prostitution and failing to take the precautions it once promised to implement in order to eliminate alleged unlawful content. [41] The letter, originally drafted by Washington Attorney General Rob McKenna, challenges Backpage to make good on its previous assurances by implementing better advertising safeguards on the site. [42] The letter also contains a myriad of ***181** demands, ominously presented as requests "in lieu of a subpoena." [43] The inquiries, all relating to the site's internal business practices, range from "describing in detail" what the site understands to constitute "illegal activity" to requesting specific advertisement statistics and company policy documents. [44]

On November 1, 2011, the waiting for a resolution in the Escorts.com case came to an end. National A-1 Advertising and R.S. Duffy, Inc., the parent companies of Escorts.com since 2007, consented to a plea deal with the United States Attorney for the Middle District of Pennsylvania whereby the operating companies agreed to forfeit millions of dollars in advertising proceeds, and admit to federal money laundering offenses premised on their online escort advertising activity. [45] Explaining that the charges arose from actions that allegedly "facilitated interstate prostitution activities," the United States Attorney's Office issued a press release confirming that the charges and forfeitures arose from the revenue generated from ads placed by escorts, along with subscription fees paid to view the advertisements. [46] The plea agreement confirmed that the criminal culpability imposed on operators of Escorts.com, arose from the prostitution-related activities of "some" escorts who advertised on the website. [47] The revenue generated by the advertisements and subscription fees constituted the purported proceeds of "violations of federal laws prohibiting interstate travel in aid of racketeering enterprises, specifically prostitution, and aiding and abetting such travel." [48] The companies are serving a probation term of eighteen months, were forced to pay $1.5 million in fines, and are required to forfeit the domain name www.Escorts.com, along with $4.9 million in cash derived from the alleged unlawful activities, to the Department of Justice. [49] Consequently, the pressure from law enforcement not only remains focused on these online media outlets but is undoubtedly increasing. Yet the underlying legal basis for these threats of prosecution is unclear where the allegedly illegal content and conduct originates from third-party subscribers.

The previous examples involving online escort sites are merely a recent sampling of the government's efforts to hold OSPs criminally responsible for ***182** acts of third parties. Countless similar instances occur on a regular basis--many of which never receive any media attention, or are quietly resolved out of the public eye. The potential for criminal liability thus remains hanging like the proverbial Sword of Damocles over the heads of OSPs. As will be addressed in more depth below, the boundaries of civil liability have become clearer, resulting in relatively well-settled law. But the seemingly more pressing issue of criminal exposure has eluded clarification time and time again. Given the complexity of the relevant state and federal criminal laws, coupled with the lack of specific interpretative judicial decisions, OSPs are potentially subject to prosecution for a wide variety of crimes, ranging from obscenity to child exploitation to prostitution--regardless of the fact that the providers, themselves, have no involvement in the creation and/or selection of the content being circulated or the activity occurring on the network. This unsettled state of affairs has resulted in a massive black hole in Internet law that can ultimately only be clarified by federal legislation providing legal protection to OSPs, with respect to criminal liability based on user-generated content.

II. Existing Legislative Protections Against Civil Liability

B. The Digital Millennium Copyright Act--A Safe Harbor

The passage of federal laws like the Digital Millennium Copyright Act (DMCA)[50] and § 230 of the CDA[51] suggest that the need for limitations on OSP liability is not completely lost on the U.S. Congress. Pursuant to one of its "safe harbor" provisions, the DMCA protects certain OSPs from monetary liability for copyright infringement actions arising from content that is transmitted or posted to the OSP's network by the network's users. However, the "safe harbor" from liability provided to service providers under the DMCA is not a blanket grant of protection. The service provider may only qualify for the protection if:

(1) The provider has no actual knowledge of the infringing material or activity on the site;

(2) The provider is not aware of facts or circumstances from which infringing activity is apparent; or

(3) The provider expeditiously removes or disables access to the material upon obtaining knowledge or awareness of the infringing material.[52]

***183** Accordingly, some legal structure exists for determining whether to insulate an OSP from liability, and when such legal protection might be forfeited. The groundwork for similar potential protection from criminal liability has thus been laid by the DMCA.

B. Section 230 Immunity

Given that the DMCA is limited to copyright infringement actions, the most often-cited statute in an OSP's battle against civil liability is § 230 of the CDA.[53] This statute covers a wide variety of potential claims, aside from intellectual property laws and federal criminal offenses. In 1995, prior to the passage of § 230, a New York state court heard one of the first cases tackling the issue of service provider liability for UGC in Stratton Oakmont, Inc. v. Prodigy Services.[54] Applying traditional defamation standards to a web user's postings, the court ultimately found the ISP liable for comments made by its users on a virtual bulletin board.[55] Citing to the fact that the ISP installed software to monitor the board's posts, the court found that the ISP had crossed the line from a simple distributor of the content to a publisher.[56] Notably, the court suggested that the ISP might want to become more passive in its operations in order to avoid future issues pertaining to third-party content.[57] As a result of Stratton Oakmont, despite any good intentions, OSPs that made any efforts to monitor or delete offensive or defamatory third-party content opened themselves up to a higher risk of liability than if they had simply turned a blind eye to the matter. Congress

recognized this decision as a severe disincentive for OSPs to fostering the growth of the Internet, still in its early stages. To avoid any further chilling effects on speech, Congress in 1996 passed the CDA, which contained § 230 immunity.

Evolving from a piece of legislation concerning efforts to protect children ***184** from indecent and obscene material on the Internet, what would become the CDA was originally proposed by Senator James Exon of Nebraska.[58] About the same time, a piece of sister legislation was proposed in the House: the Cox/Wyden Amendment.[59] The Cox/Wyden Amendment, while acknowledging the need for some regulation of the Internet, mainly sought to find a middle ground between battling unlawful content and still nurturing the Internet as a medium for disseminating speech.[60] Despite calls for caution[61] in giving the government too much regulatory control over the web, the Cox/Wyden Amendment passed and was incorporated into the first version of the CDA. However, Congress's attempt to control "indecent" communications in this fledgling medium was short-lived, as the ACLU immediately challenged the indecency provisions of the CDA on First Amendment grounds, which were enjoined before they ever took effect.[62] In striking down the indecency provisions as unconstitutional, the Supreme Court stated that the language of the CDA, as written, violated the First Amendment by incorporating a content-based restriction on legal speech.[63] However, the provisions affording immunity to ISC's for third-party material, what is known as § 230, remained intact. Section 230 affords broad immunity from liability, in certain circumstances, for OSPs that allow content provided by users to be posted on their network, as an OSP can be considered the provider of an "interactive computer service" for the purposes of the immunity granted in the statute.[64] In analyzing the potential application of § 230, all three of the following prongs must be met for immunity to apply: (1) The defendant claiming the immunity is a "provider or user of an interactive computer service;"[65] (2) The allegedly unlawful content was "provided by another information content provider;"[66] and; (3) The plaintiff's/prosecution's claims seek to "treat" the defendant as the "publisher or speaker" of the information provided by another.[67]

***185** This immunity is based on the premise that the OSP is not actually publishing material, as the term is used in mainstream media, but simply providing the forum in which the material may be published. Granted, the networks obviously play a critical role in relation to certain content by supplying such a forum, but generally do not actually cause the content to be created. It is well-settled law that § 230 provides absolute immunity on tort claims of defamation, public nuisance, and even gross negligence.[68] It is the prospect of extending that broad civil immunity to the criminal context, however, that tends to generate controversy, or at the very least uncertainty, throughout the online world. Given the dearth of case law on criminal liability for OSPs, they are essentially forced to employ the principles developed in civil case law interpreting DMCA Safe Harbor and § 230 immunity as their only guidance in determining potential exposure to criminal sanctions.

C. The Beginnings of Criminal Immunity for OSPs

As noted above, § 230's applicability and interpretation in the civil context remain well-settled. One of the seminal cases in this field is Chicago Lawyers' Commission v. Craigslist.[69] Acknowledging that § 230 did not grant a complete blanket of immunity over all civil liability claims, the Chicago Lawyers' court nevertheless upheld immunity for Craigslist against federal Fair Housing Act claims based on discriminatory statements by third parties in the site's classified ads.[70]

Shortly after the Chicago Lawyers' decision, the Ninth Circuit issued arguably conflicting precedent via the infamous Roommates.com case.[71] Roommates brought to light the fine line between acting as the provider of an interactive computer service and becoming an information content provider. The court found that the level of interaction by Roommates.com crossed the line as the site "materially contributed" to content by requiring information from users that could be used for discriminatory purposes.[72] As a result of ***186** Roommates and other cases like it,[73] if OSPs provide anything beyond a basic user interface to the public, they could open themselves up to potential liability. This interpretation could be instructive in the criminal context as well. To the extent that the OSP did not "materially contribute" to the content or conduct alleged to be illegal, it

could logically enjoy the same level of immunity regardless of whether the theory of liability was based on civil or criminal theories. The first discussion of the potential extension of § 230 immunity to the criminal context arose in 2006. Importantly, § 230(e)(3) states that no cause of action or liability may be imposed under any state or local law that is inconsistent with § 230. [74] Notably, no distinction is made as to whether the inconsistent "state or local law" must be civil or criminal in nature. As referenced above, courts have had no qualms with applying this exception to civil claims, but did not address § 230(e)(3)'s application to criminal liability until 2006 with Voicenet Communications v. Corbett. [75] In Voicenet, law enforcement raided the offices of an OSP, executing a search warrant based on alleged violations of child pornography laws. [76] Voicenet claimed that in doing so, the government violated its civil liberties, as law enforcement's only allegation connecting liability was that Voicenet hosted the venue where the unlawful images were published. [77] Suing law enforcement for First and Fourth Amendment violations, Voicenet argued that § 230 preempted any legal liability. [78] Although the lawsuit itself was ultimately unsuccessful, the Voicenet decision began to fill the gap in § 230 jurisprudence that had been a basis for speculation and forced inferences since the statute's inception: did the statute ***187** preempt inconsistent state criminal laws, as well as inconsistent state civil laws? The court compared the use of the word "federal" in § 230(e)(1) with the lack of that term and use of the term "any" in §§ 230(e)(2)-(3) to determine that § 230 undeniably preempts criminal liability under inconsistent state laws. [79]

Just a few short years after the Voicenet decision, a Michigan appeals court explored the application of § 230 to state criminal laws as well. People v. Gourlay was resolved on the premise that an OSP's actions can, in fact, cross a line--thereby placing the service provider outside of the scope of § 230's immunity--even if the defense was extended to the criminal realm. [80] In that case, Justin Berry, a minor, used the Internet to publish pornographic images of himself via a self-created website. [81] Kenneth Gourlay operated the web hosting company that hosted Berry's website. [82] The facts show that Berry and Gourlay communicated several times regarding Berry's website, and its content, and ultimately worked together to create two other websites featuring similar materials. [83] Gourlay was convicted of several counts of violating three state child pornography laws. [84] Attempting to utilize the § 230 shield, Gourlay appealed the convictions on the basis that the trial court jury should have been instructed that he "could not be convicted of the pornography offenses unless it found that he actually contributed to the creation of child pornography," that he could not have done so in his capacity as a service provider and therefore could not be treated as a publisher of the content. [85]

Finding that "because Congress specifically intended that no liability may be imposed under a state criminal law that is inconsistent with Section 230," the court rejected the State's argument that § 230 was irrelevant to the criminal charges. [86] However, distinguishing Gourlay's actions from that of a typical OSP acting as a web host, the court clarified its position on § 230's application, and went on to affirm Gourlay's guilt. [87] The court's decision hinged upon the ***188** fact that the actions of a typical web host would not have fulfilled the intent requirement necessary for a conviction under the child pornography statutes at hand; consequently, Gourlay was a knowing and active participant in creating the sites and their respective content. [88] Gourlay's actions crossed the line into acting as an information content provider (as opposed to an ICS); therefore, his convictions were consistent with § 230, which excludes liability only when acting as a passive host. These distinctions could also ultimately be helpful as building blocks in any new legislation outlining immunity or safe harbor afforded to OSP's, in the criminal realm.

The immunity provided to OSPs by § 230 also excludes violations of federal criminal law. [89] Thus, irrespective of any immunity that § 230 might provide with regard to state criminal laws, the potential application of federal criminal laws to OSPs remains a substantial concern. The federal criminal law exclusion is arguably the most definitive of the four exceptions, although it has not been expounded upon in the same depth as the state law exception referenced above. The language in § 230(e)(1) reaffirms that

OSPs are still subject to prosecution under federal criminal statutes, specifically including obscenity and child pornography. [90] Therefore, there is no question as to an OSP's potential liability in this regard under existing law.

As noted above, the case law on criminal liability under state statutes, while minimal, offers some encouraging dicta for OSPs seeking legal protection relating to user-generated content. Over the last decade, additional cases have built on the potential scope of § 230 protection and its possible applicability to state-level criminal prosecution. For example, in Doe v. America Online, a complaint was filed against AOL by a woman seeking to recover for emotional injuries suffered by her son resulting from sexual exploitation. [91] The defendant claimed that her son was lured into engaging in sexual activity with an adult and images of such activity were subsequently marketed via AOL's chat rooms. [92] The court upheld AOL's immunity against the claims of negligence based on "chat room marketing" of the pornographic ***189** images of the minor. [93] Stating that AOL, as an intermediary, was immune from liability under criminal statutes prohibiting marketing and dissemination of child pornography, the Florida Supreme Court effectively extended § 230 immunity to civil claims arising from criminal activities. [94]

Later, in 2009, an Illinois court touched on the possibility of extending § 230 to criminal actions in Dart v. Craigslist. [95] The primary argument advanced in that case was that Craigslist facilitated prostitution through its adult services advertisements, and thus constituted a public nuisance. [96] Sheriff Thomas Dart, claiming that Craigslist violated Illinois statute since it arranged "meetings of persons for purposes of prostitution and direct[ed] them to a place for the purpose of prostitution," ultimately sought to enjoin the service provider from continuing to offer its adult personals section. [97] In ruling on the request for the injunction the court stated that even if Craigslist had violated Illinois law, § 230(e) would control. [98] Sheriff Dart further alleged that Craigslist had violated the federal statute, 18 U.S.C. § 1952, which prohibits the facilitation of prostitution. [99] The court deftly avoided confronting the federal law issue [100] in a footnote where it stated that merely referencing a federal statute does not bring the public-nuisance suit within the federal criminal law exception to § 230. [101]

In coming to its decision, the court cited to an unreported Texas district court case involving private litigants bringing civil claims against OSPs predicated upon federal criminal statutes for the purposes of circumventing § 230 immunity. [102] In Doe v. Bates, Yahoo! hosted a website that was used to distribute child pornography. [103] Attempting to avoid an immunity defense, the Plaintiff argued that § 230 did not apply to the situation because the suit sought enforcement of federal child pornography statutes. [104] Acknowledging the novelty of the argument, the court nonetheless rejected the assertion that a civil claim based on an alleged violation of a federal criminal law should be recognized as falling within the exception to immunity set forth in ***190** § 230(e)(1). [105] The court also went a step further in recognizing that Congress's legislative intent was "not to allow private party litigants to bring civil claims based on their own beliefs that a service provider's actions violated the criminal laws." [106]

Based on the evolving interpretation of § 230 described above, it would appear consistent with legislative objectives and judicial policy to immunize an OSP from criminal legal exposure, so long as the provider did not take an active role in assisting the user and did not refuse to act after having been notified that its services were being used for criminal purposes. In this respect, three factors should be considered: lack of duty, lack of knowledge, and lack of intent. With regard to "duty," Congress's legislative intent is crystal clear on the issue, and courts have confirmed that OSPs have no duty to monitor third-party content published on their networks. [107] Imposing such a duty would bring Internet traffic to a screeching halt, given the sheer manpower necessary to review the millions of files uploaded to some networks on a regular basis. If a duty does exist, in the criminal context, such obligation would overshadow the absence of duty in the civil context, so as to render all of the Congressional findings and judicial interpretations on this issue meaningless. In other words, if an OSP had a duty to monitor communications to ensure compliance with criminal laws, it would likely institute such monitoring as a routine policy, irrespective of whether civil statutes recognized that this duty was not required. If the obligation to scrutinize UGC was removed in both the civil and criminal

contexts, and the OSP truly has no knowledge of specific illegal content displayed on or distributed through its network, no valid basis for criminal liability exists. As discussed infra, this lack of knowledge prevents the OSP from forming the requisite criminal intent, or scienter. The intent to violate the law is essential to the imposition of criminal liability in most instances. [108]

D. Theories of Criminal Liability for OSPs

Potential criminal liability for OSP is a controversial issue, but one that ***191** must be clarified if the Internet is to continue to function, free of government-encouraged self-censorship. The unsettled nature of this issue often causes OSPs to take the "safe route" by censoring broad categories of content or activity--in the hopes of avoiding a very public criminal indictment. Adult service providers have the unique struggle of balancing a very typical general business model with very atypical content--by their very nature, adult providers are simply more susceptible to criminal action. Various sources of potential criminal liability exist--particularly for those OSPs operating in the adult entertainment space.

1. Accomplice Liability

The most troubling concept for OSPs, from a criminal law perspective, is the theory of accomplice liability. According to the Model Penal Code, accomplice liability exists if a defendant assists another "with the purpose of promoting or facilitating the commission" of a particular offense. [109] This assistance is typically established via the criminal acts of aiding and abetting and/or conspiracy. These accomplice liability theories can be utilized to impose full punishment on those involved on the periphery of any substantive criminal offense.

Federal law describes aiding and abetting as when an individual "willfully causes an act to be done which if directly performed by him or another would be an offense against the U.S. is punishable as a principal." [110] Thus, the crime of "aiding and abetting" occurs when an actor willfully associates with and actively participates in the commission of a crime. [111] Conversely, a criminal conspiracy is distinguished from aiding and abetting as it requires knowledge of, and voluntary participation in, an agreement to commit a criminal act. [112]

The key building block in accomplice liability theory is the element of knowledge. [113] The prosecution must show more than mere association with the ***192** party actually committing the crime, even though the level of participation of the aider and abettor or conspirator may be relatively minor. [114] Given the broad scope of federal accomplice liability statutes and the uncertain obligations imposed on OSPs in the criminal context, potential liability exists for a wide variety of offenses, based solely on the presence of allegedly illegal UGC on the OSP's network. The lack of any recognized immunity afforded to OSPs for federal criminal violations relating to UGC results in immeasurable potential legal exposure based on a wholly tangential relationship with the illegal conduct or material. This exposure is particularly substantial with respect to OSPs involved with adult-oriented material or services.

2. Travel Act Violations

A federal statute that presents potential problems for OSPs like escort advertising site operators is 18 U.S.C. § 1952, also known as the Travel Act. This statute was enacted to enable easier prosecution of organized crime syndicates crossing state lines in the execution of unlawful business practices. [115] The elements necessary for a Travel Act violation [116] are as follows:

1. The use of a facility of foreign or interstate commerce (e.g., the Internet, telephone, etc.);

2. with the intent to promote or facilitate;

3. an unlawful activity (e.g., prostitution). [117]

***193** As it is used to essentially federalize state crimes, the Travel Act "refers to state law only to identify the defendant's unlawful activity, the federal crime to be proved in Section 1952 is use of the interstate facilities in furtherance of the unlawful activity, not the violation of the state law; therefore Section 1952 does not require that the state crime ever be completed." [118] As noted above, in regards to criminal liability for OSPs, Travel Act concerns may be triggered in a scenario where the OSP allows third parties to post advertisements for escorts or adult companions. For example, it might be argued by law enforcement that an OSP is utilizing the Internet, a facility of interstate commerce, to promote or facilitate the crime of prostitution, an "unlawful activity." Because the commission of the state law violation used to support the Travel Act charge need not actually be completed, [119] proof of actual prostitution resulting from a provider's network is unnecessary. Travel Act cases involving prostitution as the underlying substantive offense have traditionally dealt with brick-and-mortar establishments and more obvious chains of liability: for example, brothels or massage parlors. [120] In a situation involving an online intermediary, the Internet creates a unique situation in that the dissemination of the criminal information (i.e., the escort's advertisement), or the promotion of the unlawful activity (i.e., the escort's services) occurs in the virtual world, but the crime itself, if it occurs at all, takes place locally-- typically without the knowledge or involvement of the OSP.

In the typical case with an online escort site, the OSP has no involvement with the escorts other than providing advertising space at an agreed-upon price pursuant to a commercial advertising agreement. While most online escort directories impose certain "publishing standards" prohibiting any advertisements that offer or imply sex for money (in jurisdictions where such activity is illegal), [121] the OSP does not typically design the ad, or create the ad text. Even though it is well-settled that the Travel Act is not intended to punish local crimes, a service provider's conduct in operating a website containing escort advertisements may be considered promotion of an "unlawful act," under the Travel Act, and, further, the promotion would involve a "facility of interstate commerce," under the Act. Despite the service provider's website being international (or not local) in nature, escort advertisements are, with some exception (i.e., escorts advertising their "travel/visiting" schedule in a particular location), inherently local. However, this potential "fit" under a plain text reading of the Travel Act does not necessarily mean that § 1952 should ***194** apply to an OSP based on an escort's allegedly criminal conduct. [122] The OSP's activity as a venue for communication does not appear to fall within the intended scope of the Travel Act. Referring back to the brick-and-mortar analogy, Travel Act violations are typically committed by parties directly involved in the alleged criminal act, for example, "pimps" and "madams." [123] Such criminal liability has never been extended to mere advertisers of individuals who later engage in prostitution. Given that the OSP is a mere advertising forum for such individuals that may later engage in unlawful conduct, one of the primary defenses that any advertising outlet, such as an online classified site, could assert would be commercial speech protection under the First Amendment. [124]

Basic free speech principles would appear to automatically prevent the imposition of criminal liability on escort classified sites based solely on their customers' content--particularly if the ads themselves did not explicitly offer, or imply, sexual activity for hire. Most online escort websites impose limitations on statements that could impose such liability. [125] This is particularly true where the website imposes strict publishing guidelines that prohibit any such reference. [126] Escort activity is considered legal and specifically licensed in many counties and cities. [127] Given the site's limited involvement in the development of the escort's advertising content, and the presumptively legal activity being advertised, the OSPs position as a mere forum of the speech would appear to insulate the OSP from criminal liability. However, as described above, the broad scope of accomplice liability, coupled with the lack of any recognized legal protection for OSPs who merely provide the venue for third-party communication, has allowed law enforcement officials to bully their way into obtaining results that they may never achieve if they were forced to actually pursue criminal charges, such as the raid on the ***195** operators, to conclusion. However in the cases of both Escorts.com and Craigslist.com, the prosecuting authorities were successful in shutting down the disfavored advertisements and thus silencing a form of speech.

E. Child Pornography

OSPs often fear that their services could be used to transmit or provide access to child pornography. As seen in Doe v. America Online, the services offered by OSPs have the capability of being misused for the circulation of child pornography. [128] There are several federal criminal laws that are labeled child sexual exploitation offenses, all of which create additional potential criminal liability for an adult OSP. [129] Such crimes carry severe sanctions ranging from costly fines to double-digit prison sentences. [130] For example, to constitute guilt under 18 U.S.C. § 2252A, the statute criminalizing certain activities relating to child pornography, the government must prove the following:

(1) The defendant knowingly received or possessed an item or items of child pornography, as charged;

(2) Such items of child pornography had been transported, shipped or mailed in interstate or foreign commerce, including by computer; and

(3) At the time of such reception or possession of the materials, the defendant believed that such items constituted or contained child pornography. [131]

Theoretically, these elements could be met through an OSP's participation in the process of allowing third parties to utilize their services to make child pornographic images available to others on the Internet. Despite the gravity of ***196** their respective penalties, the sexual exploitation laws do not specifically require proof that the defendant had knowledge of the minor's age, only knowledge of receipt or distribution of the images; [132] essentially making each child pornography violation potentially a strict liability offense. [133] Accordingly, whether or not a service provider had the intent to circulate pornographic images of minors is not identified in the federal statute as a defense to the alleged exploitation resulting from the OSP's role in transmitting the material in question.

However, the Supreme Court's decision in United States v. X-Citement Video [134] suggests that parties who are charged with child pornography offenses, but not directly involved in the production of the offending content, must be able to assert a defense to such charges if they were not aware that the person(s) depicted in the material was underage. The defendant in X-Citement Video, a video store owner, was charged with violating § 2252 of the U.S. Code, prohibiting "certain activities relating to material involving the sexual exploitation of minors." [135]

The charges arose from the defendant selling and shipping pornographic videos containing an underage adult film star, although he maintained that he had no scienter, or knowledge, of the materials containing underage pornographic acts. [136] Although no criminal intent element was present in the statute, the Court construed the crime at issue to contain an element not expressly included in its statutory text and determined that the knowledge requirement in § 2252 "extends both to the sexually explicit nature of the material and to the age of the performers." [137] The Court performed these statutory gymnastics in order to save the federal child pornography law from being struck down on First Amendment grounds, meaning that a defendant-- not involved with the original production of the underlying material--who is charged with receipt of child pornography must have knowledge, not only as to the act of receipt itself, but also as to the fact that the material being received contains minors engaged in sexually explicit conduct. Again, this distinction only holds true for a defendant who is not involved in creation of the unlawful material--in other words, distributors such as OSPs. [138]

***197** In effect, the Supreme Court's decision instructs that knowledge as to a subject's age is required for most child pornography offenses, even if such a requirement is not necessarily part of the text of the relevant law, so long as the charged party is removed from the actual creation of the content. This premise is directly applicable to any involvement that an OSP

would presumably have with the transmission or receipt of underage images. [139] The scienter component is required by the First Amendment since the child sexual exploitation statutes differentiate constitutionally protected images from criminal contraband. [140] Accordingly, only those who know they are dealing in underage imagery, or those who have the opportunity to prevent its initial creation, should be held criminally liable. Therefore, the knowledge element makes all the difference for secondary producers (e.g., webmasters and distributors, including OSPs) as opposed to primary producers. [141] As noted by numerous courts in the civil context, OSPs are not Internet content providers but are, at most, distributors [142] who create a platform for communication by others. Given this status, it is clear that an OSP should be protected from criminal liability for any role they play in unknowingly allowing their users to distribute child pornographic images by its users, under this theory. X-Citement Video thus provides another piece of the puzzle for evaluating the rational level of criminal exposure that should be imposed on OSPs. Lack of knowledge of the nature of the illegal material is key to determining potential liability.

Notably, Congress has created one narrow safe harbor for OSPs in connection with child exploitation offenses, which recognizes the plight of OSPs, at least to an extent. 18 U.S.C. § 2258A allows OSPs to enjoy limited immunity from criminal liability under certain circumstances; [143] i.e., when ***198** executing good faith policing efforts to report child exploitation offenses to federal authorities. [144] Any OSP, defined by the relevant statute as an "electronic communication service" or a "remote computing service," has a duty under federal law to report evidence of apparent child exploitative activities of which it becomes aware. [145] The OSP submits the reports to the Cyber Tip Hotline established by the National Center for Missing and Exploited Children (NCMEC). [146] Actual knowledge may include the OSP's actual discovery of the images or other content that appears to violate the child exploitation statutes, but it may also include any reports of apparent violations sent directly to the OSP by customers or any other third parties.

While beneficial to all OSPs, this process is especially valuable to intermediaries involved with providing access to UGC, not only because of the potential immunity benefits, but also because the reporting requirements are quite realistic in their expectations of participants. The statute recognizes the need for customer privacy and cost-effective policing efforts by including a provision stating that OSPs are not required to monitor any of their users, subscribers, customers, or any of the contents of communications between such users. [147] This is critically important, because any immunity that is provided to OSPs must be practical in any monitoring obligations, given the impossible task that active monitoring would represent for most OSPs. Participation in the § 2258A reporting system clearly reaps certain advantages, but it is also a very serious undertaking, as liability still remains if a provider fails to report any illegal depictions of child exploitation of which it has become aware. [148]

***199 F. Section 2257 Violations**

Criminal laws directed at the adult industry are often intended to apply to those directly involved with the production, publication and sale of adult materials. Criminal accomplice laws are directed at criminal gangs, syndicates and mobs. However, when accomplice theories are combined with broad laws seeking to regulate the adult industry, unintended consequences can be suffered by OSPs. One of the substantive laws regulating the adult industry is 18 U.S.C. § 2257.

As a knee-jerk reaction to the Traci Lords scandal, wherein Ms. Lords successfully broke into the adult entertainment industry at the tender age of 15 using a fake ID, Congress passed a statute imposing a byzantine and burdensome set of record-keeping and labeling obligations on the producers of adult-oriented content. [149] As a result, the adult entertainment industry is now forced to adhere to content compliance directives known as "§ 2257." Under the penalty of felony criminal prosecution and imposition of a multi-year criminal sentence, § 2257 imposes obligations on the producers and distributors of actual and simulated sexually explicit material to maintain specified age records and post a "compliance statement" identifying the location where the required age records will be made available for inspection to the Attorney General (or his designee). [150] Such obligations include not only maintaining copies of government-issued picture ID cards for each performer, [151] but also include more obscure

requirements like cross-referencing each performer's records with any and all aliases or stage names that the performer has ever used, and compiling an accurate, real-time list of any URLs where each performer's content appears on the Internet. [152] An OSP's obligations in connection with § 2257 are uncertain, at best. Those subject to the record-keeping obligations include:

> [Any individual or company] who inserts on a computer site or service a digital image of, or otherwise manages the sexually explicit content of a computer site or service that contains a visual depiction of, an actual human being engaged in actual or simulated sexually explicit conduct, including any person who enters into a contract, agreement, or conspiracy to do any of the ***200** foregoing. [153]

Arguments can theoretically be made that operators of some OSP business models "manage" the material or "insert" "digital images" of 2257-triggering content. However, even if the OSP does not engage in this content directly, the government could argue that it is responsible for aiding and abetting a § 2257 violation under accomplice liability. Federal law provides relatively little guidance in terms of specifying exactly what type of or how much assistance is necessary to aid or abet this unique type of criminal records-keeping violation. Consequently, it could be argued that almost any willful assistance in facilitating violations of the required record-maintenance obligations constitutes a federal criminal offense. [154]

Section 2257 and the regulations promulgated within do contain exemptions for those OSPs that are involved solely with "transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication, without selection or alteration of the content of the communication . . . ." [155] The scope of these exemptions has not been interpreted by the courts as of yet, and therefore OSPs are left to guess as to whether any given business model is actually protected by the exemptions. [156] To the extent that an OSP guesses wrong in this regard, the penalties that could be suffered include five years in federal prison for a first offense, and ten years for any subsequent offense. [157] Therefore, § 2257 provides another potential basis for imposition of criminal liability on OSPs involved with adult oriented material, particularly when the concept of accomplice liability is thrown into the mix. Might an OSP substantially assist a user in violating § 2257 by ***201** providing a publication venue for non-compliant content? This and other thorny § 2257 issues are the subject of much debate and fret in the adult-oriented OSP community.

Should an OSP decide to try to comply with the obligations of § 2257, the OSP may quickly learn that any such attempt may be futile. Operators of adult dating sites, for example, are unlikely to be able to obtain government-issued age documents from their members before posting profile pictures. Most users of these sites prefer to remain anonymous--particularly if they are uploading sexually explicit images of themselves in the hopes of attracting potential romantic partners. Users uploading sexually explicit videos to tube sites or forums have similar anonymity concerns, and the First Amendment right to anonymous speech is implicated by any requirement that OSPs obtain formal age documentation from their users desiring to engage in this form of erotic communication with each other. [158]

The accomplice liability theories described above complicate matters even further for OSPs trying to sort out their potential criminal exposure under federal law. Forming an agreement (through typical online user terms) with website members who upload sexually explicit material, or providing the means and technological platform for the users to commit § 2257 violations of their own, dramatically increases the potential criminal liability of OSPs under § 2257, under aiding and abetting theories. [159] Thus, even passive activity by the OSP in allowing users to upload erotic material, without the proper age records, or without the proper compliance statement, could result in substantial criminal concerns for the OSP.

In addition to the more commonly discussed record-keeping requirements for producers set forth in § 2257, the statute also addresses "labeling" obligations imposed upon non-producer, "distributors" of the adult content. [160] Under 18 U.S.C. § 2257(f)(4), parties must not "knowingly sell or otherwise transfer" sexually explicit materials that do not contain the proper label identifying the location of the records associated with the content. [161] Thus, even if the OSP is not considered a "producer"

that is required to maintain age records relating to each of the individuals depicted on the website in a sexual ***202** manner, it may well be considered a "distributor" of the material. Yet ensuring that all UGC is associated with an appropriate record's custodian label is a virtually impossible task for most OSPs, given the usual "hands-off" approach to the content of the material. In other words, any obligation that forces an OSP to ensure that UGC contains certain disclosures (or any other element) is wildly inconsistent with the industry standard of merely providing an un-moderated venue for third-party communications. Yet, given the existence of § 2257, along with the broad potential for accomplice liability, OSPs face significant potential legal exposure for records maintenance oversights by their subscribers.

G. Obscenity

Many prosecutors know that nothing strikes fear in the hearts of participants in the adult entertainment field like the word "obscenity." This crime, which is recognized at the federal level and in most states, [162] has been used to keep the adult entertainment industry in check ever since the concept was approved by the U.S. Supreme Court in the seminal case of Miller v. California. [163] Even in recent times, the Department of Justice has prosecuted adult content producers, with varying degrees of success. [164] However, it is not just content producers who are subject to obscenity prohibitions; any person or company that knowingly distributes, transmits, or receives obscene material is subject to prosecution. [165] Such distribution, transmission or receipt can occur physically, such as the sale of a DVD, or it can occur digitally, using an "interactive computer service." [166] A zealous prosecutor, looking for headlines or a career boost, could--consistent with the broad facial scope of federal ***203** obscenity statutes--readily initiate obscenity charges against an OSP, even if the allegedly obscene material was user generated. Moreover, the OSP could be prosecuted in a remote location where the offending material was uploaded or "received." [167]

In fact, this is more than a theoretical possibility--one OSP was already prosecuted by state authorities in Florida for obscenity violations, based purely on UGC. [168] The author had the privilege of defending the OSP in that case, in which the defendant was charged with over 300 counts of obscenity, based on material posted by its users. The case was ultimately resolved by a favorable plea deal after an appellate court issued an emergency Writ of Habeas Corpus ordering the release of the website operator, who was being held in jail in violation of the First Amendment for continued operation of the site after posting bail. [169] While all the felony charges were ultimately dismissed against the OSP after a hard-fought legal battle, the prosecution stands as a stark example of the criminal exposure facing all OSPs, since they often have no control of the nature of the materials posted to their network. The defendant in the Florida case had no specific knowledge of the hundreds of thousands of images posted on the site at any given time. The obscenity charges stemmed from certain adult-oriented material uploaded by users to his site, from many locations across the globe. The prosecutors found some of these more sexually explicit materials uploaded to the site to be "obscene" based on the local community standards of Polk County, Florida. Any OSP that permits erotic materials on its network could find itself facing a similar prosecution, should a prosecutor in some conservative jurisdiction find certain material distasteful or offensive.

Unfortunately for OSPs, there is no litmus test for obscenity. An expressive work can only be declared obscene by a judge or a jury applying the three-part test set forth in Miller v. California. [170] Therefore, even if an OSP were to independently review each file before it was uploaded to the Internet by a third- ***204** party user, the OSP would have no way of knowing, in advance, what material might be found to be obscene by some jury, in some remote community where the material could be "received." Federal law relating to venue for prosecution of obscenity cases is very favorable to the government, essentially allowing it to pick its jurisdiction, and download the material to a computer located therein. [171]

While OSPs are no longer legally responsible for transmission of "indecent" material through their networks, [172] state and federal obscenity laws still provide an intimidating weapon for prosecutors to wield against any OSP that allows adult-themed material to be uploaded to its servers. This includes a wide variety of OSPs including adult dating sites, adult tube sites,

adult-friendly hosts, [173] and adult-themed forums. Moreover, unlike many other crimes, the government is not required, in an obscenity case, to prove that the defendant knew the material being transmitted or received was "obscene." The government need only show that the defendant was aware of the nature and character of the materials; i.e., that they involved sexually-explicit subject matter. [174] As a result, any OSP that permits users to upload sexually-explicit material is at risk of criminal prosecution for obscenity violations, particularly in light of the broad accomplice liability concepts of criminal jurisprudence. Moreover, as discussed below, obscenity violations can serve as a "racketeering activity" under federal RICO statutes, thus significantly raising the stakes for OSPs, given the lack of any recognized immunity or safe harbor defenses. [175]

H. Racketeering

The Racketeer Influenced and Corrupt Organizations Act, [176] better known as RICO, illustrates another opportunity for law enforcement to impose severe criminal sanctions against an OSP, [177] based on little more than a showing that ***205** two or more underlying offenses occurred in a ten-year period. [178] State and federal RICO laws were initially passed in the attempt to pursue organized crime syndicates. [179] However, over time, the statute became increasingly popular as a tool to pursue "garden variety" business fraud and vice activity. [180] A RICO violation involves the following five elements [181]: (1) Conduct or participation in (2) the affairs of an enterprise [182] (3) through a pattern [183] (4) of racketeering activity [184] (5) affecting interstate or foreign commerce.

Operation of an escort site advertising prostitution-related activities, or a "tube" site containing "hard-core" pornography, [185] could easily subject the OSP to RICO charges, if the government can prove that the OSP was legally responsible for two or more types of racketeering activity relating to prostitution or obscenity. The remaining elements such as the existence of an "enterprise," the "pattern" of racketeering activity, and the effect on interstate commerce, rarely present significant hurdles for the prosecution, when dealing with a website operator. Virtually all websites affect interstate commerce, by virtue of their presence on the World Wide Web. A service provider's online business structure--whether a partnership, corporation, or unincorporated association of individuals--is generally sufficient to meet the "enterprise" requirement. Commonly, these sites will generate revenue by offering memberships or advertising space to third-party customers, thus satisfying the remaining elements of the RICO charge. The only real dispute in these cases relates to whether the OSP should even be criminally responsible for the underlying act alleged to be the "racketeering activity." If the answer is yes, RICO liability can become a foregone conclusion for many OSPs.

For example, the posting or distribution by an intermediary's customer of obscene material at least twice, in ten years, although falling within the realm ***206** of user-generated content, may (depending on proof of criminal intent) suffice to establish a prima facie case of "transmitting obscene matter" or aiding and abetting the transmitting or receiving of obscene material. [186] With the remaining elements of the RICO charge reduced to mere technicalities, an OSP could face devastating criminal sanctions under federal RICO law, for merely providing a venue allowing others to communicate on the Internet. The author has been involved in several criminal cases where RICO charges were threatened against OSPs as leverage to support plea deals involving lesser charges. When faced with the prospect of a RICO indictment, most OSPs will give in to the demands of the government, no matter how unreasonable. While RICO itself does not require an element of intent, the underlying crimes constituting the "racketeering activity" often do. Meaning, in prosecuting an OSP for "transmitting obscene matter," the government must prove that the OSP intended to commit the predicate obscenity offense, but not that it intended to violate RICO. As noted above, given the generous standard afforded to the government for proving intent to transmit obscenity (or to aid in the commission of such offense), pursuit of obscenity charges against adult-oriented OSPs by the Department of Justice (or state authorities) would be tantamount to shooting fish in a barrel, assuming that the OSP knew that users were routinely posting sexually-explicit material. Notably, a RICO conviction enables the federal government to hit the defendant where it hurts, as the penalties include loss of liberty--potentially for decades--along with huge fines and seizure of all business assets. [187]

Given the traditionally collusive characteristics of RICO-triggering activities, [188] it is no surprise that the statute contains a provision warranting additional criminal liability for a defendant found to have "conspired" to violate any of the law's proscribed actions. [189] Therefore, an OSP could theoretically be convicted both of substantive RICO offenses, for its role in "knowingly" allowing its network to be used to transmit allegedly obscene material, and of conspiracy to commit RICO, for its role in forming an agreement with the third-party user to commit this offense-- otherwise known as the website's electronic user agreement. [190] Because it constitutes a separate ***207** violation of the statute, the conspiracy charge essentially provides prosecutors with two bites at the RICO apple. While it contains the same foundational aspects as the general federal conspiracy statute, a RICO conspiracy violation does not require proof of an overt act committed for the purpose of affecting the object of the conspiracy. [191] Practically speaking, a RICO conspiracy claim permits a defendant to face imprisonment over the single element of entering into an agreement that results in criminal activity by a third-party. [192]

The following is a typical scenario that may lead to significant RICO liability for an OSP: an adult-themed dating site enters into a legitimate business agreement with a customer, to permit the use of the OSP's services. This agreement allows the user to access the OSP's network to upload a profile describing the user to potential social acquaintances on the site--either for networking or for romantic affairs. The profile may include pictures, video or other media depicting the user. Considering the services in question involve the Internet, any subsequent activities occurring via such services "affect" interstate commerce and the operator constitutes an "enterprise." Should that user employ the provider's adult dating site to upload sexually-explicit depictions of himself or herself that a prosecutor believes to be obscene, such actions potentially expose the OSP to criminal liability under the federal obscenity statutes. [193] If the customer posts such images on two or more occasions, and some revenue is generated from the overall activity, the service provider may find itself facing a federal RICO charge for transmitting obscene material. Furthermore, the OSP might also be guilty of conspiring to transmit obscene material based on its standard user agreement, merely by permitting the customer's use of its dating site's network. While many prosecutors would view a case of this sort to be a stretch, given the absence of any legal protection afforded to OSPs by Congress, and the lack of clear case law on the issue, the OSP is left with no choice but to factor this potential liability into its risk analysis when deciding whether to do business. [194] The dangerous result that can be produced by this lingering liability is substantial "self-censorship" whereby the OSP restricts the content of the material that can be uploaded to the point that no erotic materials are permitted, or the OSP avoids the risks entirely by simply not providing the forum for communication. Sheriff Grady Judd, from Polk County, Florida, effectively used the threat of RICO prosecutions to scare away all adult-themed entertainment from his jurisdiction ***208** over the past two decades. [195] The end result is reduced access to protected speech and online communication, as a result of the "chilling effect" created by the potential for criminal prosecution. [196]

III. The Future of Criminal Liability for Online Service Providers

Most OSPs have come to grips with the reality that no formal legal immunity or safe harbor exists (outside of possible § 230 arguments) to protect them from the imposition of criminal liability. Accordingly, the result has been a concerted effort in the OSP industry to self-regulate--even to the point of self-censorship in certain cases. Some OSPs such as Escorts.com have been forced to shut down based solely on material posted by third parties. [197]

A number of OSPs have implemented self-policing efforts, or "best practices," in the attempt to ward off potential criminal exposure. [198] Another self-regulatory device that has become somewhat of an industry standard is the concept of "community policing," which relies on the OSP's customers or users to identify inappropriate or illegal content and report it to the network operator for possible removal. However, as with most notice and takedown-type systems utilized in the adult Internet industry, this reporting model easily lends itself to abuse by web users. For example, a competitor of an OSP containing adult content may contact the site's operator claiming that models depicted in certain user profiles are underage, even if that is not the truth. Fearing

serious criminal liability stemming from child pornography violations, the network operator removes the content, allowing a competitor's abuse of the system to effectively eliminate perfectly legal speech and gain a leg up on the competition in the process. This very scenario has played out repeatedly in the author's representation of online escort sites, whereby competing escort agencies submit false “take down notices” claiming various illegalities with competitors' advertising copy.

Despite good faith efforts by OSPs to implement best practices and community policing of illegal content, legal liability for a wide variety of criminal offenses at the state and federal levels remains a real possibility. Law enforcement officials targeting particular OSPs will predictably continue to ***209** exploit this weakness, and obtain results that would not be realistic if pursued in court, and which may even amount to unconstitutional censorship. Even if specific instances of illegal conduct by users were established, such would not be grounds for shutting down entire communication networks. Nonetheless, the old adage, “you can beat the rap but you can't beat the ride,” has never been more applicable than with large, often publicly listed OSP corporations threatened with criminal prosecution based on UGC. [199]

Ultimately, large respected OSPs cannot risk being caught up in any “messy” business like allowing third parties to engage in controversial speech, absent clear statutory protection from criminal prosecution. The end result is massive self-censorship, designed to avoid any criminal problems. The Craigslist.org case is a prime example. Given the absence of any statutory protection allowing it to continue providing a venue for erotic-themed personal ads, Craigslist chose to shut down that portion of its website, a sobering example of an instance where censorship of an entire category of protected speech becomes the only realistic option for a company.

In practice, the only factor that has kept criminal prosecutions against OSPs in check is the political fallout associated with taking on those companies that provide access to online communications. Large, publicly traded ISPs maintain close relationships with lobbyists and politicians. Any criminal prosecution that could jeopardize their business model, or cause major uncertainty for their shareholders, is discouraged by the political system. Therefore, the only instances of criminal prosecution in this arena have been directed against adult-themed OSPs, and not against mainstream operators. But the precedent set by application of criminal laws against any OSP, regardless of content, puts at risk all OSPs, given the inability to control each and every kilobyte of content uploaded to their networks. Therefore, what may seem like an isolated problem faced by an unpopular subset of OSPs will ultimately impact even mainstream OSPs like Facebook or Google.

The § 2258A reporting regime offers the only source of formal immunity for criminal liability based on third-party activity. This is clearly insufficient to address the myriad risks facing OSPs in the criminal realm. The only realistic solution to this pervasive problem is decisive legislative action at the federal level.

Surprisingly, the last time Congress considered any action to protect OSPs from criminal liability was in 2002, when Rep. Bob Goodlatte introduced the Online Criminal Liability Standardization Act (OCLSA). [200] Noting the plight ***210** of OSPs (as detailed in this article), the sole intention of the bill was to minimize the criminal exposure of OSPs as a result of third-party conduct. [201] Although the bill was relatively well received in the House, it ultimately died in committee a few short months after its introduction. [202] The OCLSA was intended to amend the federal criminal code to ensure that no interactive computer service provider could be found liable for a crime arising from transmitting, storing, distributing, or making available material provided by another person--in other words, UGC. [203] However, this limitation on criminal liability would be waived if it were proven that the OSP itself intended that the service be used in the commission of the crime in question. [204] Delving into the issue of intent, the OCLSA stated that the OSP would not be found to have the requisite intent to defeat the liability limitation unless: (1) the provider's employee or agent possessed intent to commit the crime; and (2) the conduct constituting the offense was authorized, requested, commanded, or performed by a managerial member of the corporate structure acting for the benefit of the provider. [205]

Thus, almost an entire decade ago, Capitol Hill took notice of the concerns detailed herein, and considered taking rational, appropriate action. For reasons unknown, no similar legislation has been introduced in the House or the Senate since that time. Yet the criminal liability issues for OSPs have only increased with the surging popularity of social networking sites, tube sites, and other user-generated content platforms. A resurgent lobbying effort in support of new OCLSA-type legislation would be an immense benefit to the OSP community. Similar to the Congressional intent behind § 230, fostering cooperation between law enforcement and service providers is a key priority for any such legislation. A major detriment to this symbiotic theory of teamwork between these interests is the valid fear held by OSPs that any efforts on their part to assist law enforcement investigations will ultimately be used against them. Clarity in statutory obligations with associated immunity is the only way to alleviate those concerns, so that OSPs are properly incentivized to provide maximum cooperation in investigations relating to customer activity, without taking on additional potential criminal exposure themselves. For that reason, ***211** the introduction of new federal legislation similar to OCLSA is essential. Such legislation could build in appropriate procedural safeguards to ensure that OSPs that are complicit in encouraging illegal use of their services could still be held accountable, while providing broad immunity covering otherwise innocent OSPs who are themselves victimized through illegal conduct by their customers or end users.

Should Congress not act in addressing this increasingly urgent concern, those OSPs still operating in the United States will be forced to question the cost-benefit ratio of operating a UGC site within U.S. borders. As it stands, many popular adult "tube" sites and adult dating sites have established themselves overseas and, presumably, outside U.S. criminal jurisdiction.[206] This trend of scaring OSPs out of the country over concerns of criminal prosecution based on UGC--with the associated U.S. job loss--will only continue in the absence of some grant of immunity.

Conclusion

Given the uncertainty surrounding the potential exposure facing OSPs for criminal violations, the draconian penalties associated with the relevant criminal offenses, and the stakes relating to the free flow of information on the Internet, continued inaction on this issue cannot be ignored any longer. The failure of the United States to take the lead in developing clear protections for innocent service providers whose networks are exploited by criminals has led to a movement of the industry offshore--which has already begun. The ambiguities associated with obscenity and other statutes directed at the adult entertainment industry have fostered paranoia by service OSPs causing them to make premature, and sometimes irrational, business decisions. As seen first-hand with cases involving Craigslist.org and Escorts.com, OSPs are reaching a point of utter panic where they are more willing to revamp an entire business model, or cease doing business entirely, rather than face the unknowns of criminal liability. The situations experienced by Craigslist.org and Backpage.com amount to nothing more than glorified bullying by certain law enforcement agencies that seek to exploit the loophole in criminal liability that has not been addressed by Congress. In the case of Craigslist, the censors won. Backpage.com is fighting off boycotts, threats, and intimidation by everyone from local politicians to the National Organization of Women. Escorts.com appears to have given up and shut down as incompatible with fundamental First Amendment principles. Realistically, until an OSP calls the bluff of law enforcement (possibly through multiple appeals), the cycle will simply continue. For many established OSPs, a criminal test case is simply not a realistic option. Thus, until Congress acts with a rational piece of legislation ***212** that is long overdue, or a court interprets existing law to provide protection for criminal liability, the stalemate remains.

Certainly the Internet should not become a venue for anarchy, but by the same token, current law should not result in the stifling of online speech and innovation. The lack of any recognized statutory protection for service OSPs has resulted in the chilling of speech via a medium of communication that was created for the sole purpose of promoting the dissemination of speech. At present, adult-themed OSPs are on the front lines of this battle. The public has, in essence--knowingly or otherwise--used the adult industry as a barrier for decades, allowing the industry to take the hits and fight the First Amendment battles from the trenches. Meanwhile, mainstream society remains blissfully unaware of the time, effort, and resources expended in challenging questionable laws affecting Internet speech. Adult entertainment businesses are accustomed to operating with a

target on their backs, and although this Article focuses on adult content-themed OSPs, the potential criminal liability is shared by all online businesses that permit user-generated content on their networks. Despite any personal opinions one might have relating to adult content, the material itself, although possibly offensive to some, enjoys a presumption of legality.[207] Thus, from a legal standpoint, the publication of erotic material is no different from the average citizen expressing his inner-most thoughts on a blog or admonishing the federal government on a news forum. Erotic material is, constitutionally speaking, just as "valuable" a category of speech as any other topic of expression. Should state and federal authorities continue down the current path of criminalizing the mere act of providing an online venue for expressive activities, the danger of censorship will not stop at the door of erotica. All other forms of speech are only as safe under the First Amendment as are the most offensive and controversial communications.

In recent decades, the Internet has provided the public with an unprecedented venue for the dissemination of speech. Regrettably, as with most novel platforms of speech, there are those who desire to misuse such venues for illicit purposes. When confronting crime occurring by means of the World Wide Web, it is imperative to impose strong consequences on those who choose to commit crimes, while at the same time instituting a uniform liability standard for OSPs who are, at most, passive conduits of information. Allowing or even tolerating the possibility of OSPs being held criminally liable for the actions of their users creates an intolerable situation that results in self-censorship and migration of valuable business operations overseas, where the laws are clearer, or law enforcement less aggressive against OSPs. By sitting idly by, Congress fosters such instability. By any standard, the remedy for illegal activity by third parties is not to shoot the messenger.

Footnotes

a1 Lawrence Walters is a nationally recognized First Amendment expert, and is the founder of Walters Law Group. This Article was written with the invaluable assistance of the firm's associate attorney, Kimberly Harchuck, LLM. Walters has served as the President and National Chairman of the First Amendment Lawyers Association (2008-2010), and currently serves as General Counsel to the Woodhull Sexual Freedom Alliance, and the Association of Sites Advocating Child Protection. Many of the firm's clients are online service providers, and Mr. Walters has been involved in much of the cutting-edge litigation relating to service provider liability. He can be reached at Larry @FirstAmendment.com.

1 Nate Anderson, Porn Pros Hope to Squelch Online Piracy by 2012, Ars Technica (Oct. 25, 2010, 1:22 PM), http://arstechnica.com/tech-policy/news/2010/10/porn-pros-hope-to-squelch-online-piracy-by-2012.ars.

2 Mathew J. Schwartz, Adult Content Producers Take On BitTorrent Traders, Info. Wk. (Sept. 7, 2010), available at http://www.informationweek.com/news/infrastructure/traffic_management/227300248.

3 See Free Speech Coalition, http://fscapap.com (last visited Nov. 15, 2011).

4 G. Zisk Rice, Flava Works Sues Website Members Over Copyright Infringement, YNOT (July 29, 2011, 10:18 AM), http://www.ynot.com/content/117056-flava-works-sues-website-members-copyright-infringement.html.

5 See Anderson, supra note 1.

6 See Jon Swartz, Online Porn Often Leads the High Tech Way, USA Today (Mar. 9, 2004), available at http:// www.usatoday.com/money/industries/technology/2004-03-09-onlineporn_x.htm.

7 Viacom v. YouTube, No. 10-3270 (2d Cir. filed Aug. 11, 2010); see also Daniel Diskin, Why Google Will Prevail In Viacom's YouTube Copyright Lawsuit, Copyright & Trademark Blog (Mar. 24, 2011), http:// copymarkblog.com/2011/03/24/why-google-will-prevail-in-viacoms-youtube-copyright-lawsuit.

8 See, e.g., 18 U.S.C. § 2 (2006) (establishing liability for aiding and abetting); 18 U.S.C. § 371 (2006) (establishing liability for conspiring to commit a crime).

9 See, e.g., 18 U.S.C. §§ 1961-1968 (2006) (defining and providing liability for engaging in racketeering).

10 See Pleasant Grove City v. Summum, 555 U.S. 460, 461 (2009) (citing Carey v. Brown, 447 U.S. 455, 463 (1980)).

11 See Complaint at 23, Craigslist, Inc. v. McMaster, No. 2:09-1308-CWH (D.S.C. May 20, 2009) ("As a practical matter, the only way for Craigslist to assure compliance with Defendant McMaster's demands would be to shut down completely all portions of its website dedicated to the State of South Carolina. This is so because McMaster has demanded that, in order to avoid criminal investigation and prosecution, Craigslist must prevent third parties from posting ads or notices that may contain material McMaster has identified as illegal, and the only way to assure that such material is not posted would be to shut down entirely all portions of the site dedicated to the state of South Carolina.").

12 For example, Malta has an increasingly sophisticated bandwidth capacity. See Infrastructure and Communications, Malta Enterprise (last updated June 25, 2008), http://www.maltaenterprise.com/infrastructure_ communications.aspx. Gibraltar has also experienced exponential growth in bandwidth resources. See Gibtelecom Brings New Telecommunications Cable to Gibraltar, Gibtelecom (Feb. 23, 2011), http://www.gibtele.com/about-us/news/newsroom/eig_activation.php.

13 Julia Scheeres, ISP Guilty in Child Porn Case, Wired (Feb. 16, 2001), http://www.wired.com/culture/lifestyle/news/2001/02/41878.

14 See id.

15 Id.

16 Id.

17 See 47 U.S.C. § 230 (2006) (providing in relevant part that "[n]o 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").

18 An access software provider is "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." 47 U.S.C. § 230(f)(4) (2006).

19 47 U.S.C. § 230(f)(2) (2006).

20 Universal Commc'n Sys. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007).

21 Batzel v. Smith, 333 F.3d 1018, 1030 n.15 (9th Cir. 2003); see also Ben Ezra Weinstein & Co. v. AOL, Inc., 206 F.3d 980, 985 (10th Cir. 2000) (holding that AOL was an interactive computer service when it published an online stock quotation service); Zeran v. AOL, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (finding the same when AOL-operated bulletin board service for subscribers); Blumenthal v. Drudge, 992 F. Supp. 44, 49-50 (D.D.C. 1998) (finding the same when AOL functioned as the publisher of an online gossip column); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Ct. App. 2002) (holding that an online auction website is an "interactive computer service"); Barrett v. Clark, No. 833021-5, 2001 WL 881259, at *9 (Cal. Sup. Ct. July 25, 2001) (considering newsgroup an "interactive computer service"); Schneider v. Amazon.com, 31 P.3d 37, 40-41 (Wash. Ct. App. 2001) (finding the same for online bookstore Amazon.com).

22 See, e.g., Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

23 The best-known example of this UGC business model is YouTube.com.

24 Everton Bailey, Jr., State AGs: Craigslist Should Drop Adult Services, Seattle Times (Aug. 24, 2010, 10:07 AM), http://abcnews.go.com/Technology/wireStory?id=11472712; see also Alex Johnson, Authorities Seek to Crack Down on Craigslist, NBC Wash. (May 6, 2009, 1:45 AM), http://www.nbcwashington.com/the-scene/archive/Authorities_seek_to_crack_down_on_Craigslist.html.

25 Michael Arrington, South Carolina Gives Craigslist Ultimatum: Remove Prostitution or Face Criminal Charges, Tech Crunch (May 5, 2009), http:// techcrunch.com/2009/05/05/south-carolina-gives-craigslist-ultimatum-remove-prostitution-or-face-criminal-charges.

26 Greg Sandoval, Craigslist to Remove 'Erotic Services' Section, CNET (May 13, 2009, 9:33 AM), http:// news.cnet.com/8301-1023_3-10239610-93.html? part=rss&subj=news&tag=2547-1023_3-0-5.

27 Clif LeBlanc, McMaster Says No to Craigslist Deal, The State (May 14, 2009), available at http://web.archive.org/ web/20090618032125/http:// www.thestate.com/local/story/785877.html.

28 Craigslist, Inc. v. McMaster, No. 2:09-1308-CWH (D.S.C. filed May 22, 2009); see also Jonathan E. Skillings, Craigslist Sues So. Carolina Attorney General, CNET (May 20, 2009, 8:58 AM), http://news.cnet.com/8301-1023_ 3-10245380-93.html.

29 Chris Matyszczyk, Craigslist Censored: Adult Section Removed, CNET (Sept. 4, 2010), http:// news.cnet.com/8301-17852_3-20015629-71.html.

30 Craigslist stepped out of the limelight for a while after it removed the U.S. escort ads. After initially agreeing to dismiss its litigation against South Carolina Attorney General Henry McMaster seeking an injunction permanently barring criminal charges against Craigslist executives related to the site's adult advertisements, in December 2010, the company filed a motion to reconsider with the South Carolina District Court, effectively reopening the case. A hearing on the effort to reinvigorate the case was set for March 10, 2011, but was later cancelled as Craigslist quietly and unexpectedly withdrew its request for reconsideration without explanation. Again, no legal decision clarifying the liability of an online service provider for the acts of third parties was issued, and the case merely disappeared. See Wendy Davis, Craigslist Drops Suit Involving Execs, Adult Ads, Media Post (Mar. 7, 2011, 3:31 PM), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_ aid=146263.

31 In Our Own Backyard: Child Prostitution and Sex Trafficking in the United States: Hearing Before the Subcomm. on Human Rights of the S. Comm. on the Judiciary, 111th Cong. 1 (2010) (statement of Sen. Ruchard Durbin), available at http://www.gpo.gov/fdsys/ pkg/CHRG-111shrg58003/pdf/CHRG-111shrg58003.pdf.

32 Geoff Duncan, Attorneys General Target Backpage Online Classifieds, Digital Trends (Sept. 23, 2010), http:// www.digitaltrends.com/computing/attorneys-general-target-backpage-online-classifieds; see also Letter from State Atty's Gen. to Samuel Fifer, Sonnenschein, Nath & Rosenthal, LLP, Re: backpage.com (Sept. 21, 2010), available at http://ago.mo.gov/pdf/ Backpage.pdf.

33 Press Release, Conn. Att'y Gen.'s Office, Attorney General's Statement on Backpage.com Refusal to Take Steps That Block Prostitution Ads (Sept. 21, 2010), available at http://www.ct.gov/ag/cwp/view.asp? Q=466074&A=3869.

34 Wendy Davis, Village Voice Sued for Aiding and Abetting Sex Trafficking, Media Post (Sept. 20, 2010, 8:03 PM), http:// www.mediapost.com/publications/article/136047/; see also M.A. v. Village Voice Media Holdings, No. 4:10cv1470, 2011 WL 3607660, at *15 (E.D. Mo. Aug. 15, 2011) ("Plaintiff artfully and eloquently attempts to phrase her allegations to avoid the reach of § 230. Those allegations, however, do not distinguish the complained-of actions of Backpage from any other website that posted content that led to an innocent person's injury. Congress has declared such websites to be immune from suits arising from such injuries.").

35 See The Backpage.com Blog, http://blog.backpage.com (last visited June 4, 2012).

36 Backpage Steps up Safety Efforts, Calls for National Task Force, The Backpage.com Blog (Oct. 17, 2010, 11:00 PM), http:// blog.backpage.com.

37 See Press Release, Montgomery Cnty., Md. Sheriff's Office, Vice and Intelligence Detectives Develop Initiatives Against Human Trafficking (Nov. 8, 2010), available at http://connectedcommunities.us/showthread.php?t=39997 ("The Vice Section is also requesting that Backpage and EROS discontinue the future advertisement of these individuals or be prepared to be found complicit in the crime of human trafficking."). The press release has since been removed from the Montgomery County website.

38 Rhett Pardon, FBI Agents Raid Hotmovies' Office, XBIZ (Oct. 27, 2010, 9:15 AM), http://newswire.xbiz.com/view.php?id=126774. While the timing of these events is suspicious, there is no evidence that they are directly linked.

39 Agents Raid Porno Giant in Philadelphia, UPI (Oct., 28, 2010, 10:53 PM), http://www.upi.com/Top_News/US/2010/10/28/Agents-raid-porno-giant-in-Philadelphia/UPI-56781288320801.

40 Widespread industry speculation suggested that the closure of Escorts.com resulted from some sort of negotiation with the prosecuting authorities. See Escorts.com is Shutting Down, Confessions of a Message Bd. Hooker (May 27, 2011), http:// jennydemilo.com/2011/05/escorts-com-is-shutting-down/.

41 See Letter from Nat'l Ass'n of Att'ys Gen. to Samuel Fifer, Counsel for Backpage.com, LLC (Aug. 31, 2011), available at http:// www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2011/NAAG_Backpage_ Signon_08-31-11_Final.pdf.

42 Id.

43 Id.

44 Id.

45 See Plea Agreement, United States v. R.S. Duffy, Inc., No. 4:11-cr-00305-CCC (M.D. Pa., Nov. 11, 2011).

46 Press Release, U.S. Att'y Gen.'s Office Middle Dist. of Pa., Internet Escort Services Firms Charged With Money Laundering; Agree to Fine And Forfeiture Totaling $6.4 Million (Nov. 11, 2011), available at http:// www.justice.gov/usao/pam/news/2011/R.S. %20Duffy_A-1_11_1_2011.htm.

47 See R.S. Duffy, Plea Agreement, supra note 45, at *4.

48 See Press Release, supra note 46.

49 See R.S. Duffy, Plea Agreement, supra note 45, at *9-*12. Notably, although the settlement bans the government from bringing additional criminal charges against the companies and their other related business ventures, the agreement does not bind the Internal Revenue Service from pursuing any tax-related criminal charges arising from the money laundering. Further, prosecutors have reserved the right to criminally pursue individuals associated with both companies, however, there is no indication that the government intends to pursue such an option.

50 17 U.S.C. § 512 (2006) (providing limitations on civil liability for certain acts of providing online communication ability or data storage to third parties).

51 47 U.S.C. § 230 (2006).

52 17 U.S.C. § 512(c) (2006). Service providers must also designate an individual to receive the notifications of copyright infringement and be sure to make the contact information of such an agent readily available to the users of its website.

53 47 U.S.C. § 230(c) (2006) states, in part:
Protection for ‘Good Samaritan’ blocking and screening of offensive material. (1) Treatment of publisher or speaker: No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2) Civil liability: No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).
47 U.S.C. § 230(c) (2006).

54 Stratton Oakmont, Inc. v. Prodigy Servs., No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24,1995).

55 Id. at *1.

56 Id. at *5.

57 Id. (“Prodigy's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice.”).

58 141 Cong. Rec. S1944 (daily ed. Feb. 1, 1995) (statement of Sen. Exon).

59 See 141 Cong. Rec. H8478-79 (daily ed. Aug. 4, 1995).

60 141 Cong. Rec. H8469-70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox) (“[O]ur amendment will ... protect [online service providers] from taking on liability such as occurred in the Prodigy case in New York.”).

61 Cong. Rec. supra note 60, (citing 141 Cong. Rec. 16009-10 (1995) (statement of Sen. Leahy)); see also 141 Cong. Rec. S8334-35 (daily ed. Jun. 14, 1995) (statement of Sen. Feingold).

62 Reno v. ACLU, 521 U.S. 844 (1997).

63 Id. at 874.

64 Section 230 effectively immunizes both users and providers of an interactive computer service from tort liability.

65 47 U.S.C. § 230(f)(2) (2006) (“The term ‘interactive computer service’ means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.”).

66 18 U.S.C. § 230(c)(1) (2006).

67 18 U.S.C. § 230(c) (2006).

68 See, e.g., Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997); Dart v. Craigslist, 665 F. Supp. 2d 961 (N.D. Ill. 2009); Doe IX v. MySpace, Inc., 629 F. Supp. 2d 663 (E.D. Tex. 2009).

69 519 F.3d 666 (7th Cir. 2008).

70 Id.

71 Fair Hous., Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).

72 Id. at 1165. Roommates.com used drop-down boxes to solicit personal data from its users, and required certain information from all users, including:
Roommates requires subscribers to specify, using a drop-down menu provided by Roommate, whether they are ‘Male’ or ‘Female’ and then displays that information on the profile page. Roommates also requires subscribers who are listing available housing to disclose whether there are currently ‘Straight male(s),’ ‘Gay male(s),’ ‘Straight female(s)’ or ‘Lesbian(s)’ living in the dwelling. Subscribers who are seeking housing must make a selection from a drop-down menu, again provided by Roommates, to indicate whether they are willing to live with ‘Straight or gay’ males, only with ‘Straight’ males, only with ‘Gay’ males or with ‘No males.’ Similarly, Roommates requires subscribers listing housing to disclose whether there are ‘Children present’ or ‘Children not present’ and requires housing seekers to say ‘I will live with children’ or ‘I will not live with children.’ Roommates then displays these answers, along with other information, on the subscriber's profile page. This information is obviously included to help subscribers decide which housing opportunities to pursue and which to bypass.
Id.

73 See NPS LLC v. StubHub, Inc., No. 06-4874-BLS1, 2009 WL 995483 (Mass. Super. Ct. Jan. 26, 2009). The court found that StubHub "materially contributed" to the illegal "ticket scalping" of its sellers, and that there was sufficient evidence to prove the ticket scalping violations, placing StubHub outside the immunity provided by § 230. Id. at *13.

74 47 U.S.C. § 230(e)(3) (2006) ("Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

75 Voicenet Commc'n v. Corbett, No. 04-1318, 2006 WL 2506318 (E.D. Pa. Aug. 30, 2006). Usenet service providers and Internet access providers sued Pennsylvania law enforcement officials under 42 U.S.C. § 1983, seeking to remedy violations of their constitutional rights as a result of the state's action. Id. at *1.

76 Id.

77 Id.

78 Id.

79 Id. at *4. The court further stated that whenever possible, statutes should be interpreted to give effect to every word used and the defendants' understanding of § 230 would render superfluous the word "federal" in subsection (e)(1). Moreover, if Congress had intended for state criminal laws to preempt the CDA, it would have specifically stated so.

80 People v. Gourlay, No. 278214, 2009 WL 529216, at *1 (Mich. App. Ct. 2009).

81 Id.

82 Id.

83 Id. The offenses required proof that the defendant actively and intentionally directed the child to engage in sexual activity for the purpose of producing child pornography.

84 Id.

85 Id. at *2.

86 Id. at *3.

87 Id. at *5 n. 4. The court concluded that Gourlay was an "active participant" in the creation of the illegal materials on the basis that he: (1) knew the minor operated a website containing pornographic images of a minor and further recognized that was also the purpose for the two newly launched sites; (2) hosted the websites containing the illegal images with his web hosting company and registered the domain names as well; (3) programmed the websites to generate a live video stream; (4) created the members-only sections for the websites; and (5) provided the minor with additional tools to aid in the creation of the pornographic image. Notably, these actions were not provided to any of the other websites hosted by the Defendant, further proving that Gourlay was not simply acting as a passive service provider.

88 Id. ("An interactive computer service provider, by providing bandwidth, by publishing content that was generated by an information content provider's use of the service's general features and mechanisms, or by knowing of the nature of the published content, has not taken an intentional action directed toward a child to engage the child in child sexually abusive activity.").

89 47 U.S.C. § 230(e)(1) (2006).

90 Id. ("Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.").

91 Doe v. Am. Online, 783 So. 2d 1010 (Fla. 2001).

92 Id. at 1011. Doe did not allege that photographs or images of her son were transmitted via the AOL service.

93 Id. at 1012-13.

94 Id. at 1018.

95 Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009)

96 Id. at 961.

97 Id. at 963.

98 Id. at 965.

99 18 U.S.C. § 1952 (2006).

100 The federal law issue avoided here is whether § 230's stated inapplicability to federal criminal statutes would strip it of any immunity from the Sheriff's public nuisance claims.

101 Dart, 665 F. Supp. 2d at 961; see also 47 U.S.C. § 230(e)(1) (2006).

102 Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *1 (E.D. Tex. Dec. 27, 2006).

103 Id.

104 Id. at *2.

105 Id. at *3.

106 Id. at *5 (emphasis added).

107 See Stoner v. eBay, Inc., No. 30566, 2000 WL 1705637, at *3 (Cal. Sup. Ct., Nov. 1, 2000) (“[M]any of these products may be contraband, and however many it might be possible for defendant to identify as such, Congress intended to remove any legal obligation of interactive computer service providers to attempt to identify or monitor the sale of such products.”); 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

108 Over time, some exceptions to the scienter requirement have developed, and these are known as “strict liability offenses.” Exploitation of a minor often falls into this category, since neither consent nor lack of knowledge of the minor's age are typically considered as valid defenses to such a charge. However, scienter is an essential element of the vast majority of criminal offenses--particularly those involving communications potentially protected by the First Amendment. Cf. United States v. X-Citement Video, Inc., 513 U.S. 64 (1994).

109 Model Penal Code § 2.06(3)(a) (1981).

110 18 U.S.C. § 2(a) (2006).

111 Note that, though the crime of aiding and abetting requires the ultimate completion of a crime, a defendant may still be liable under § 2 even if said defendant does not actually take part in the criminal offense. See Casino City, Inc. v. U.S. Dep't of Justice, No. 04-CV-00557 (M.D. La. filed Aug. 9, 2004).

112 18 U.S.C. § 371 (2006). Although facially limited to conspiracy to “defraud” the United States, this term has been defined extremely broadly, to involve any scheme to interfere with government functions, or cheat the government out of money or property through criminal acts. See also Hammerschmidt v. United States, 265 U.S. 182 (1924); Hass v. Henkel, 216 U.S. 462 (1910). In addition, many criminal statutes have their own “conspiracy” sections, creating a separate offense to conspire to engage in the substantive offense addressed in the statute.

113 For example, in a situation involving an escort directory website, if a user posts a public ‘review’ of the escort's services, and indicates that the escort engaged in sexual activity for hire (without regard to whether the statement is truthful or not) this information could be used by law enforcement to demonstrate actual or constructive knowledge of illegal activity by the website operators.

114 Model Penal Code § 2.06(3).

115 H.R. Rep. No. 966, at 3 (1961), reprinted in 1961 U.S.C.C.A.N. 2664, 2666; see also United States v. Ruiz, 987 F.2d 243, 250-51 (5th Cir. 1993), cert. denied, 510 U.S. 855 (1993) (holding that the government is not required to prove that the defendant personally engaged in a continuous course of conduct, but rather the government must prove that there was a continuous business enterprise and that the defendant participated in the enterprise); United States v. Vaccaro, 816 F.2d 443, 454 (9th Cir. 1987), cert. denied, 484 U.S. 914 (1987) (holding that defendant's involvement in three jackpot cheating incidents over a three-year period was sufficient to show continuous and illegal conduct for a Travel Act conviction).

116 Travel Act convictions result in imprisonment for not more than five years and/or fines of the greater of not more than twice the gain or loss associated with the offense or $250,000 ($500,000 for an organization). See 18 U.S.C. § 1952(a)(3) (2006).

117 18 U.S.C. § 1952(b)(1) (2006) states in part:
As used in this section (i) ‘unlawful activity’ means (1) any business enterprise involving gambling, liquor on which the Federal excise tax has not been paid, narcotics or controlled substances (as defined in section 102(6) of the Controlled Substances Act), or prostitution offenses in violation of the laws of the State in which they are committed or of the United States, (2) extortion, bribery, or arson in violation of the laws of the State in which committed or of the United States, or (3) any act which is indictable under subchapter II of chapter 53 of title 31 ....
Id.

118 United States v. Montague, 29 F.3d 317, 322 (7th Cir. 1994).

119 Id.

120 See, e.g., United States v. O'Dell, 671 F.2d 191 (6th Cir. 1982) (describing a massage parlor that placed advertisements in a newspaper).

121 As most websites serve international clientele, some escorts in countries that do not prohibit prostitution are legally permitted to offer compensated sexual services. This would also include escorts operating in certain licensed brothels in Nevada.

122 Id.; see also Rewis v. United States, 401 U.S. 808 (1971) (inferring that Congress did not intend for the Travel Act to reach activities that may be advertised across state lines but will take place locally).

123 See, e.g., United States v. Peets, 165 F.3d 15 (2d Cir. 1998).

124 See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980).

125 Id.

126 A significant issue confronting the operators of such sites is keeping up with the ever-changing “slang” terms used to describe sex for money. Some online escort sites maintain lists of hundreds of words or phrases that cannot be included in ads, because they contain slang references to prostitution-related activity.

127 Escorts participate in a lawful business per local licensing laws specifically drafted to govern escorting activities, for example, various city and county ordinances across the United States enacted specifically for the escorting business model. See L.A. Cnty., Cal., Code ch. 7.38 (Escort Bureaus); Atlanta, Ga., Code ch. 30, art. VIII, div. 2 (Escort Permit); New Orleans, La., Code ch. 30, art. VII (Escort Services); Las Vegas, Nev., Code ch. 6.36 (Escort Bureaus & Personnel); Charlotte, N.C. Code § 6-303 (Escort & Dating Service Permit); Dallas Cnty., Tex., Code § 10-111 (License for a Sexually Oriented Business).

128 18 U.S.C. § 2256(8) (2006) states that:

Any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
Id.

129 See 18 U.S.C. § 2251 (2006) (“Sexual exploitation of children”); 18 U.S.C.§ 2251A (2006) (“Selling or buying of children”); 18 U.S.C. § 2252 (2006) (“Certain activities relating to material involving the sexual exploitation of minors”); 18 U.S.C.§ 2252A (2006) (“Certain activities relating to material constituting or containing child pornography”); 18 U.S.C. § 2260 (2006) (“Production of sexually explicit depictions of a minor for importation into the United States”); 18 U.S.C. § 1466A (2006) (“Obscene visual representations of the sexual abuse of children”).

130 See, e.g., 18 U.S.C. § 2251(e) (2006); 18 U.S.C. § 2252(b) (2006); 18 U.S.C.§ 2252A(b) (2006).

131 18 U.S.C. § 2258A (2006).

132 Such “knowledge” could be fulfilled via repeated notifications that a service provider's network is being used as a medium to circulate child pornography.

133 Such “strict liability” remains the result regardless of alleged or proven consent or misrepresentation of age by the minor.

134 United States v. X-Citement Video, Inc., 513 U.S. 64 (1994).

135 18 U.S.C. § 2252; see also Protection of Children Against Sexual Exploitation Act of 1977, 18 U.S.C. §§ 2251-2259 (2006).

136 X-Citement Video, Inc., 513 U.S. at 66-67; see also Tilton v. Playboy Entm't Grp., Inc., 554 F.3d 1371, 1378 (11th Cir. 2009) (upholding the district court's finding that the scienter requirement found in § 2252(a) and § 2252A(a) extends both to the sexually explicit nature of the material and to the age of the performer).

137 X-Citement Video, Inc., 514 U.S. at 78.

138 Id. at 76. The Supreme Court in X-Citement Video intended to discern the difference between producers of sexually explicit materials and other parties associated with the distribution, sale, or receipt of such material.

139 But see United States v. Extreme Assocs., Inc., 431 F.3d 150 (3d Cir. 2005) (holding that the defendant, charged with distributing obscene content, is an interactive computer service as defined by statute but because the defendant is also liable for the creation of the content as a producer, no defenses pertaining to scienter were available). Accordingly, if the OSP is also involved with the production of the contraband, the scienter defense will be unavailing.

140 See supra note 138 and accompanying text.

141 See Sundance Assocs., Inc. v. Reno, 139 F.3d 804, 808 (10th Cir. 1998); Am. Library Ass'n v. Reno, 33 F.3d 78, 82 (D.C. Cir. 1994) (acknowledging the existence and definition of “secondary producers” pertaining to adult content).

142 See, e.g., United States v. Lacy, 119 F.3d 742, 747 (9th Cir. 1997) (“This interpretation was necessary, as the [X-Citement] Court held, because the elements at issue were crucial to establishing liability. Distribution of sexually explicit material involving adults is legal, while distribution of sexually explicit material involving minors is not. Unless a distributor knew the performers were underage, the Court reasoned, he would have reasonably expected his conduct to be legal.”).

143 Such immunity applies to reported cases of child pornography only. Despite participation in the reporting program and/or any good faith policing efforts, a service provider is still liable for any illegal content found on its network.

144 This reporting requirement dates back to 1998, when it was included as part of the Protection of Children from Sexual Predators Act of 1998, Pub. L. No. 105-314, 122 Stat. 4229; see also 42 U.S.C. § 13032 (1998) (repealed 2008). In October of 2008, the Protect Our Children Act was passed, and it included an amendment that repealed the old reporting protocol while creating a more detailed and complex reporting requirement. Pub. L. No. 110-401, 122 Stat. 4229 (2008).

145 An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications" while a "remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. §§ 2510(15), 2711(2) (2006). Given the breadth of these definitions, almost any hosting or other online service allowing users to upload or otherwise transmit data would qualify as a service provider.

146 18 U.S.C. § 2258A(a)(1) (2006); see also The CyberTipline, Nat'l Center for Missing & Exploited Children, available at http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_ US&PageId=2936 (last visited Nov. 17, 2011).

147 18 U.S.C. § 2258A(f) (2006). Additionally, registered service providers are not required to affirmatively seek facts or circumstances that would lead to triggering the reporting requirement.

148 The immunity afforded by the NCMEC reporting system only extends to actions taken in connection with discharging the reporting obligation; it does not provide blanket relief from liability for the participating entity.

149 See 18 U.S.C. §§ 2257, 2257A (2006); 28 C.F.R. pt. 75 et seq. (2010).

150 18 U.S.C. § 2257.

151 Id. The basic obligations listed in § 2257 are as follows: (1) Identify obtain and examine a valid and legal identification document containing the performer's name and date of birth and to record and maintain such information; (2) Create and maintain retrievable, valid identification records; (3) Include on each copy of the content, digital or otherwise, a statement of compliance, which identifies the title of the work, the date of production, the identity of the custodian of record and the address where the records are held; and (4) Make such identification records readily available for inspection.

152 18 U.S.C. § 2257(e).

153 28 C.F.R. § 75.1(c)(2).

154 Although only addressed in the civil context, numerous courts have determined that "Intermediaries are not culpable for 'aiding and abetting' customers who misuse their services to commit unlawful acts." Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 967 (N.D. Ill. 2009); see also Chi. Lawyers' Comm. for Civil Rights under Law, Inc. v. Craiglist, Inc., 519 F.3d 666, 668 (7th Cir. 2008) ("Online services are in some respects like the classified pages of newspapers, but in others they operate like common carriers such as telephone services."); Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003).

155 28 C.F.R. § 75.1(c)(4)(v) (2010).

156 Notably, in the Official Comments to the 2008 amendments to the Code of Federal Regulations, the Department of Justice indicated that a social networking site would be protected by the exemptions, although no thorough analysis of the details was provided in the commentary: "First, most social networking sites would appear not to be covered by the statute and the rule under the definition of 'produces' in section 2257(h)(2)(B)(v) and§ 75.1(c)(4)(v), respectively." Revised Regulations for Records Relating to Visual Depictions of Sexually Explicit Conduct, 73 Fed. Reg. 77,432 (Dec. 18, 2008) (to be codified at 28 C.F.R. pt. 75.1). The statutory definition excludes from produces, "the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication, without selection or alteration of the content of the communication." Id.

157 18 U.S.C. § 2257(i).

158 See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (holding that the freedom to publish anonymously is protected by the First Amendment).

159 Notably, section 2257 liability may be triggered without the requirement that the government prove a knowledge or intent element, effectively turning a mere record-keeping oversight into a strict liability crime. See Plaintiff's Memorandum in Opposition to Defendant's Motion to Dismiss and Reply to Defendant's Memorandum in Opposition to Plaintiff's Motion for Preliminary Injunction at 33-35, Free Speech Coal., Inc. v. Holder, 729 F. Supp. 2d 691 (E.D. Pa. 2010) (No. 09-4607) (“Plaintiffs challenge [18 U.S.C. § 2257(f)(1) and 18 U.S.C. § 2257A(f)(1)] on the ground that they impose strict liability for failure to create and maintain records in connection with the production of sexually explicit expression and therefore, unconstitutionally chill protected expression.”).

160 18 U.S.C. § 2257(f)(4).

161 18 U.S.C. § 2257(e).

162 Alaska, Maine, New Mexico, Vermont, West Virginia, Montana, and South Dakota have no statewide obscenity laws and the courts in the states of Oregon and Hawaii have essentially invalidated their respective obscenity laws. See Summary of Obscenity and Related Law, Catholic News Agency, http:// www.catholicnewsagency.com/resource.php?n=1071 (last visited Nov. 9, 2011).

163 413 U.S. 15 (1973).

164 United States v. Little, 365 Fed. App'x 159 (11th Cir. 2010) (sentencing defendant to five years in prison for obscenity violations); United States v. Extreme Assocs., Inc., 431 F.3d 150 (3d Cir. 2005) (sentencing defendant to a year in prison for creating allegedly obscene material and mailing it across state lines); United States v. Stagliano, 729 F. Supp. 2d 215 (D.D.C. 2010) (dismissing all charges against this defendant, in what was considered a major loss for the Department of Justice); see also Mark Kernes, Feds Lose Stagliano Obscenity Case--First in Over 30 Years, XBIZ (July 18, 2010), http://businessavn.com/articles/Feds-Lose-Stagliano-Obscenity-Case-First-in-Over-30-Years-403911.html; Paula R. Ward, Porn Producer, Wife Get 1-Year Jail Terms, Pittsburgh Post-Gazette, July 2, 2009, http://www.post-gazette.com/pg/09183/981250-53.stm.

165 18 U.S.C. §§ 1462, 1465 (2006) (prohibiting a variety of activities with regard to obscene materials).

166 18 U.S.C. §§ 1462(c), 1465 (referencing the definition of an ICS pursuant to§ 230).

167 United States v. Thomas, 74 F.3d 701 (6th Cir. 1996). It can now safely be assumed that the act of transmitting obscene materials over the Internet, or via direct connections using modems, would trigger the application of 18 U.S.C. § 1465 and could subject the person or entity who transmitted the obscene materials to a criminal prosecution either in the jurisdiction from which the transmission originated, or the jurisdiction into which the transmission is received. Each individual item of obscene material which is transmitted could be treated as a separate offense.

168 State v. Wilson, No. 05-7738 (Fla. Cir. Ct. filed Oct. 7, 2005); see also David Kushner, Casualty of Porn, Rolling Stone, Dec. 5, 2005, http:// www.firstamendment.com/articles/Rolling_Stone_11.28.05.pdf?pageid=rs.NewsArchive&pageregion=mainRegion&rnd=1133276886977&has-player=true&version=6.0.12.1040.

169 Wilson v. Judd, 917 So. 2d 876 (Fla. Dist. Ct. App. 2005).

170 413 U.S. 15, 24 (1973). Obscenity means the status of a material in which (a) the average person, applying contemporary community standards, would find, taken as a whole, appeals to the prurient interest in sex, nudity or excretion; (b) depicts or describes, in a patently offensive way, sexual conduct as specifically described by statute; and (c) taken as a whole, lacks serious literary, artistic, political or scientific value.

171 See Thomas, 74 F.3d at 709 (permitting venue in district where government agent downloaded offending images).

172 Reno v. ACLU, 521 U.S. 844 (1997) (holding 47 U.S.C. § 223 unconstitutional under the First Amendment as it created criminal penalties for transmissions of obscene or indecent communications).

173 Some hosting companies specifically market to the adult webmaster customers, while others remain indifferent to the content of the communication on the customer's site, or actively restrict adult-oriented material on their servers.

174 New York v. Ferber, 458 U.S. 747 (1982); Hamling v. United States, 418 U.S. 87 (1974); Smith v. California, 361 U.S. 147 (1959).

175 See Alexander v. United States, 509 U.S. 544 (1993) (upholding the post-trial forfeiture provisions of RICO that mandate forfeiture of assets associated with a racketeering enterprise even in the context of an expressive business such as a bookstore); see also Adult Video Ass'n v. Barr, 960 F.2d 781 (9th Cir. 1992).

176 18 U.S.C. §§ 1961-1968 (2006).

177 An OSP is at risk for unintentionally violating RICO based on various offenses, ranging from involvement in obscenity, to wire fraud, to money laundering. Cf. 18 U.S.C.§ 1961(a) (2006).

178 A pattern of racketeering activity "requires at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years (excluding any period of imprisonment) after the commission of a prior act of racketeering activity." 18 U.S.C. § 1961(5) (2006).

179 J.F. Lawless & L.R. Jacobs, Criminal RICO (Racketeer Influenced and Corrupt Organizations Act)--The Gang's All Here, 22 Trial 9, 40-47 (1986).

180 See Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479 (1985) (holding the RICO statute applicable to "garden variety" business fraud).

181 18 U.S.C. § 1962(a)-(c).

182 This may be indicated by association or control of a business entity or an employee-employer type relationship with other involved parties. See 18 U.S.C. § 1961(4).

183 A pattern of racketeering activity requires at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years. See 18 U.S.C. § 1961(5).

184 Racketeering activity is defined by the particular federal laws specified in the statute. See 18 U.S.C. § 1961(1).

185 See Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (noting that obscenity laws were constitutionally limited in their applicability to "hard-core pornography"). This decision pre-dated Miller, but its general proposition is still followed in practice.

186 18 U.S.C. §§ 1462, 1465 (2006).

187 18 U.S.C. § 1963 (2006).

188 RICO was enacted in response to the difficulty in prosecuting organized crime syndicates. Unable to implicate higher-level crime bosses for the crimes committed by lower-level agents or associates, the legislature drafted the Act with the intent of eliminating the legal loophole that enabled actors that only passively participated in a crime to circumvent liability based on their limited involvement in the crime at issue. This type of distant chain of liability is precisely the sort of model that could enable the judiciary to find an online service provider criminally liable for third-party content, despite the provider's lack of involvement in the actual creation of the unlawful content.

189 18 U.S.C. § 1962(d) (2006).

190 Most, if not all, OSPs implement some sort of user terms that all users must agree to before uploading any material to the network. These agreements have come to be known as "click-wrap agreements."

191 Salinas v. United States, 522 U.S. 52, 65 (1997).

192 18 U.S.C. § 1962(d).

193 18 U.S.C. §§ 1462, 1465 (2006).

194 See, e.g., Doe v. Fry, No. 10-825 (M.D. Fla. filed May 21, 2010). Utilizing accomplice liability theories, plaintiff, a minor, sought to hold civilly responsible payment processors and other entities remotely associated with a website's publication of allegedly child-pornographic content.

195 Jeff Gore, Church and State, Orlando Wkly., Feb. 24, 2011, http:// orlandoweekly.com/news/church-and-state-1.1109454; see also Michael Kruse, Polk Sheriff Grady Judd Makes His Name on Moral Outrage, St. Petersburg Times, Feb. 6, 2011, http:// www.tampabay.com/news/publicsafety/article1149570.ece.

196 See generally United States v. Stevens, 130 S. Ct. 1577 (2010) (finding that 18 U.S.C. § 48 was substantially overbroad as it had the potential of infringing upon legal, protected speech and was therefore declared invalid under the First Amendment).

197 See R.S. Duffy, Plea Agreement, supra note 45.

198 For example, the Interactive Advertising Bureau has developed and promotes a set of best practices relating to interactive media advertising. See About The IAB, Int'l Adver. Bureau, http://www.iab.net/about_the_iab (last visited Nov. 9, 2011).

199 See Indictment, New York v. Fuchs, No. 2699/2006 (N.Y. Sup. Ct. Nov. 15, 2006). Charges of enterprise corruption, first-degree promotion of gambling, money laundering, and conspiracy were brought against several corporate entities and their agents in connection with a sports wagering website. Notably, among the named defendants were companies that merely provided web design services and communications and connectivity services to the website. See id.

200 See Online Criminal Liability Standardization Act of 2002 (OCLSA), H.R. 3716, 107th Cong. § 25(a)-(b)(1) (2002) (“[N]o interactive computer service provider, or corporate officer of such provider, shall be liable for an offense against the United States arising from such provider's transmitting, storing, distributing, or otherwise making available, in the ordinary course of its business activities as an interactive computer service provider, material provided by another person. The liability limitation created by this section does not apply if the defendant intended that the service be used in the commission of the offense.”).

201 Id.

202 See H.R. 3716 Bill Status, Govtrack.us, http:// www.govtrack.us/congress/bill.xpd?bill=h107-3716 (last visited Nov. 30, 2011).

203 Indictment, supra note 199.

204 OCLSA, supra note 200.

205 Id.

206 For example, popular adult tube sites like Redtube.com (Panama) and Pornhub.com (Hong Kong) are based overseas.

207 The two obvious exceptions are obscenity and child pornography. See United States v. Playboy Entm't Grp., 529 U.S. 803 (2000); Reno v. ACLU, 521 U.S. 844 (1997).