Doe v. MySpace, Inc.: Liability for Third Party Content on Social Networking Sites

MICHAEL D. MARIN AND CHRISTOPHER V. POPOV

MySpace is a Web 2.0 phenomenon. In less than four years, it has become one of the most visited sites on the Web, boasting over 150 million user profiles and wielding unprecedented potential for collaboration and marketing power. The MySpace concept, often referred to as online social networking, is simple. MySpace users create online profiles, or personal webpages, on which they post photographs, videos, and information about themselves. These profiles serve as a platform for users to network with an online community of people with common interests. This simple concept has revolutionized online advertising, politics, news, music, and ordinary Internet chatter.

But the tremendous popularity of social networking has been tarnished by a parallel public outcry over sexual predators who use the Internet to meet and seduce minors into having sex. This outcry has captured the attention of both politicians and plaintiffs' lawyers.

In June 2006, a fourteen-year-old girl and her mother filed a highly publicized lawsuit in Austin, Texas, against MySpace and its parent, News Corp., after the girl was sexually assaulted by a man she allegedly met on MySpace. The plaintiffs' suit, *Doe v. MySpace, Inc.*, sought $30 million in damages and alleged that MySpace and News Corp. were negligent and grossly negligent for failing to implement age verification procedures and to protect the fourteen-year-old from sexual predators. If successful, the suit would have been a significant, if not fatal, blow to social networking.

Last February, however, Judge Sam Sparks of the Western District of Texas dismissed the *Doe* case.[1] Relying upon the immunity afforded to "interactive computer services" under the Communications Decency Act (CDA) and upon Texas common law, the court held that MySpace could not be required to implement age verification procedures nor be held liable for claims flowing from its users' online communications.

Although the *Doe* case allowed MySpace and other social networking sites to breathe a temporary sigh of relief, it is unlikely to end attempts to hold such sites liable for their users' conduct. The *Doe* case is on appeal, and four new sexual predator suits have been filed against MySpace in Los Angeles.[2]

Political pressures continue to mount as well. A coalition of forty-four state attorneys general are pushing for laws that would require social networking sites to verify the age and identity of their users and to implement various protections for minors who use the sites, and at least one state legislature is currently debating such a bill.[3]

This article sets forth the legal defenses available to social networking sites faced with private lawsuits stemming from the criminal or tortious conduct of individuals who use the sites to harm another person. The article also discusses why proposed state statutes aimed at holding these websites liable for third party conduct are unlikely to survive legal scrutiny.

Defending Private Lawsuits

Social networking websites are not the first entities to encounter lawsuits based upon third party conduct. For years, plaintiffs have sought to hold traditional e-mail and Internet service providers liable for publishing defamatory or otherwise actionable content generated by third party users. Even before the advent of the Internet, parties sought to hold defendants with deep pockets liable for the tortious or criminal acts of a third person. Furthermore, social networking sites are not the first sites to face demands for online age verification; Congress has tried for nearly a decade to impose such a requirement on Internet sites offering pornography.

Claims based on these theories of liability have been largely unsuccessful and have given rise to well-established legal defenses. First, in light of the Communications Decency Act of 1996, courts have been virtually unanimous in their holdings that websites cannot be held liable for publication of third party content or for real world injuries that flow from the publication of third party content. Second, well-established common law principles provide that a person typically has no duty to protect another from a third party's criminal or tortious acts. Finally, the Supreme Court has made clear that requiring websites to institute online age verification violates the First Amendment because age verification is an ineffective means of protecting minors from harmful content and is an overly restrictive limitation on constitutionally protected speech.

As discussed below, these defenses apply with equal force in the social networking context and work to shield websites from liability for the criminal and tortious acts of their users.

CDA Immunity

The first line of defense against any claim based on content generated by a website's users, or based on its users' related offline conduct, is the immunity provided under the Communications Decency Act of 1996 (CDA), 42 U.S.C. § 230. In short, the CDA bars claims against interactive computer services based on the publication of third party content. Congress enacted the CDA for the stated purpose of promoting "the continued development of the Internet . . . unfettered by Federal and State regulation."[4] The act recognizes that is impossible to scrutinize the millions of postings made by users over e-mail or on Internet message boards. The act further recognizes that holding interactive computer services liable for posting defamatory or otherwise harmful user-generated content would severely diminish the online posting of third party content of all kinds.

Michael D. Marin (mmarin@velaw.com) is a partner and Christopher V. Popov (cpopov@velaw.com) is an associate in the Austin office of Vinson & Elkins, LLP. They represented MySpace, Inc. and its parent company, News Corp., in Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843 (W.D. Tex. 2007).*

To ensure that websites and other interactive computer services would not be crippled by such lawsuits, the CDA provides interactive computer services with broad immunity.[5] In pertinent part, it provides 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."[6] Importantly, the CDA further provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[7]

In light of these provisions, courts have broadly applied CDA immunity to all claims in which

(1) the defendant is "a provider or user of an interactive computer service,"
(2) "the cause of action treats the defendant as a publisher or speaker of information," and
(3) "the information at issue" is provided by a third party information content provider.[8]

The first and third prongs are easily satisfied in the social networking context. Social networking sites are providers of interactive computer services, and user-generated profiles found on social networking sites obviously constitute information provided by third party information content providers. In cases where a third party merely posts defamatory content on his profile, the second prong of the CDA analysis is easily satisfied as well; and the website clearly cannot be held liable as the publisher or speaker of that content.

The claim in a prototypical sexual predator case, in contrast, is less about speech (the actual words published online) and more about conduct, i.e., what happens when the parties meet offline. Indeed, the words themselves may be completely innocuous. Importantly, however, the *Doe* case held that this distinction between a sexual predator case and a typical defamation case is irrelevant for purposes of CDA immunity. This holding is proper under the CDA's plain language and necessary to effectuate its legislative purpose. But to fully appreciate why CDA immunity should apply in this circumstance, it is important to consider the similarities and differences between sexual predator cases and the more typical CDA case that merely involves some form of otherwise actionable speech.

Actionable Speech

The CDA has been most frequently applied to bar defamation-based claims. In the typical case, a plaintiff who believes that he or she has been defamed online by a third person sues the website that allowed the third person to publish the defamatory statement. Because the plaintiff's claim against the website in that case is based solely on its role as the publisher of the third party content, courts have held with virtual unanimity that such claims are barred under the CDA.[9]

A website's immunity from claims based on actionable speech is not diminished by allegations that it was on notice of the content at issue. In *Zeran v. America Online, Inc.*, for instance, the victim of a vicious prank sued AOL for its failure to remove a false advertisement for T-shirts featuring tasteless slogans relating to the 1995 bombing of the Oklahoma City federal building. The ad instructed interested buyers to call the plaintiff to place an order.[10] After receiving death threats from people who were enraged by the ad, Zeran learned of the prank and immediately demanded that AOL remove the ad from its bulletin board and post a retraction. Zeran argued that even if AOL were immune from liability for the initial posting, it was negligent for failing to remove the ad after Zeran gave notice of its falsity. The Fourth Circuit, however, affirmed the district court's dismissal of Zeran's claims, explaining that the CDA necessarily protects interactive computer services from liability even after they are notified of an allegedly defamatory or threatening post because the insupportable legal burden imposed by potential tort liability would undermine the CDA's goal of promoting speech on the Internet through interactive computer services.[11]

Under *Zeran* and its progeny, websites and other interactive computer services cannot be held liable for publishing defamatory or otherwise actionable speech generated by a third party.

Actionable Speech and Resulting Physical Injuries

Although the CDA is directed at claims that seek to hold an interactive computer service liable as the "publisher or speaker" of third party content, the immunity provided under § 230(c) is not limited to defamation- or speech-based torts. Courts have routinely applied CDA immunity to bar negligence and other claims based on physical harm that a plaintiff suffered as a result of defamatory or otherwise harmful content, and they have explicitly rejected arguments that CDA immunity is limited to claims for defamation.[12]

Indeed, applying CDA immunity to torts flowing from actionable speech is necessary to effectuate the act's purpose. Many, if not all, online defamation cases can be pleaded to include a claim for negligence or some other more general tort.

A classic example of such a case is *Carafano v. Metrosplash.com, Inc.*,[13] in which an unidentified third party posted a false online personal ad on Matchmaker.com portraying an actress named Christine Carafano to be a sexually promiscuous woman in search of random sexual partners. Shortly after the ad was posted, Carafano began receiving sexually explicit phone calls, letters, and hand-delivered notes at her home. The messages were so threatening that Carafano was forced into hiding for months. After the ordeal, Carafano sued Matchmaker.com. Although the essence of her lawsuit was defamation, Carafano asserted various causes of action including negligence, and she sought damages not just for the harm to her reputation but also for the emotional damage she suffered as a result of threats she received.

The Ninth Circuit affirmed the dismissal of all the claims, including negligence, holding that under § 230(c) of the CDA, "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity."[14] In so holding, the Ninth Circuit recognized that imposing tort liability of any kind on a website for its failure to ensure that all third party postings are "safe" or otherwise problem free would threaten the viability of websites and other interactive computer services and thereby reduce the channels of communication available on the Internet.

Physical Injuries Flowing from Facially Innocuous Speech

The prototypical online sexual predator case is at least superficially distinguish-

able from the prior two categories in that the suit might not involve a speech-based tort whatsoever. In the *Doe* case, for instance, the plaintiffs asserted no claim for defamation and explicitly argued that their claims were not based upon any particular posting on MySpace.com but rather on the fact that MySpace knowingly maintained a forum in which sexual predators could communicate with and seduce minors. As such, the plaintiffs argued that the CDA did not bar their claims against MySpace.

The court, however, concluded that this attempt to plead around the immunity provided by the CDA was disingenuous. Specifically, the court noted that no matter how artfully the plaintiffs attempted to plead their lawsuit, the underlying basis of their claims was that MySpace was negligent for allowing the minor and the man who assaulted her to exchange phone numbers and other personal information on MySpace. The court observed that the sole causal connection between MySpace and the plaintiffs' injuries was MySpace's publication of the communications between the minor and her attacker. For that reason, the court found, MySpace was entitled to immunity under the CDA regardless of the particular causes of action or theories of liability that the plaintiffs actually asserted.[15]

The *Doe* court's analysis is sound both as a matter of statutory interpretation and as a matter of public policy. Although defamation and other claims based on independently harmful speech are the most common claims barred by immunity geared toward the publication of third party content, nothing in the CDA limits the scope of its immunity to defamation or other speech-based torts. Rather, the CDA states in unmistakably clear terms that interactive computer services are immune from all claims stemming from their publication of such information: "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."[16] Thus, any claim that seeks to hold an interactive computer service liable based solely on its causal connection as the publisher of third party content is barred under the CDA.

Furthermore, this application of the CDA to harm flowing from facially innocuous publications is just. As explained above, Congress provided for broad CDA immunity because it is the "policy of the United States" to promote the further development of the Internet. Congress realized that imposing liability on interactive computer services for the publication of third party content would have a profound chilling effect on Internet speech. Due to the practical impossibility of screening the staggering volume of third party content posted online daily, websites faced with liability for user-generated speech would have no choice but to greatly restrict the volume of third party content they publish.

Courts applying these principles have concluded that the same practical limitations apply where liability is premised on the website's failure to respond when given notice of objectionable user-generated speech on its site. These arguments were only more compelling when applied in the context of the *Doe* case, where the communications appeared harmless on their face. If interactive computer services cannot reasonably be expected to screen patently objectionable content, including content that has been identified as objectionable, logic compels that it would be even more unreasonable to expect interactive computer services to screen facially innocuous content. If social networking sites were suddenly required to ensure that the millions of third party postings published on their sites daily were not only true but also well intentioned, social networking would no longer be viable as a business model.

No Duty Principles

In addition to the statutory immunity of the CDA, negligence claims seeking to hold social networking sites liable for the conduct of its users may be barred in many instances by well-established principles of common law. To state a claim for negligence or gross negligence, a plaintiff typically must establish the existence of a legal duty, a breach of that duty, and damages proximately caused by the breach. As the *Doe* court established, there is no legal basis for the proposition that a social networking website has a duty to protect its users from the criminal or tortious actions of other users. The general rule in Texas and elsewhere is that "a person has no legal duty to protect another from the criminal acts of a third person or to control the conduct of another."[17]

The general rule, of course, has exceptions. Certain special relationships may impose a duty upon one party to control the actions of another, including employer-employee and parent-child relationships. And many jurisdictions impose a duty on owners to protect their guests from foreseeable third party criminal acts occurring on their premises. None of these exceptions applies in the case of online social networking. The website's relationship with its users is not the type of special relationship that gives rise to a duty to control their actions. With respect to MySpace, each user is merely one of over 150 million people who have posted a profile on the website. MySpace, like most of its competitors, charges no fee, so users are not even customers.

Notwithstanding this attenuated relationship between the website and its users, the plaintiffs in the *Doe* case argued that MySpace has a duty to protect its users from sexual predators. Their argument was based on the novel theory that MySpace.com is a "cyber premises" on which it is foreseeable that predators will prey upon unsuspecting children. The court rightfully rejected the argument, noting that there is no legal basis for cyber-premises liability and that imposing liability under these circumstances would mean the end of social networking: "To impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in its tracks and close this avenue of communication."

Although *Doe* is the only case that addresses the issue with respect to social networking websites, it was not the first to reject the notion that interactive computer services have a duty to prevent injuries to their users. In *Doe v. GTE Corp.*, the Seventh Circuit affirmed the district court's dismissal of claims against a web hosting service for hosting clandestine videos of collegiate athletes who were unknowingly videotaped nude in a locker room.[18] Judge Easterbrook, writing for the court, rejected the notion that an Internet service provider has a duty to prevent injuries to third parties, comparing Internet service providers to other communication intermediaries, such as the postal service or a phone company,

which routinely enable third parties to commit crimes or perpetrate torts:

> Landlord, phone company, delivery service, and web host all could learn, at some cost, what [the user] was doing with the services and who was potentially injured as a result; but state law does not require these providers to learn, or to act as Good Samaritans if they do. The common law rarely requires people to protect strangers, or for that matter acquaintances or employees.[19]

Judge Easterbrook's observations are as astute as they are far-reaching. Just as phone companies and couriers have no duty to prevent third parties from using their services to perpetrate criminal and tortious activity, social networking sites should not be saddled with a legal duty to prevent third parties from using their services to commit crimes.

First Amendment Defense

In addition to claiming generally that MySpace had a duty to protect its users from one another, the plaintiffs in *Doe* argued that MySpace had a legal duty to verify the age and identity of its users; i.e., the plaintiffs argued that without effective age verification, MySpace's efforts to protect minors who use the site are meaningless. The argument echoes the primary battle cry of politicians seeking to put pressure on social networking sites to prevent sexual predators from contacting minors online. Although the *Doe* court rightly rejected this theory of liability as inconsistent with common law principles and the immunity provisions of the CDA, mandatory age verification is also prohibited by the First Amendment.

Against Age Verification

For years, Congress has unsuccessfully attempted to impose age verification requirements on websites that display pornographic images and videos. Its first attempt was embodied in § 223 of the CDA, 47 U.S.C. § 223, which criminalized the "knowing" transmission to any recipient under eighteen years of age any "obscene or indecent" message and any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Porn site operators could avoid criminal liability under § 223 by instituting age verification through certain designated forms of identification, such as a credit card or an adult identification number.[20]

Not long after the section was enacted, however, the Supreme Court issued its opinion in *Reno v. ACLU*, which held that the mandatory age verification scheme violated the First Amendment because it was not narrowly tailored to serve a compelling interest and because there were less restrictive alternative means of preventing minors from viewing adult content.[21] This conclusion turned largely on the trial court's findings that (1) there is no available technology that would permit a noncommercial website to verify the age or identity of its users, and (2) localized filtering and content-blocking software is a less restrictive and more effective means of keeping minors off of adult websites. Ultimately, the Court concluded that mandatory age verification would have a chilling effect on constitutionally protected Internet speech because (1) some adults may not have the necessary identifying credentials (e.g., credit cards), and (2) even those who have the necessary identifying credentials would be unwilling to provide them out of fear of identity theft or other misuse of the personal information.[22]

Congress's second attempt to shield minors from online pornography was embodied in the Child Online Protection Act (COPA), 47 U.S.C. § 231, which, like the CDA, imposed criminal and civil penalties on websites that made online pornography available to minors. Although COPA was designed in part to address the faults that the Supreme Court found with the CDA, it contained an affirmative age verification defense that was virtually identical to the CDA provision struck down by the *Reno* Court.

Immediately after COPA became law, a consortium of plaintiffs challenged the COPA statute in a case now called *ACLU v. Gonzales*.[23] Based largely on the Supreme Court's holding in *Reno,* the district court preliminarily enjoined the government from enforcing the age verification scheme. In 2002, the Supreme Court affirmed that preliminary injunction and remanded the case for trial with instructions to the district court to update the factual record to reflect current technological developments, account for any changes in the legal landscape, and determine whether there are more effective and less restrictive means of preventing minors from viewing pornography than an across-the-board age verification requirement.[24] On March 22, 2007, the district court issued a lengthy opinion that examined the relevant technologies and again concluded that localized filtering and content-blocking software is a less restrictive and more effective means of keeping minors off adult websites than age verification.[25]

Less Restrictive Means

The *Reno* and *Gonzales* opinions establish that however attractive it may seem to require adult websites to institute age verification, the technology for them to do so does not exist. Age verification ultimately amounts to identity verification, and the online verification process simply verifies the age of the person associated with whatever form of identification is used; there is no way to ensure that the online user is actually the person associated with that form of identification. The problem is compounded when dealing with minors, for whom there is little accessible data in the first place.[26] Accordingly, blocking software (i.e., software that restricts access to certain websites or categories of websites on a given computer) is a more effective means of shielding minors from adult content online.

The *Reno* and *Gonzales* opinions also establish that blocking software is a less restrictive means of regulating child access to adult content because it applies at the point of consumption instead of the distribution level. The opinions note that requiring all users, including adults, to present identification before viewing adult content is likely to reduce the number of adults who would otherwise view this constitutionally protected form of expression.[27] Some adults will not have the required form of identification, and some who do will not be willing to provide it out of fear of identity theft or out of a preference to visit the sites anonymously. Blocking software, on the other hand, can be installed on a given computer that is likely to be used by minors without impairing the access of adults to certain sites; and, as such,

blocking software is a more effective and less restrictive form of regulation. Thus, mandating age verification violates the First Amendment.

These arguments apply with even greater force to mainstream social networking. Although much of the speech exchanged over social networking sites might be considered trivial, there is no doubt that, on average, these sites consist of higher value speech than pornography sites. In addition to serving as a primary means of online communication for many, social networking sites have become avenues to learn more about political candidates, social causes, music, and art.[28] To the extent that the public square has ever existed in American culture, it is fair to say that it exists on MySpace, Facebook, and their competitors. Imposing liability standards that would chill access to social networking would offend First Amendment principles at their core.

Although *Reno* and *Gonzales* struck age verification requirements in federal criminal statutes, the analysis from these cases applies with full force to attempts to impose civil tort liability for failure to institute age verification. It is well established that "the application of state rules of law in state courts in a manner alleged to restrict First Amendment freedoms constitutes 'state action' under the Fourteenth Amendment."[29]

Third Party Standing

Furthermore, social networking websites should have valid third party standing to invoke the First Amendment rights of their users to invalidate an age verification liability scheme directed at the websites themselves. First, it is well established that a third party may invoke the rights of an individual if the individual is unlikely to have an opportunity to uphold her rights directly. This principle is demonstrated in *Eisenstadt v. Baird*, where the Supreme Court sustained a doctor's challenge to an anticontraceptive law based on the rights of an unmarried individual denied access to contraceptives. The Court allowed the doctor to raise the defense because the law did not subject patients to prosecution and so "denied them a forum in which to assert their own rights." Second, third parties may invoke the rights of another where there is a close relationship between the third party and the individual whose rights the third party seeks to invoke. In *Craig v. Boren*, for instance, the Supreme Court held that a bartender was permitted to challenge a state drinking age law that discriminated against men on the basis of gender because the bartender suffered economic injury through the loss of customers.

Both of these principles of third party standing should apply to social networking sites. Given that the anticipated claim—tort liability for failure to institute age verification measures—would apply to the social networking site operator, and not its users, the site operator should have the right under the first example to assert its users' rights. And social networking companies should be able to invoke their users' rights under the second example because they are closely connected to their users' constitutionally protected activity. That is, like the bartender in *Craig,* social networking companies face a restriction on their own operations through state laws aimed at their users' activities.

State Enforcement

Enterprising plaintiffs' attorneys are not the only ones demanding that social networking companies be held liable for their users' conduct. Perhaps no issue garners greater bipartisan political support than child safety, a point that is evidenced by the fact that a coalition of attorneys general from forty-four states is demanding that social networking sites be required to institute age verification.[30]

The Connecticut legislature, for instance, is currently debating legislation that would require social networking sites to implement age and identity verification for all users accessing the sites from computers in Connecticut.[31] The Connecticut bill, which is championed by Connecticut Attorney General Richard Blumenthal, would prohibit owners or operators of social networking websites from allowing a minor to create or maintain online profiles without (1) first obtaining written consent from the minor's parent and (2) giving the parent access to the profile page at all times.[32] The bill would also require social networking sites to implement procedures to verify the accuracy of age and other personal information collected from users upon registration, although the bill offers no explanation of how such information would be verified. Companies failing to comply with the bill's age verification requirement would be subject to injunctions and statutory penalties under Connecticut's unfair trade practices act. What is more, Attorney General Blumenthal has publicly stated that ten to twenty other attorneys general are thinking of introducing similar legislation in their respective states.[33]

If enacted, however, the Connecticut bill and those like it are unlikely to survive legal challenge. First, the CDA's immunity provisions bar liability for all claims based on third party content, including those based on state statutes. The CDA's expansive language grants broad immunity limited only by specific statutory exceptions that exclude four categories of claims from its reach: (1) claims involving a "federal criminal statute," (2) "any law pertaining to intellectual property," (3) "any State law that is consistent with [the] section," and (4) claims under the "Electronic Communications Privacy Act."[34] Furthermore, as noted previously, § 230(e)(3) states that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[35] Courts have applied these provisions broadly to bar claims based on both state and federal statutes. As one court applying the CDA to bar claims based on a federal civil rights statute explained, "Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied. . . ."[36] Accordingly, the Connecticut bill, even if enacted, will be barred by the CDA.

The Connecticut bill would also be vulnerable to a First Amendment challenge much like the one successfully launched by the ACLU against the age verification provisions of the CDA and COPA statutes. As explained above, the Supreme Court has held that requiring adult websites to verify the age of their users violates intermediate scrutiny under the First Amendment because there are more effective and less restrictive means of protecting minors from adult content. Those arguments apply with greater force to social networking websites, which provide a higher value medium for speech than do porn sites.

Aside from the legal challenges facing mandatory age verification, commentators are beginning to question whether

age verification is even a desirable solution to this complicated social problem.[37] Indeed even if online age verification were technologically feasible, it is unlikely to ever be foolproof. Instituting it on a broad scale may give parents and minors a false sense of security, or, worse, the burden of administering the age verification system could force mainstream social networking sites offshore, where meaningful regulation would become virtually impossible.[38]

Conclusion

There is no denying that society has an obligation to protect its children from sexual predators, wherever they operate. The problems related to online sexual predators, however, are complicated. Although it may seem attractive to place the burden to stop these heinous crimes on social networking sites that inadvertently enable them, imposing such a liability scheme would chill Internet speech and could ultimately have the unintended consequence of forcing mainstream websites overseas.

Notwithstanding these realities, however, social networking websites and lawyers who represent them should be prepared to face private lawsuits and legislation seeking to hold them liable for what their users say and do. As outlined in this article, well-established statutory, common law, and constitutional principles should shield websites from such liability and hopefully encourage lawmakers to focus on more productive law enforcement and education based solutions to the problem of online sexual predators.

Endnotes

1. Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007).
2. *See* Doe II v. MySpace, Inc., No. SC092421 (L.A. Super. Ct. filed Jan 17, 2007); Doe III v. MySpace, Inc., No. SC092423 (L.A. Super. Ct. filed Jan 17, 2007); Doe IV v. MySpace, Inc., No. SC092424 (L.A. Super. Ct. filed Jan 17, 2007); Doe V v. MySpace, Inc., No. SC092422 (L.A. Super. Ct. filed Jan 17, 2007).
3. John O'Brien, *Blumenthal Wants More MySpace Regulations*, LEGALNEWSLINE.COM, Mar. 12, 2007, www.legalnewsline.com/news/contentview.asp?c?191808; Jennifer Medina, *States Ponder Laws to Keep Web Predators from Children*, N.Y. TIMES, May 6, 2007, at 29.
4. 42 U.S.C. § 230(b)(1).
5. *See* Dimeo v. Max, 433 F. Supp. 2d 523, 528 (E.D. Pa. 2006) ("The provision 'precludes courts from entertaining claims that would place a computer service provider in a publisher's role,' and therefore bars 'lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content.'") (quoting Green v. Am. Online, Inc., 318 F.3d 465, 471 (3d Cir. 2003); Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997)).
6. 42 U.S.C. § 230(c)(1).
7. 42 U.S.C. § 230(e)(3).
8. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 712–16 (Ct. App. 2002).; Michelangelo Delfino v. Agilent Techs., 145 Cal. App. 4th 790, 804–05 (Ct. App. 2006).
9. *See, e.g.,* Batzel v. Smith, 333 F.3d 1018, 1034 (9th Cir. 2003); Ben Ezra, Weinstein, & Co., Inc. v. AOL, Inc., 206 F.3d 980, 986 (10th Cir. 2000); Blumenthal v. Drudge, 992 F.Supp. 44, 53 (D.D.C. 1998).
10. Zeran v. AOL, Inc., 129 F.3d 327, 334 (4th Cir. 1997).
11. *Id.* at 330, 333.
12. *See* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 536 (D. Md. 2006) (noting that "courts have extended the reach of the CDA to immunize ISPs from liability in several settings besides defamation suits").
13. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).
14. *Id.*
15. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007) ("Plaintiffs argue this suit is based on MySpace's negligent failure to take reasonable safety measures to keep young children off of its site and not based on MySpace's editorial acts. The Court, however, finds this artful pleading to be disingenuous.").
16. 42 U.S.C. § 230(e)(3).
17. Walker v. Harris, 924 S.W.2d 375, 377 (Tex. 1996).
18. Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).
19. *Id.* at 661.
20. *See* 47 U.S.C. § 223(e)(5)(B).
21. Reno v. ACLU, 521 U.S. 844 (1997).
22. *Id.* at 855–57.
23. ACLU v. Gonzales, No. 98–5591, 2007 WL 861120 (E.D. Pa. Mar. 22, 2007).
24. Ashcroft v. ACLU, 542 U.S. 656 (2004).
25. *Gonzales,* 2007 WL 861120, at *34–40.
26. *See* Lisa Lerer, *Why MySpace Doesn't Card,* FORBES.COM, Jan. 25, 2007, www.forbes.com/security /2007/01/25/myspace-security-identity-tech-security-cx_ll_0124myspaceage.html.
27. *See Gonzales,* 2007 WL 861120, at *36; *Reno,* 521 U.S. at 856–57 & n.23.
28. *See, e.g.,* Jenny Lee, *MySpace Generation Getting to Know Presidential Hopefuls Online,* QUADCITIES ONLINE, Apr. 30, 2007, http://qconline.com/archives/qco/display.php?id ? 336280; Chris DeWolfe, *The MySpace Generation: How a Project of Feed Burritos to the Hungry in L.A. Spread All the Way to Damascus,* FORBES.COM, www.forbes.com/free_forbes/2007/0507/072.html.
29. Cohen v. Cowles Media Co., 501 U.S. 663, 668 (1991).
30. John O'Brien, *Blumenthal Wants More MySpace Regulations,* LEGALNEWSLINE.COM, Mar. 12, 2007, www.legalnewsline.com/news/contentview.asp?c?191808.
31. H.B. 6981, 2007 Leg., Reg. Sess. (Conn. 2007).
32. *Id.*
33. O'Brien, *supra* note 3 (noting that Attorney General Blumenthal "told the Associated Press that 10–20 other attorneys general are thinking of introducing similar legislation in their respective states").
34. 42 U.S.C. § 230(e)(1)–(4).
35. *Id.* § 230(e)(3).
36. Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 539 (E.D. Va. 2003) (quoting TRW, Inc. v. Andrews, 534 U.S. 19, 28 (2001)).
37. *See* Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,* PROGRESS ON POINT 3 (Mar. 2007), www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf.
38. *Id.*