Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Backpage Dismissal Does Not Solve Websites' Woes

By **Ariel Neuman and Julian Burns, Bird Marella Boxer Wolpert Nessim Drooks Lincenberg & Rhow PC**


Ariel A. Neuman

Law360, New York (December 21, 2016, 2:11 PM EST) -- A California court's recent dismissal of criminal charges against the CEO and former owners of online classifieds site Backpage.com reaffirmed a broad view of website operators' immunity from liability for content posted by third parties. But while the court's ruling bolsters the weight of precedent favoring expansive immunity under Section 230 of the Communications Decency Act, an existing "exception" stripping website owners of immunity when they "materially contribute" to the illegality of posted content ensures that innovative plaintiffs lawyers and state prosecutors will continue to advance novel theories of website operator liability. Further clarity on the scope of Section 230 immunity is imperative.

Section 230 of the Communications Decency Act


Julian C. Burns

Section 230 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."[1] While Section 230 does not "impair" enforcement of federal criminal law, it explicitly preempts inconsistent state and local laws and enforcement actions.

Section 230 resolved a key question in the dawning age of the internet: whether internet service providers became liable for third-party content by exercising "editorial discretion" over third-party content. Before the CDA, courts gave conflicting answers.[2] But when a New York state court found Prodigy liable for defamatory statements posted to a Prodigy-owned forum — holding that Prodigy acted as a "publisher" by moderating content, reviewing as many postings as possible, and flagging posts containing offensive language — Congress leapt to action and Section 230 was born.

Congress intended Section 230 to facilitate a vibrant and open internet by protecting website operators from liability for failing to adequately monitor every word posted to their site by users. Consistent with this legislative intent, courts have generally construed Section 230 immunity expansively, emphasizing that close cases should be resolved in favor of immunity. In the majority of cases, website operators have been allowed to solicit user answers via drop-down menus, text boxes,[3] and customer rating systems,[4] and they remain immune from liability based on failure to flag and remove offensive or illegal content.[5]

A "Narrow Exception" Leaves Room for Creative Lawyering?

A 2008 decision allowing a suit against online roommate matchmaking service Roommates.com set forth a "narrow" exception that has become a favorite loophole for plaintiffs and prosecutors. In Roommates, a local fair housing organization sued Roommates for violating the federal Fair Housing Act's prohibition on rental advertisements that indicate a preference for tenants based on protected categories such as race, gender or sexual orientation.[6] Because Roommates required users to populate a field in each category when registering for the site, plaintiffs alleged Roommates' website design violated the Fair Housing Act.

The court agreed. The "website [was] designed to force subscribers to divulge protected characteristics and discriminatory preferences, and to match those who have rooms with those who are looking for rooms based on criteria that appear to be prohibited by the FHA."[7] Roommates' required fields were discriminatory, regardless of what a user inputted; it was not only the user who discriminated, but Roommates. Cautioning that its ruling was a limited "exception" to the rule of immunity, the Roommates court held that a website owner was not immune when it "helps to develop unlawful content" by "materially [contributing] to the alleged illegality of the conduct."[8] "Close cases," the court instructed, "must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites."[9]

Though the Ninth Circuit was explicit that its opinion was not an invitation for "clever" attorneys to argue that "something the website operator did encouraged the illegality,"[10] plaintiffs lawyers and prosecutors have taken it as an invitation to do exactly that. Courts generally have rejected these efforts to chip away at Section 230 immunity. But a few have entertained such claims, inviting attacks by those who would repeal the CDA's broad grant of immunity and leaving operators vulnerable to costly litigation and unjust prosecutions.

People v. Ferrer: The Most Recent Attack on Section 230 Immunity

California State Attorney General Kamala Harris led the most recent attack on Section 230 immunity, starting with a splashy and headline-grabbing public arrest of Backpage's CEO and two of the site's former owners. In People v. Ferrer et al., Attorney General Harris and Texas Attorney General Ken Paxton charged the Backpage defendants with pimping, attempted pimping, and conspiracy, alleging that they knew their site was rife with illegal advertising and intentionally exploited this illegal market for profit.[11]

The charges were harshly criticized by journalists and First Amendment activists, who noted that Attorney General Harris herself admitted that Section 230 immunized Backpage's conduct by signing a letter from 47 state attorneys general asking Congress to strip online classifieds sites of immunity. And Backpage had just defeated civil claims alleging that it deliberately structured its website to facilitate sex trafficking — an allegation that, like the allegations in Ferrer, invoked the Roommates exception.[12]

Defendants moved to dismiss the charges, arguing their conduct was immune under Section 230. They argued that the attorney general sought to hold them liable for third-party ads promoting prostitution, advancing precisely the sort of publisher liability theory that the CDA was intended to negate. The attorney general countered that Backpage was a content creator; it "helped develop content" by telling advertisers what they could not say, and it "spoke" by repackaging Backpage classifieds and posted them on a mobile app and affiliate site, exercising "editorial discretion" by cropping images, removing references to illegal services, and characterizing ads as "seeking men" or "seeking women."

Judge Michael G. Bowman of the California Superior Court agreed with the defendants that this was merely an attempt to "plead around Section 230," reaffirming a broad view of CDA immunity. Backpage did not "create" content by reformatting it or extracting snippets for reposting. Instead, Backpage was merely republishing the same content to generate more views. And because Backpage did not require users to submit illegal information, it did not fit into the narrow Roommates exception. All charges were dismissed.

Fuzzy Boundaries Lead to Uncertain and Arbitrary Results

Judge Bowman's survey of Section 230 case law highlights just how fuzzy the bounds of CDA immunity really are. What does it mean to "contribute materially to the alleged illegality of the conduct"?[13] Must the website force subscribers to divulge protected information, as in Roommates?[14] Or is it enough that the website provides content guidelines that may allegedly "help" advertisers provide thinly-veiled advertisements for illegal transactions? Or is the standard something else entirely?

As Roommates warned, a "clever lawyer" can always come up with "something the website

operator did [to] encourage[] the illegality" in order to hail the operator into court as a "speaker" rather than publisher. Roommates itself provided unclear and potentially conflicting answers to the question of when its "narrow exception" applies; the court alternately said that website operators lose Section 230 immunity when they are "directly involved in" the illegal activity; when they "materially contribute" to the illegality of the challenged content; or when they "elicit" information on the basis of protected characteristics.[15] But these terms are vague and leave open the very danger of which the Roommates court warned. While Ferrer reaffirms that website operators cannot be liable for third-party content so long as they merely "publish," lawyers who dislike the content of a website continue to allege that the operator is somehow the "speaker."

Occasionally these allegations succeed, at least at the pleading stage. In J.S. v. Village Voice Media Holdings LLC, the Washington Supreme Court affirmed the denial of a motion to dismiss a civil case filed on behalf of three minors whose traffickers advertised them on Backpage.com.[16] The plaintiffs alleged that Backpage's content rules — which prohibit certain terms and advertisements for illegal activity — were "adopted and intended to assist pimps in using ambiguous language to avoid police attention." This, plaintiffs argued, meant that Backpage "helped develop the content" of illegal advertisements and became a content creator for purposes of Section 230 immunity. Despite the allegations' similarity to those at issue in Ferrer, the J.S. court reached the opposite conclusion: the allegations, if true, suggested the site did more than simply maintain neutral policies prohibiting or limiting certain content, and crossed into "speaker" territory.

While J.S. is still pending, the ruling highlights the conundrum website operators face when trying to oust illegal activity from their sites. Posting content guidelines, prohibiting obviously illegal conduct, and monitoring the ads on a site bolsters an argument that the operator is helping criminals "avoid police detection." But failure to do so is just as risky: by allowing unfiltered posting of advertisements for illegal activity, the operator may be accused of facilitating criminal conduct. What should a website operator do if it tries to run a "clean" website by posting guidelines and prohibiting certain content, but suspects that some users engaged in criminal conduct may nonetheless sneak through? Shut the whole thing down? The CDA was meant to encourage this type of filtering and monitoring, not discourage it.

The mere decision by California to file the Ferrer case demonstrates that the law is not clear enough to protect website operators from prosecution. Despite her very public prior concession that the law immunizes sites like Backpage, the attorney general gambled on the possibility that a slight deviation from previously immunized conduct — the reposting of edited ads — might turn Backpage into a "speaker." The potential to garner headlines and praise for attacking human trafficking during an election cycle by taking advantage of the fuzzy bounds of Section 230 immunity apparently proved too tempting to resist. The defendants were forced to face the scandal of criminal indictment, the fear of imprisonment, and the expense of counsel despite being immune from prosecution under the CDA. Not all operators have Backpage's resources, and a smaller site could well be driven out of business by an aggressive prosecutor.

Criminal statutes are not meant to be used in this "gotcha" fashion. A website operator should be able to determine whether its conduct constitutes speech or publication without guessing whether it might face civil or criminal prosecution.

Where Do We Go From Here?

The Roommates exception is an important one: It allows prosecutors to go after websites whose operators are truly engaged in illegal activity. In the case of Rentboy.com, founder Jeffrey Hurant pleaded guilty to money laundering conspiracy charges based on allegations that his site — which contained programmed fields asking male escorts to advertise their penis size, favorite sexual positions and fetishes — was clearly built to facilitate prostitution.[17] In People v. Bollaert, the defendant designed two "revenge porn" websites to extract blackmail payments from victims in exchange for removing their intimate images and personal identifying information. Because the defendant required users to submit third-party personal identifying information in violation of privacy laws, he was not entitled to immunity under Section 230.[18]

But further clarity on the boundaries of Section 230 immunity is needed. As is often observed, the law cannot keep up with the rapid pace of technological development, particularly on the internet.

Section 230's drafters could not have contemplated its application to the complex and sophisticated social media networks that exist today.

Congress is unlikely to revisit the issue, leaving it to courts to refine their standards. Is the real rule that an operator is only liable for illegality inherent in its platform design a la Roommate? Is it fair to say that by explicitly excluding certain language from ads constitutes facilitation of advertisers' efforts to evade law enforcement scrutiny? Can a site provide content guidelines and terms of use without fear that those guidelines will be used as evidence that the operator "materially contributes" to the illegality of hosted content? Website operators need clarity on these questions.

The CDA was intended to allow website operators to run their businesses without fear that users' conduct would result in their own criminal or civil liability — a laudable and important goal as technology continues to develop. Yet despite the CDA's clear intent and the strength of judicial decisions upholding Section 230 immunity, victims of tragedies continue to look to website operators for a remedy. Just this week, the families of victims of the Pulse nightclub shooting in Orlando sued Google Inc., Facebook Inc. and Twitter Inc. for allegedly providing "material support" to international terrorism by allowing ISIS to have accounts from which it spread propaganda.[19]

Courts should clarify Roommates' boundaries to specify that immunity applies unless the website requires or specifically invites illegal activity; otherwise, it is the illegal actors themselves that should be prosecuted, not the websites whose platforms they exploit. Unless a site is built for illegal activity, the fact that users engage in such activity in part through their postings to the site should not be enough to eviscerate Section 230 immunity. Efforts to "plead around" Section 230 immunity — even if made with the best intentions — should be rejected at every turn.

Ariel A. Neuman is a principal at Bird Marella Boxer Wolpert Nessim Drooks Lincenberg & Rhow PC in Los Angeles and a former federal prosecutor. Julian C. Burns is an associate at the firm.

[1] 47 U.S.C. § 230(c)(1) (emphasis added).

[2] Compare Cubby, Inc. v. CompuServe, Inc., 776 F.Supp. 135 (S.D.N.Y. 1991) and Stratton Oakmont, Inc. v Prodigy Services Co. 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

[3] Carafano v. Metrosplash.com Inc., 339 F.3d 1119 (9th Cir. 2003).

[4] Gentry v. eBay, Inc., 99 Cal.App.4th 816, 121 Cal.Rptr.2d 703 (2002).

[5] See Carafano, supra note 3; Gentry, supra note 4; see also Zeran v. America Online, 129 F.3d 327, 328-29 (4th Cir. 1997).

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

[7] Id. at 1172 (emphasis added).

[8] Id. at 1174.

[9] Id. at 1175 (emphasis added).

[10] Id. at 1174 (emphasis original).

[11] See People v. Ferrer, et al., No. 16FE019224 (Sup. Ct., Sacramento Cnty 2016).

[12] See Doe v. Backpage, 104 F.Supp.3d 149 (D. Mass. 2015), aff'd 817 F.3d 12 (1st Cir. 2016).

[13] See Roommates.com, supra note 6, at 1174.

[14] See id. at 1172; see also People v. Bollaert, 248 Cal.App.4th 699 (2016) (holding that CDA immunity did not apply under Roommates where owner of revenge porn website required users to provide the personal identifying information of third parties when uploading photographs, then used the personal information to extort victims).

[15] See Roommates, supra note 14, at 1168-70.

[16] 184 Wash.2d 95 (2015).

[17] United States v. Easy Rent Systems, Inc. d/b/a Rentboy.com, et al., No 16-cr-00045 (E.D.N.Y. Jan. 27, 2016).

[18] See Bollaert, supra note 15, at 720-22.

[19] Crosby, et al. v. Twitter, Inc., et al., No. 16-cv-14406-CML-DRG (E.D. Mich. Dec. 19, 2016), ECF No. 1 (Dec. 19, 2016).
