Washington Journal of Law, Technology & Arts

Volume 11 | Issue 2 Article 4

8-1-2015

Paying for Nude Celebrities: Testing the Outer Limits of *Roommates.com*, *Accusearch*, and Section 230 Immunity

Christian Kaiser

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 11, ISSUE 2 SUMMER 2015

PAYING FOR NUDE CELEBRITIES: TESTING THE OUTER LIMITS OF *ROOMMATES.COM*, *ACCUSEARCH*, AND SECTION 230 IMMUNITY

Christian Kaiser

Cite as: 11 Wash. J.L. Tech. & Arts 125 (2015)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1478

ABSTRACT

The Internet is a powerful tool that promotes commerce, free thought, and free speech. It is these exact values that Congress sought to solidify when it passed Section 230 of the Communications Decency Act. The Internet also has a dark side, which is filled with obscenities, pornography, and illegal activity. In order to protect positive values and activities on the Internet, Congress decided to incentivize websites to police the content posted by their users. This was done by providing broad immunity from lawsuits based on content posted by third parties. But this immunity is not absolute. In the Fair Housing Council of San Fernando Valley v. Roommates.com *the court held that a website is a developer of the allegedly illegal content, and thus not immune, when it materially contributes to the alleged illegality of such content. Under* Roommates.com*, a website "materially contributes" if it forces its users to provide the allegedly illegal content. The* F.T.C. v. Accusearch *decision represents a different approach to the material contribution standard created in* Roommates.com*, but nevertheless affirms the broad immunity created by Section 230. Finally, the progeny cases of* Roommates.com *and* Accusearch *provide examples and reasons why Section 230 is so broad. This Article applies the above-mentioned cases to a hypothetical where a website receives payment to promote stolen celebrity photos on its website. This*

application concludes that the facetious website is not liable under the current law, regardless of the fact that its actions are morally suspect.

TABLE OF CONTENTS

I. INTRODUCTION

The Internet is a powerful tool that enables businesses to reach customers all over the world and empowers people to speak out against their government. However, it would be a mistake to view the Internet through rose-colored glasses, for there are many dark, disturbing, and illegal activities it supports. This Article analyzes the immunity created under Section 230 of the Communications Decency Act.[1] Two recent and contentious cases[2] are used to analyze a hypothetical constructed in light of recent changes in social media and an event concerning popular culture.[3] This section introduces the hypothetical, sections II, III and IV discuss Section 230, the *Roommates.com* and *Accusearch* decisions, section V discusses the progeny cases, and section VI applies all the cases to the facts of the hypothetical.

The hypothetical is as follows: A social networking website called "Squawker" has recently decided to accept payment from users in exchange for promoting their "squawks"[4] to all other users of the website. An anonymous user ("Anon") of a popular imageboard site[5] called "3Chan" pays Squawker to promote his squawks. Anon explains that he will be squawking pictures that he found on the Internet. These pictures consist of nude celebrities and were stolen from various iCloud accounts owned by said

[1] 47 U.S.C. § 230 (2006).

[2] F.T.C. v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

[3] This hypothetical is based on an article in Venture Beat and the hacked celebrity photos posted to 4Chan and Reddit. *See* Kia Kokalitcheva, *Twitter will soon start to show you tweets from folks you don't follow*, VENTURE BEAT NEWS (Oct. 16, 2014, 5:48 PM), http://venturebeat.com/2014/10/16/twitter-will-soon-start-to-show-you-tweet-from-folks-you-dont-follow/.

[4] A "squawk" can be analogized to a tweet used on Twitter, where users have 140 characters to write whatever they feel like or post images. *See Character Counting*, TWITTER, https://dev.twitter.com/overview/api/counting-characters (last visited July 23, 2015).

[5] An imageboard site is an online forum that revolves around posting images with minimal associated text. An example of such a site would be 4Chan or Imgur. *See Imageboard*, WIKIPEDIA, http://en.wikipedia.org/wiki/Imageboard (last updated July 13, 2015).

celebrities.[6] While Anon did not steal the photos himself, he is obsessed with getting upvotes[7] and is convinced that these squawks will raise his notoriety in the Squawker community. Squawker believes that these photos will be incredibly popular and will draw greater amounts of traffic to its webpage, increasing its revenues from selling advertising.

Squawker's promotion of Anon's squawks goes viral. Millions of Squawker users see the photos on their accounts and re-squawk them amongst their friends. This also draws millions of new users to Squawker's webpage, increasing its revenues substantially. These photos are eventually squawked to the celebrity victims' official Squawker accounts. Squawker received multiple takedown orders from the celebrities' attorneys, but ignored them. The celebrities are now suing Squawker for millions of dollars. Additionally, many cable news pundits have expressed their disdain for Squawker's behavior, labeling it the "Pinhead of the Week."

Squawker's attorneys are confident that Squawker will be able to get this case dismissed. Should Squawker be liable?

---

[6] This massive hacking event took place in the summer of 2014 and is proverbially known as "The Fappening" or "Celebgate." *See* Barbara Defranco, *Hacked! Jennifer Lawrence Nude Photos Leaked, Plus 24 Other Naked Celeb Photo Scandals*, CELEBUZZ (Sept. 1, 2014), http://www.celebuzz.com/2014-09-01/hacked-jennifer-lawrence-nude-photos-leaked-plus-21-other-naked-celeb-photo-scandals/. It is also important to clarify that Anon did not obtain these photos in violation of 18 U.S.C.A. § 2511(1) (West 2008) (Interception and disclosure of wire, oral, or electronic communications).

[7] On imageboard sites such as Imgur or Reddit, users create an account in order to post content. If a user posts an image, for example, and other users like it, then they can give the poster an upvote equal to one "point." If a user has many popular posts, he will receive many upvotes and his profile will gain notoriety. The opposite is true if the content is unpopular and the user will receive downvotes, decreasing his notoriety. *See* Sergius49, *What Does it Really Mean to Upvote/Downvote a Post?*, REDDIT, http://www.reddit.com/r/TheoryOfReddit/comments/1lpws2/what_does_it_really_mean_to_upvotedownvote_a_post/ (last visited July 7, 2015).

II. SECTION 230 OF THE COMMUNICATIONS DECENCY ACT CREATES BROAD IMMUNITY FOR WEBSITES.

Federal courts generally agree that Section 230 of the Communications Decency Act provides interactive computer services, such as websites, broad immunity from various types of civil lawsuits.[8] State courts also recognize this consensus where "all but a handful . . . find that the website is entitled to immunity from liability."[9] This consensus is consistent with the text of Section 230, which clearly bars plaintiffs from bringing civil suits against websites and other online service providers when the suit is based on content provided by a third party.[10]

Congress passed Section 230 to achieve two main goals. First, it wanted to encourage free speech and promote e-commerce on the Internet without burdensome involvement from the government.[11] Imposing tort liability on the "new and burgeoning Internet medium" was seen "simply as another form of intrusive government regulation of speech."[12] In various statutory findings, Congress recognized that the Internet offered "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[13] Furthermore, websites "have flourished, to the benefit of all Americans" without the burden of governmental involvement.[14] Therefore, it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by

[8] *See, e.g.*, Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010) (citation omitted) ("The majority of federal circuits have interpreted [Section 230] to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."). *See also* 47 U.S.C. § 230(f)(2) (1998).

[9] Hill v. StubHub Inc., 727 S.E.2d 550, 558 (N.C. Ct. App. 2012).

[10] 47 U.S.C. § 230(c)(1) ("No provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."). However, Section 230 makes it clear that it does not place any limitation on the application of federal criminal statutes. § 230(e)(1).

[11] *See, e.g.*, Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003).

[12] Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

[13] 47 U.S.C. § 230(a)(3).

[14] *Id.* § 230(a)(4).

Federal or State regulation."[15]

Second, Congress wanted to encourage online service providers to "self-police" potentially harmful or offensive material on their services.[16] While one goal was to keep government regulation to a minimum in order for the Internet to flourish, another was "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[17] Using tort liability as the incentive for self-policing was not feasible because, at the time, "commercial online services had almost twelve million individual subscribers."[18] The cost and effort required to monitor and police content would likely lead to online service providers greatly restricting what was posted on their sites. Essentially, Congress decided that the speech and commerce interests outweighed the threat of potentially injurious content.[19] Ultimately, "plaintiffs may hold liable the person who creates or develops unlawful content, but not the interactive computer service provider who merely enables that content to be posted online."[20]

III. SECTION 230 IMMUNITY IS BROAD, BUT NOT ABSOLUTE.

Section 230 does not extend immunity to a person or entity that creates or develops content "in whole or in part."[21] In most cases, the user is the person or entity that either creates or develops the content; the online service provider merely provides the platform. However, in the *Fair Housing Council of San Fernando Valley v. Roommates.com*, the court found that a website host can create or

[15] *Id.* § 230(b)(5).

[16] *Batzel*, 333 F.3d at 1028. *See also* 47 U.S.C. § 230(c)(2)(a).

[17] 47 U.S.C. § 230(b)(5). *But see* Reno v. ACLU, 521 U.S. 844 (1997) (The Supreme Court struck down the parts of the Communications Decency Act that regulated "indecent" content because it infringed upon the First Amendment. Section 230 is now the only piece of the Communications Decency Act left standing and we are left with a sort of free-floating statute granting expansive immunity to websites.).

[18] Reno v. ACLU, 521 U.S. 844, 850 (1997).

[19] Zeran v. America Online, Inc, 129 F.3d 327, 331 (4th Cir. 1997).

[20] Nemet Chevrolet, Ltd. v. Consumersaffairs.com, Inc., 591 F.3d 250, 254 (4th Cir. 2009).

[21] *See* 47 U.S.C. § 230(f)(3).

develop content in conjunction with the user when it materially contributes to the alleged illegality of the content[22] by *forcing* the user to provide such content.[23] This is known as the "material contribution" test.

Roommates.com is a website designed to match people renting out spare rooms with people searching for a place to live.[24] At the time of the case, in order to use the website, prospective subscribers were required to create a profile.[25] This process required them to give information—such as name, location and email.[26] However, Roommates.com also *required* subscribers to disclose their gender, sexual orientation and whether they would bring children into the household.[27] Additionally, subscribers had to disclose their preference in roommates with respect to the previously listed categories.[28] Finally, the site also encouraged subscribers to provide "Additional Comments" describing themselves and their desired roommate.[29] Roommates.com was sued by the Fair Housing Counsel of the San Fernando Valley, alleging the business violated the Fair Housing Act by asking users for this information.[30]

The decision in *Roommates.com* "turned entirely on the website's decision to *force* subscribers to divulge the protected characteristics and discriminatory preferences as a condition of using its services."[31] Therefore, by forcing the subscribers to provide this content, Roommates.com materially contributed to its illegality by acting as a co-developer. Limiting the holding further, the court held that merely encouraging or inducing a user to post

---

[22] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1168 (9th Cir. 2008).

[23] *Id.* at 1175.

[24] *Id.* at 1161.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.* at 1162.

[31] Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1198-99 (N.D. Cal. 2009). *See also* Atl. Recording Corp. v. Project Playlist, Inc., 603 F. Supp. 2d 690, 701 (S.D.N.Y. 2009) (finding *Roommates.com* "readily distinguishable" because it "was based solely on the fact that the content on the website that was discriminatory was supplied by Roommates.com itself").

illegal information or content is not enough to establish liability:

> [T]here will always be close cases where a clever lawyer could argue that *something* the website operator did encouraged the illegality. Such close cases, we believe, 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, fighting off claims that they promoted or encouraged—or at least tacitly assented—to the illegality of third parties. Where it is very clear that the website directly participates in developing the alleged illegality—as it is clear here with respect to Roommate's questions, answers and the resulting profile pages—immunity will be lost. But in cases of enhancement by implication or development by inference—such as with respect to the "Additional Comments" here—section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.[32]

The dissent in *Roommates.com* argues that this decision is inconsistent with at least five other circuits.[33] However, *Roommates.com* can be read consistently with the five circuits cited by the dissent.[34] In *Chic. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, the Seventh Circuit found Craigslist immune under Section 230 because "nothing in the service Craigslist offers induces anyone to post any particular listing or express a preference for discrimination."[35] In *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, the First Circuit held that a message board owner was not liable because "there is not even a colorable argument that any misinformation was prompted by Lycos's registration process or its link structure."[36] In *Green v. America Online (AOL)*, there was no allegation that AOL actually

[32] *Roommates.com*, 521 F.3d at 1174.
[33] *Id.* at 1177.
[34] *Id.* at 1179-80.
[35] 519 F.3d 666, 671-72 (7th Cir. 2008).
[36] 478 F.3d 413, 420 (1st Cir. 2007).

solicited the content; rather, the plaintiff claimed AOL's user terms waived 230 immunity by stating the company would attempt to remove offensive content.[37] In *Ben Ezra, Weinstein, and Co. v. America Online, Inc.*, the Tenth Circuit held AOL immune from relaying inaccurate stock price information because "Plaintiff could not identify any evidence indicating Defendant developed or created the stock quotation information."[38] Finally, in *Zeran v. America Online, Inc.*, the Fourth Circuit held AOL immune for another defamatory message board posting because it merely provided the platform for such a post to occur and had no actual involvement in the post.[39]

The *Roommates.com* decision can be summed up as follows: *Roommates.com* creates the "material contribution" test, which is met when, and only when, a website *forces* users to provide the allegedly illegal content. A website is not liable if it merely *encourages* the user to post the allegedly illegal content, otherwise the protections of Section 230 would be eroded. Other courts agree that liability was found solely because the website required users to input the illegal content.[40] Therefore, the reader should not be distracted by the confusing language or examples that appear throughout the *Roommates.com* decision.[41]

IV. *F.T.C. V. ACCUSEARCH INC.*, WHILE LACKING IN ANALYSIS, AFFIRMS THE BROAD IMMUNITY AND LIMITED EXCEPTION TO SECTION 230 EXPOUNDED IN *ROOMMATES.COM*.

In *F.T.C. v. Accusearch Inc.*,[42] the Tenth Circuit, through sparse analysis, also instituted a high bar for the plaintiffs. In this case, Abika.com, which was run by Accusearch Inc., sold various

[37] 318 F.3d 465, 471 (3d Cir. 2003).

[38] 206 F.3d 980, 985 (10th Cir. 2000).

[39] *See* Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

[40] Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1198-99 (N.D. Cal. 2009); Doe v. MySpace, Inc., 629 F. Supp. 2d 663, 665 (E.D. Tex. 2009); Atl. Recording Corp. v. Project Playlist., 603 F. Supp. 2d 690, 701 (S.D.N.Y. 2009).

[41] *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1172 (9th Cir. 2008) (describing what amounts to development/materiality). *See also id.* at 1169 (offering an example of materiality that is somewhat different than those given elsewhere in the case).

[42] F.T.C. v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009).

data, including phone records.[43] The website stated that its customers could acquire "details of incoming or outgoing calls from any phone number, prepaid calling card or Internet Phone," and that "Phone searches are available for every country in the world."[44] The court found that acquisition of this information "would almost inevitably require someone to violate the Telecommunications Act or to circumvent it by fraud or theft."[45] Essentially, Accusearch was "paying researchers to acquire telephone records, knowing that the confidentiality of the records was protected by law . . . ."[46] The Tenth Circuit held that Accusearch was liable because it fell within the exception to Section 230.[47]

The court in *Accusearch* correctly identifies the standard used by the Ninth Circuit in *Roommates.com*. "It summarized: 'A website helps to develop unlawful content, and thus falls within the exception to Section 230, if it contributes materially to the alleged illegality of the conduct.'"[48] Other circuits have also identified this as the standard.[49] However, the Ninth Circuit clearly explained how that standard was met: "The message to website operators is clear: If you don't . . . design your website to require users to input illegal content, you will be immune."[50]

The *Accusearch* opinion essentially ignores the *Roommates.com* force requirement and simply applies the "material contribution" test. The court concluded Accusearch materially contributed to the illegality because it paid researchers to acquire telephone records.[51] "Accusearch solicited requests for confidential information protected by law . . . . Accusearch's actions were not 'neutral' with respect to generating offensive

[43] *Id.* at 1190.
[44] *Id.* at 1191.
[45] *Id.* at 1192.
[46] *Id.* at 1200.
[47] *Id.*
[48] *Id.* at 1200 (quoting Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1168 (9th Cir. 2008)).
[49] Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 412 (6th Cir. 2014).
[50] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008).
[51] *Accusearch*, 570 F.3d at 1200.

content; on the contrary, its actions were intended to generate such content."[52] That is the end of the analysis; the facts of the case meet the test. While this analysis is less than sufficient, it still affirms the high bar for plaintiffs created by Section 230. In order to rely on *Accusearch*, plaintiffs would need to show that their facts are substantially similar, which would be very difficult. Accusearch did not require the users to do anything. Rather, it was the one who created the illegal content by employing people to break the law. Therefore, unless potential plaintiffs can show that the website in their case is also generating illegal content on its own, they will not be able to show that Section 230 immunity is inapplicable.

Accusearch applies the "material contribution" test created in *Roommates.com*, but declines to accept its force requirement. Accusearch was found to have materially contributed to the alleged illegality because it was the source of the illegal content; it was the developer.

V. THE PROGENY OF *ROOMMATES.COM* AND *ACCUSEARCH* DEMONSTRATE THE BREADTH OF SECTION 230 IMMUNITY.

While both *Roommates.com* and *Accusearch* are seminal cases in the discussion of Section 230 immunity, a brief discussion of other cases is necessary to fully comprehend the current state of the law.

A. A Website Is Still Immune Even If It Receives a Takedown Notice for the Illegal Content.

In *Zeran v. America Online, Inc.*, the Fourth Circuit concluded that subjecting websites to notice liability would defeat the purposes of Section 230.[53]

> If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party,

[52] *Id.* at 1201.
[53] 129 F.3d 327, 333 (4th Cir. 1997).

> concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.[54]

Furthermore, requiring websites to respond to takedown notices, and face potential liability should the content be illegal, is ludicrous considering the sheer amount of current Internet users.[55] Additionally, while the number of takedown notices varies from website-to-website, the number of notices received by certain websites is increasing rapidly. For example, in 2014 Reddit received a mere 218 takedown notices,[56] whereas, in 2012, Google and Twitter received 441,370 and 6,646 takedown notices respectively.[57] For Google, this was an increase of 711,887 percent

[54] *Id; cf.* Auvil v. CBS 60 Minutes, 800 F. Supp. 928, 931 (E.D. Wash. 1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot discretionary calls").

[55] As of 2014, the number of Internet users worldwide was 2.92 billion. *Number of worldwide internet users from 2000 to 2015 (in millions)*, STATISTA (Apr. 18, 2015, 1:42 PM), http://www.statista.com/statistics/273018/number-of-internet-users-worldwide.

[56] *Reddit transparency report, 2014*, REDDIT (Jul. 16, 2015, 10:00 AM), http://www.reddit.com/wiki/transparency/2014.

[57] Ernesto Van der Sar, *Google Takedown Notices Surge 711,887 Percent in Four Years*, TORRENTFREAK (Mar. 25, 2014), https://torrentfreak.com/google-takedown-notices-surge-140325.

in just four years.[58] Analyzing and responding to nearly half a million takedown notices would be a monumental task for even a company as large as Google and would significantly change the functionality and environment of the Internet. Specifically, companies would necessarily devote substantial time to responding to takedown notices, inevitably causing a decline in content quality. Moreover, the disparity in the quantity of takedown notices between websites makes it impossible to implement a one-size-fits-all solution of imposing liability.

B. The Fact That the Business Is Motivated By Profit Is Irrelevant To Whether Section 230 Immunity Applies.

Even if the complained-of actions by the website are designed to increase its revenues, the profit motive is not enough to defeat Section 230 immunity.[59] "[T]he fact that a website elicits online content for profits is immaterial; the only relevant inquiry is whether the interactive service provider 'creates' or 'develops' that content."[60]

C. Section 230 Immunity Still Applies When an Owner of a Website Knows the Third-Party Content Is Legally Questionable Absent a Takedown Notice.

Similar to notice, a website owner's own knowledge that the content is illegal does not preclude Section 230 immunity.[61]

---

[58] *Id*.

[59] *See, e.g.*, Hill v. StubHub, Inc., 727 S.E.2d 550, 560 (N.C. Ct. App. 2012).

[60] *Id.* (quoting Goddard v. Google, Inc., No. C 08-2738 JF, 2008 WL 5245490, at *3 (D. Cal. Dec. 17, 2008)).

[61] *See, e.g.*, Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 421 n.3 (1st Cir. 2007).

VI. ANALYZING THE HYPOTHETICAL UNDER *ROOMMATES.COM*, *ACCUSEARCH*, AND THE CASE LAW IN SECTION IV, MAKES IT CLEAR SQUAWKER WILL NOT BE LIABLE.

As a refresher, the hypothetical involves Squawker—a website—and Anon—a user. Anon took advantage of Squawker's paid promotions program and paid it to advertise nude celebrity photos which he obtained online. Those celebrities are now suing Squawker but will decidedly fail because Squawker is immune under Section 230. Squawker did not require Anon to submit such content (or any content) as a condition of using its service, nor did it illegally obtain the celebrity photos from the iCloud accounts.

Roommates.com makes it clear that a website is not protected by Section 230 when it materially contributes to the alleged illegality of the content by requiring users to provide illegal content. Squawker offered to promote Anon's nude celebrity photos in exchange for a fee. It did not require or compel Anon to provide illegal content as a condition for using its services. Furthermore, Anon could have posted the photos on his Squawker profile even without paying. Therefore, it is clear that Squawker will not be liable under the *Roommates.com* analysis.

Under the *Accusearch* analysis, Squawker will also be immune. Accusearch was liable because it was the developer of the illegal content. Arguably, if Squawker had hacked the celebrity iCloud accounts and posted the pictures, then its actions would be analogous to Accusearch's. Since that is not what happened, Squawker will continue to enjoy Section 230 immunity.

Finally, although Squawker received a takedown notice, is making money off the photos, and knew the photos were likely obtained illegally, it will likely remain immune from all civil claims brought by the celebrities under Section 230.

CONCLUSION

Congress intended Section 230 to promote free speech and commerce on the Internet, while simultaneously encouraging self-policing of illegal and vulgar content.[62] Essentially all courts agree

[62] Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).

that the immunity established by Section 230 is broad.[63] However, as *Roommates.com* and *Accusearch* have shown, that immunity is not absolute. Under *Roommates.*com, a website will be found liable if it requires a user to submit allegedly illegal content. Under *Accusearch*, a website is not immune when it is found to be the developer of the content. Furthermore, the progeny cases demonstrate that Section 230 immunity remains incredibly broad. Therefore, regardless of the degree of depravity, websites like Squawker will continue to enjoy the protections of Section 230.

PRACTICE POINTERS

- To avoid any chance of falling outside the immunity provided by Section 230, make sure your client is neither:
  1. forcing its users to provide potentially illegal content; nor
  2. committing a crime to obtain content for its webpage.

- Attorneys who do not want their lawsuit against a website dismissed because of Section 230 have few options. One option is to bring a promissory estoppel claim against the website.[64]

- Attorneys defending websites should focus on the case law cited within the Article and emphasize the breadth of Section 230 and its virtual unanimity across the country.

[63] *See, e.g.*, Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010) (citation omitted) ("The majority of federal circuits have interpreted [Section 230] to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.").

[64] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1108 (9th Cir. 2009) (holding that § 230(c)(1) does not preclude causes of action based on the theory of promissory estoppel).