Proskauer

Ninth Circuit Releases Another Important CDA Section 230 Opinion With Broad Application – Automated Content Recommendation and Notification Tools Do Not Make Social Site the Developer of User Posts

New Media and Technology Law Blog on **August 28, 2019**

In the swirl of scrutiny surrounding the big Silicon Valley tech companies and with some in Congress declaiming that Section 230 of the Communications Decency Act (CDA) should be curtailed, 2019 has quietly been an important year for CDA jurisprudence with a number of opinions enunciating robust immunity under CDA Section 230. In particular, there has been a trio of noteworthy circuit court-level opinions rejecting plaintiffs' attempt to make an "end run" around the CDA based on the assertion that online service providers lose immunity if they algorithmically recommend or recast content in another form to other users of the site.

- In *Herrick*, the Second Circuit found that the CDA barred claims that sought to ascribe liability to a mobile dating service for the design of its platform, finding it within the purview of protected "traditional editorial functions."
- In *Marshall's Lockmsith*, the D.C. Circuit affirmed dismissal of claims brought by multiple locksmith companies against the operators of the major search engines for allegedly publishing the content of fraudulent locksmiths' websites and translating street-address and area-code information on those websites into map pinpoints that were displayed in response to user search requests.
- In the *Force* case, the Second Circuit found that claims related to supplying a communication forum and failing to completely block or eliminate hateful terrorist content necessarily treated the platform as the publisher of such content and were therefore barred under the CDA.

This week, in a case with an unsettling fact pattern, the Ninth Circuit made it a quartet – ruling that a now-shuttered social networking site was immune from liability under the CDA for connecting a user with a dealer who sold him narcotics that culminated in an overdose. The court found such immunity because the site's functions, which included content recommendations and notifications to members of discussion groups, were "content-neutral tools" used to facilitate communications. (*Dyroff v. The Ultimate Software Group, Inc.*, No. 18-15175 (9th Cir. Aug. 20, 2019)).

On social media and other sites that process user postings, automated processes are an integral part of how content is displayed, shared or organized, and as such, the current decision is significant in firmly placing such automated site functions within the ambit of CDA immunity.

In the *Ultimate Software* case, the site in question, Experience Project, was a now-defunct social networking website made up of various online communities or groups where users anonymously shared their experiences and posted and answered questions with other users about different topics. Experience Project allowed users to register with anonymous user names and thereafter join or start groups based on their interests, without limitation, ranging from the inoffensive "I Like Dogs" to the more nefarious "I Love Heroin." The defendant, using advanced data-mining algorithms, analyzed the posts and other user data to, among other things, steer users to other groups on its website through its proprietary recommendation functionality and transmit alerts about posts to members within groups, some of which were dedicated to narcotics and facilitated illegal drug sales.

The plaintiff Kristanalea Dyroff ("Plaintiff") sued Ultimate Software after her son died from an overdose from heroin he allegedly bought from a drug dealer he met online through their respective posts on the Experience Project. (Incidentally, the drug dealer was ultimately arrested and prosecuted.) Plaintiff claimed that defendant Ultimate Software operated Experience Project in an unlawful manner that facilitated extensive drug trafficking and that its mining of data from users' posts to make recommendations steered the plaintiff's son toward heroin-related discussion groups. She advanced negligence and other related tort claims, including a separate failure to warn claim. Defendant countered that the CDA barred most of the claims, as the site was an interactive computer service and plaintiff was attempting to treat the defendant as a publisher of third-party content.

In November 2017 the district court dismissed the action, finding, in pertinent part, that the defendant's "[content]-neutral tools" facilitated communication but did not create or develop the postings in question. In a succinct opinion, the Ninth Circuit affirmed the dismissal. The appeals court held that the recommendation and notification functions of the defendant's site helped facilitate user-to-user communication, but it did not materially contribute, as Plaintiff argued, to the alleged unlawfulness of the content. The court noted that plaintiff failed to plead that Ultimate Software required users to post specific content, made suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts.

> "It is true that Ultimate Software used features and functions, including algorithms, to analyze user posts on Experience Project and recommended other user groups. This includes the heroin-related discussion group to which Greer posted.... Plaintiff, however, cannot plead around Section 230 immunity by framing these website features as content. By recommending user groups and sending email notifications, Ultimate Software, through its Experience Project website, was acting as a publisher of others' content."

In a separate portion of the opinion, the appeals court also found that the defendant, as site owner, did not owe a duty to the plaintiff's son because the site's features "amounted to content-neutral functions that did not create a risk of harm."

The *Ultimate Software* case is a reminder of the scope of CDA immunity and that many of its applications result in somewhat controversial outcomes – indeed, the case is reminiscent of the recent *Seaver* decision, where a district court had found that the CDA shielded the organization responsible for maintaining the Tor Browser from various claims stemming from an incident where a minor died after taking illegal narcotics purchased from a site on the "dark web."

While *Ultimate Software* and *Seaver* address very unfortunate factual situations, the decisions do represent the principle that an online service provider, in fashioning its various offerings (particularly social elements or outside content aggregation functions) can rely on the CDA for legal immunity from claims stemming from most automated manipulations of hosted third party content as long as the provider stays within the parameters of the statute.

View Original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner