Snapchat Case May Offer Opening For Design Defect Plaintiffs

By James Rotondo and Andrew Ammirati, Day Pitney LLP

Since the Communications Decency Act[i] was enacted in 1996, almost all courts have construed the statute broadly to provide immunity to internet platforms for third-party content.[ii]

In *Lemmon v. Snap Inc.*,[iii] however, the U.S. Court of Appeals for the Ninth Circuit recently reversed the district court's dismissal of an action against Snap. The court held that the CDA did not grant Snap immunity for a design defect claim relating to the Snapchat application itself.

Snapchat allows users to take photos or videos — commonly called snaps — with their smartphones, and share them with other Snapchat users. *Lemmon* concluded that the harm was not caused by the publication of a snap sent by another user, but instead by the design's encouragement of reckless conduct by the original user.

Although *Lemmon* is in the minority of cases that have not applied CDA immunity to design claims against internet platforms, it does not represent a radical departure from earlier decisions construing the CDA — and certainly does not represent a wholesale rejection of the broad immunity under the CDA suggested by U.S. Supreme Court Justice Clarence Thomas in Malwarebytes Inc. v. Enigma Software Group USA LLC.[iv]

In his comments regarding the denial of certiorari in Malwarebytes, Justice Thomas suggested that the lower courts had allowed the policy and purpose of the CDA to expand the immunity extended to internet companies far beyond what the language of the statute permits.

But *Lemmon* reflects careful analyses of whether a claim seeks to treat the defendant as a publisher, and what constitutes third-party content under the CDA — and may suggest that courts may be more restrictive in the future in granting immunity for so-called neutral tools.

CDA Immunity Generally

The CDA 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,"[v] in essence shielding internet companies from liability for the publication of a third party's content.

The CDA also provides direct immunity from certain civil liability, namely, for (1) good faith acts to restrict access to or remove certain types of objectionable content; or (2) acts taken to give consumers tools to filter the same types of content.[vi]

Courts determining the scope of this immunity have developed a three-part analysis to determine whether CDA immunity applies, analyzing whether: (1) the defendant is a provider or

user of an interactive computer service; (2) the claim is based on information provided by another information content provider; and (3) the claim would treat the defendant as the publisher or speaker of that information.[vii]

Lemmon v. Snap

In *Lemmon*, three boys between the ages of 17 and 20 died after their car ran off the road, crashed into a tree and burst into flames. Before the day of the accident, one or more of the boys had downloaded Snapchat to their mobile phones.

Snapchat rewards users with trophies, streaks and social recognitions based on the snaps they send. Snapchat also enables users to superimpose a filter over a photos or video at the moment they take it. The Speed Filter enables users to document their speed, and many users suspect that they will be rewarded for recording a 100 miles per hour or faster snap using the filter.[viii]

Shortly before the crash, the car began accelerating to a speed significantly above the speed limit, and one snap captured the vehicle's speed at 123 mph. Police investigators estimated the speed of the vehicle to be 113 mph when it ran off the road.[ix]

The boys' parents brought a negligent design lawsuit against Snap, alleging that the company knew or should have known that users believed a reward system existed, and that the filter was incentivizing users to drive at dangerous speeds. The U.S. District Court for the Central District of California dismissed the action in 2020 for failure to state a claim on the basis of CDA immunity.

In reaching its decision, the district court concluded that "the Speed Filter is a neutral tool, which can be utilized for both proper and improper purposes."[x] On appeal, the Ninth Circuit held that Snap did not enjoy immunity from suit under the CDA and reversed, because the plaintiffs' claim did not treat Snap as a publisher or speaker, and did not rely on "information provided by another information content provider."[xi]

In reaching its conclusion, the court did not focus solely on the Speed Filter, but instead on how the Speed Filter and the "incentive system then supposedly worked in tandem to entice young Snapchat users to drive at speeds exceeding 100 MPH."[xii] In essence, the plaintiffs sought to hold Snap liable for its duties as a product manufacturer — duties fully independent from the duties Snap might have as a publisher in relation to editing, monitoring or removing third-party content.

Although the rejection of the publisher and "content of another" arguments resolved the CDA immunity issue against Snap, the Ninth Circuit also proceeded to consider and reject the argument that Snap should be protected from liability for the use of content-neutral tools, stating that its case law had never suggested that:

internet companies enjoy absolute immunity from all claims related to their content-neutral tools. ... Those who use the internet thus continue to face the prospect of liability, even for their "neutral tools," so long as plaintiffs' claims do not blame them for the content that third parties generate with those tools.[xiii]

Lemmon in Context

Lemmon is among the minority of cases that have rejected applying CDA immunity to a claim of design defect.[xiv] Most of the cases considering design defect claims against internet companies have held that those claims are barred, on the theory that the alleged defect resulted in a third-party communication that caused the harm, and the CDA protects internet companies from liability for third-party content.[xv]

Three years before *Lemmon*, in 2018, the Georgia Court of Appeals reached the same conclusion in a case involving almost identical facts — with the key difference being that the operator of the speeding vehicle had not yet posted her speed on Snapchat. In *Maynard v. Snapchat*,[xvi] the plaintiff was injured when her vehicle was struck by another vehicle traveling 113 mph.

In rejecting the argument that Snap should be held immune, the court noted that the plaintiffs — the injured driver and her husband, who was pursuing a loss of consortium claim — had not alleged that the operator had "uploaded or posted a snap using the Speed Filter before the accident occurred."[xvii] *Maynard* emphasized that the plaintiffs did not seek to hold Snap liable for publishing a snap by a third party.

Instead, the plaintiffs sought to hold Snap liable for its own conduct — specifically, creating the Speed Filter and failing to warn users that the filter could encourage speeding and unsafe driving practices. Accordingly, the court held that "CDA immunity does not apply because there was no third-party user content published."[xviii]

Lemmon and *Maynard* fit squarely within existing CDA jurisprudence. In the Ninth Circuit's seminal 2008 decision, *Fair Housing Council of San Fernando Valley v. Roommates.com LLC*,[xix] the court held that the CDA provided no immunity for content that a website itself had developed by virtue of the way that it had designed the website — but that it did apply to the use of neutral tools that allowed users to provide appropriate or inappropriate content.

In *Roommates*, the defendant operated a website designed to match people renting out spare rooms with people looking for a place to live. Before subscribers could search listings or post housing opportunities on Roommates' website, they needed to create profiles, a process that required answering a series of questions about gender, family status and sexual orientation — categories that were prohibited by the federal Fair Housing Act[xx] and California housing discrimination laws.

The Ninth Circuit concluded that by illegally requiring subscribers to provide information about gender, family status and sexual orientation by selecting choices available on a drop-down menu as a condition of accessing its service, Roommates became the developer of that information.[xxi] Roommates was therefore not entitled to immunity, because the CDA only provides immunity when a plaintiff's claim faults the defendant for information provided by third parties, and the claim against Roommates implicated content it developed itself.

Conversely, the Ninth Circuit held that the CDA shielded Roommates from liability for discriminatory comments that users made in the "additional comments" section of the profile pages. That section appeared at the end of the registration process as a blank text box.

Roommates encouraged subscribers to personalize their profiles, but did not provide any specific guidance as to what subscribers should say, and did not urge subscribers to express discriminatory preferences. Predictably enough, some subscribers indicated discriminatory preferences, such as "[prefer] white Male roommates," "[t]he person applying for the room MUST be a BLACK GAY MALE," and "NOT looking for black muslims."

The court viewed the additional comments box as a neutral tool through which the users could express their own views and preferences, which were protected third-party content.[xxii] Courts repeatedly have relied on the neutral tools analysis in *Roommates* to shield internet companies from liability for illegal third-party content on websites that was not compelled by the website.[xxiii]

In its 2019 decision in *Dyroff v. Ultimate Software Group Inc.*,[xxiv] for example, the Ninth Circuit extended CDA immunity to a website that had facilitated the illegal purchase of drugs, rejecting the argument that the design of the website took it outside the scope of immunity. *Dyroff* concerned a social networking website where users anonymously shared their experiences, posted and answered questions, and interacted with other users about different topics.

The site did not limit or promote the experiences that users shared. The site used certain algorithms to analyze user posts and recommended other user groups, including a heroin-related discussion group. In response to a post in the heroin-related group seeking information about where to "score heroin in jacksonville, fl" the site sent that user an email notification when another user, an Orlando-based drug dealer, posted in the same group.

The two users then connected off the site for a heroin purchase, and the first user died the next day from fentanyl toxicity.[xxv] The Ninth Circuit concluded that the defendant was acting as a publisher of others' content by recommending user groups and sending notifications. In short, the algorithm-driven recommendations and posts were neutral tools "meant to facilitate the communication and content of others. They are not content in and of themselves."[xxvi]

Conclusion

Lemmon is consistent with prior CDA jurisprudence, but it does leave an opening for expanded liability in the future. If the facts permit, plaintiffs may be able to avoid CDA immunity by focusing on how the website's design affected the user, rather than how the user's content affected a third party.

Similarly, *Lemmon*'s rejection of the concept of absolute immunity from all claims related to content-neutral tools may result in a closer examination of the potential for liability arising from the role of algorithms in the creation of recommendations and posts. In addition, plaintiffs bringing other traditional tort claims may find the reasoning of *Lemmon* to be supportive of their claims.[xxvii]

---

[i] 47 U.S.C. § 230.

[ii] See, e.g., *Herrick v. Grindr LLC*, 765 F. App'x 586, 589 (2d Cir.), cert. denied, 140 S. Ct. 221 (2019); *Almeida v. Amazon.com Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006).

[iii] *Lemmon v. Snap Inc.*, No. 20-55295, 2021 WL 1743576 (9th Cir. May 4, 2021).

[iv] *Malwarebytes Inc. v. Enigma Software Group USA LLC*, 141 S. Ct. 13, 15 (2020).

[v] 47 U.S.C. § 230(c)(1).

[vi] 47 U.S.C. § 230(c)(2).

[vii] *FTC v. LeadClick Media LLC*, 838 F.3d 158, 173 (2d Cir. 2016).

[viii] *Lemmon v. Snap Inc.*, 440 F. Supp. 3d 1103, 1105 (C.D. Cal. 2020), rev'd and remanded, No. 20-55295, 2021 WL 1743576 (9th Cir. May 4, 2021).

[ix] Id. at 1106.

[x] Id. at 1111.

[xi] Lemmon, 2021 WL 1743576, at *2.

[xii] Id. at *4.

[xiii] Id. at *6.

[xiv] See e.g., *Fair Housing Council of San Fernando Valley v. Roommates.com LLC*, 521 F.3d 1157, 1161–62 (9th Cir. 2008) (website that requires answers to discriminatory housing questions not immune under CDA); *J.S. v. Village Voice Media Holdings LLC*, 184 Wash. 2d 95 (2015) (Backpage website promoted sex trafficking).

[xv] E.g., *Herrick v. Grindr LLC*, 765 F. App'x 586 (2d Cir.) (design defects allowed ex-boyfriend to create fake Grindr profile, leading to harassment), cert. denied, 140 S. Ct. 221 (2019); *Dyroff v. Ultimate Software Group Inc.*, 934 F.3d 1093, 1094–95 (9th Cir. 2019) (design defect facilitated illegal purchase of drugs, resulting in death by fentanyl toxicity), cert. denied, 140 S. Ct. 2761 (2020); *Jane Doe No. 1 v. Backpage.com LLC*, 817 F.3d 12 (1st Cir. 2016) (design defects encouraged sex trafficking); *Daniel v. Armslist LLC*, 386 Wis. 2d 449 (design features allowed husband to acquire a gun illegally and murder his wife and two other people, and injure four others), cert. denied, 140 S. Ct. 562 (2019); *Stokinger v. Armslist LLC*, No. 1884CV03236F, 2020 WL 2617168 (Mass. Super. Ct. April 28, 2020) (website design feature facilitated an illegal firearm sale, which resulted in the shooting of a police officer). "In response to Backpage.com, LLC, Congress enacted Public Law 115-164, titled 'Allow States and Victims to Fight Online Sex Trafficking Act of 2017' (the '2018 Amendment'), to clarify that the CDA 'was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution ....'" Stokinger, 2020 WL 2617168, at *5 (citations omitted).

[xvi] *Maynard v. Snapchat*, 346 Ga. App. 131 (2018).

[xvii] Id. at 132.

[xviii] Id. at 136.

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

[xx] 42 U.S.C. § 3601 et seq.

[xxi] 521 F.3d at 1164–66.

[xxii] Id. at 1169, 1173–75.

[xxiii] See supra note 15 (collected cases).

[xxiv] *Dyroff v. Ultimate Software Group Inc.*, 934 F.3d 1093 (9th Cir. 2019), cert. denied, 140 S. Ct. 2761 (2020),

[xxv] Id. at 1095.

[xxvi] Id. at 1097–99.

[xxvii] See, e.g., *Bolger v. Amazon.com LLC*, 267 Cal. Rptr. 3d 601, 605 (2020) (strict liability claims against Amazon not barred when they depend on Amazon's own activities, and not its status as a speaker or publisher of content provided by third party for its product listing), review denied (Nov. 18, 2020); *Airbnb Inc. v. City of Boston*, 386 F. Supp. 3d 113, 120 (D. Mass. 2019) (penalties imposed by municipality on Airbnb by virtue of its roles in booking rental agreements and collecting and distributing payments, not for publications), appeal dismissed, No. 19-1561, 2019 WL 6522166 (1st Cir. Sept. 3, 2019); *Doe v. Internet Brands*, 824 F.3d 846 (9th Cir. 2016) (failure to warn claim not barred by CDA where plaintiff alleged that website had actual knowledge that individuals had used the website as part of a scheme to lure women to fake modeling auditions and rape them).

***

James Rotondo is a partner and Andrew Ammirati is an associate in Day Pitney's Hartford, CT office.

This article was first published in Law 360 on May 28, 2021.