United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued October 12, 2018 Decided June 7, 2019

No. 18-7018

MARSHALL'S LOCKSMITH SERVICE INC., ET AL.,
APPELLANTS

v.

GOOGLE, LLC, ET AL.,
APPELLEES

Appeal from the United States District Court
for the District of Columbia
(No. 1:16-cv-02360)

Barry Roberts argued the cause and filed the briefs for appellants.

Kathleen E. McCarthy argued the cause for appellees. With her on the brief were *Taylor T. Lankford*, *Amy W. Ray*, *Kelsi Brown Corkran*, *Benjamin Aiken*, *Joseph R. Palmore*, and *Jeff A. Jaeckel*.

Before: GARLAND, *Chief Judge*, MILLETT, *Circuit Judge*, and EDWARDS, *Senior Circuit Judge*.

Opinion for the Court filed by *Chief Judge* GARLAND.

GARLAND, *Chief Judge*: Fourteen locksmith companies allege that Google, Microsoft, and Yahoo! have conspired to "flood the market" of online search results with information about so-called "scam" locksmiths, in order to extract additional advertising revenue. Am. Compl. ¶ 36. According to the amended complaint, the defendants further this scheme by publishing the content of scam locksmiths' websites, translating street-address and area-code information on those websites into map pinpoints, and allegedly publishing the defendants' own original content. The district court dismissed the amended complaint as barred by the Communications Decency Act, which states 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." 47 U.S.C. § 230(c)(1). We affirm.

I

"This case arises from a motion to dismiss, and so we accept as true the factual allegations in the [plaintiffs'] amended complaint." *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 5 (2010). The plaintiffs operate businesses that provide legitimate locksmith services.[1] They face competition from "scam" locksmiths who misrepresent their businesses in terms of "services offered, pricing, expertise, training, who is behind the website, their location, contact information, and whether

[1] The plaintiffs refer to themselves as "legitimate" locksmiths. Although they do not define the term, they appear to mean businesses that are resident, and registered and/or licensed, in the jurisdictions in which they advertise and operate. *See, e.g.*, Am. Compl. ¶¶ 36-38; Locksmiths' Reply Br. 9.

they are licensed or registered to do business." Am. Compl. ¶ 57.

According to the plaintiffs, the internet allows scam locksmiths to amplify their influence. Consumers typically call locksmiths when they are locked out of their homes or cars. In emergencies of this kind, consumers prioritize identifying the locksmith closest to where they are located. Today, the "primary means" that an inquiring consumer uses to find a nearby locksmith is "[l]ocation-based internet search." *Id.* ¶ 54.

Both the importance of proximity and the internet's potential to create the facade of proximity are not lost on scam locksmiths. These companies actively cultivate online presences that give the appearance of locality. Scam locksmiths "publish hundreds or thousands of unique websites targeting nearly every heavily populated geographic location all around the country." *Id.* ¶ 57. These pages "display either a fictitious or no address, and include false claims that [scam locksmiths] are local businesses." *Id.* ¶ 58. Moreover, scam locksmiths use call centers to generate "local-area phone number[s]," when in reality they may be located far away from the querying consumer. *Id.* ¶ 59. All of these efforts are designed to take advantage of the structure of the defendants' search engines. By so doing, the scam locksmiths have "tricked Google into displaying [scam locksmiths] as physical stores in [the consumers'] neighborhoods, when in reality, they're ghosts." *Id.* ¶ 61B (internal quotation marks omitted).

Legitimate locksmith businesses have suffered significant economic losses due to competition from scam locksmiths. *Id.* ¶¶ 42-43. Yet the plaintiffs focus their blame not on the scam locksmiths themselves, but rather on the search engines that Google, Microsoft, and Yahoo! operate. Collectively, these companies control approximately 90% of the online search

market. *Id.* ¶ 33. According to the plaintiffs, the defendants use their market power with respect to online search to extract payments from legitimate locksmith companies like themselves. The defendants do this by "deliberately flood[ing] their own organic and map results with locksmith listings they know are seriously inaccurate or even nonexistent to induce both legitimate and scam locksmiths to participate in paid [advertised] results to overcome the false information." *Id.* ¶ 66.

The amended complaint alleges that the defendants carry out this scheme by publishing three kinds of content that boost scam locksmith search results and generate advertising revenue. (As discussed below, the plaintiffs also contend that these kinds of content are unprotected by the Communications Decency Act.) First, the defendants publish "[t]hird-party websites created by scam locksmith[s] that Defendants know do not exist at the addresses stated thereon." *Id.* ¶ 63. Second, the defendants publish "[e]nhanced content that was derived from third-party content, but has been so augmented and altered as to have become new content." *Id.* ¶ 62. Finally, the defendants publish "original content, created out of whole cloth." *Id.* Taken together, the defendants' publication of these categories of content has "severely restricted" consumers' ability to "discover and contact Plaintiffs and other legitimate locksmiths." *Id.* ¶ 37.

In January 2017, the plaintiffs filed their amended complaint alleging eight violations of federal and state law. The three federal counts allege that the defendants engage in false advertising under the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), abuse their monopoly power under § 2 of the Sherman Act, 15 U.S.C. § 2, and conspire in restraint of trade under § 1 of the Sherman Act, *id.* § 1. The five state-law counts allege common-law fraud, tortious interference with economic advantage, unfair competition, conspiracy, and breach of contract.

The defendants moved to dismiss the amended complaint on several grounds. As relevant here, they argued that they are immune from suit under § 230 of the Communications Decency Act, 47 U.S.C. § 230, which protects online intermediaries from liability for third-party content posted on their websites.

The district court granted the motion to dismiss, holding that all counts other than the breach-of-contract count should be dismissed under § 230. *Baldino's Lock & Key Serv., Inc. v. Google, LLC*, 285 F. Supp. 3d 276, 278 (D.D.C. 2018). The court reasoned that "it is the scam locksmiths who provide the original location claim, and the [defendants] have created a website that simply re-publishes that information along with associated mapping information." *Id.* at 283. Any "extra information is wholly dependent on the original location claim." *Id.* The court dismissed the remaining breach-of-contract count for failure to state a claim. *Id.* at 284.

The plaintiffs timely appealed the district court's dismissal of the seven counts that the court held are barred by the Communications Decency Act. We review de novo the district court's grant of the motion to dismiss based on § 230. *Bennett v. Google, LLC*, 882 F.3d 1163, 1165 (D.C. Cir. 2018).

II

Section 230 of the Communications Decency Act is the statutory provision that controls this case. Section 230(c)(1) states: "No 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." 47 U.S.C. § 230(c)(1). Section 230(f)(3) goes on to define an "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer

service." *Id.* § 230(f)(3). As courts uniformly recognize, § 230 immunizes internet services for third-party content that they publish, including false statements, against causes of action of all kinds. *See, e.g.*, *Bennett*, 882 F.3d at 1166; *Klayman v. Zuckerberg*, 753 F.3d 1354, 1356 (D.C. Cir. 2014).[2]

Consistent with Congress' intent to confer broad immunity for the re-publication of third-party content, internet services may invoke § 230 immunity as grounds for dismissal under Federal Rule of Civil Procedure 12(b)(6). "Preemption under the Communications Decency Act is an affirmative defense, but it can still support a motion to dismiss if the statute's barrier to suit is evident from the face of the complaint." *Klayman*, 753 F.3d at 1357; *see Nemet Chevrolet, Ltd. v. Consumeraffairs.com,*

---

[2] *See also, e.g.*, *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016); *Jones v. Dirty World Entm't Recordings, LLC*, 755 F.3d 398, 406-07 (6th Cir. 2014); *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009); *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008); *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 418-19 (1st Cir. 2007); *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006).

Section 230 effectively confers immunity against federal causes of action where the claims involve treating the defendant as the "publisher or speaker." *See Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 n.4, 1102 (9th Cir. 2009), *as amended* (Sept. 28, 2009); *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (en banc). It also contains a preemption provision that expressly extends that immunity to "State or local law" claims "inconsistent with this section," 47 U.S.C. § 230(e)(3). Although the Act contains some exceptions, *see, e.g.*, *id.* § 230(e)(1) (exempting enforcement of federal criminal laws), the plaintiffs acknowledge that none of those exceptions applies to this case, 12/19/17 Hr'g Tr. 10 (J.A. 57); *see Baldino's Lock & Key Serv.*, 285 F. Supp. 3d at 283.

Inc., 591 F.3d 250, 254 (4th Cir. 2009) ("Section 230 immunity, like other forms of immunity, is generally accorded effect at the first logical point in the litigation process.").

To determine whether dismissal is appropriate, this circuit has adopted a three-pronged test that tracks the text of § 230(c)(1):

> The Communications Decency Act mandates dismissal if (i) [the defendant] is a "provider or user of an interactive computer service," (ii) the information for which [the plaintiff] seeks to hold [the defendant] liable was "information provided by another information content provider," and (iii) the complaint seeks to hold [the defendant] liable as the "publisher or speaker" of that information.

Klayman, 753 F.3d at 1357 (quoting 47 U.S.C. § 230(c)(1)); *accord Bennett*, 882 F.3d at 1166.

In this case, the parties contest only the second prong. *See* 12/19/17 Hr'g Tr. 8 (J.A. 55). The defendants satisfy the first prong because the Act broadly defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server . . . ." 47 U.S.C. § 230(f)(2). Search engines fall within this statutory definition. *See, e.g.*, *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016). And the defendants satisfy the third prong because the plaintiffs acknowledge that they seek to hold the defendants liable in their capacity as a "publisher or speaker" of the content at issue. *See* 12/19/17 Hr'g Tr. 8 (J.A. 55).[3]

---

[3] For example, Count I, for monopolization, faults the defendants for "listing large numbers of artificial listings in their organic results,"

The sole question on appeal, therefore, is whether the plaintiffs seek to hold the defendants liable for "information provided by another information content provider," as required by the second prong. 47 U.S.C. § 230(c)(1). If not, then the suit may proceed. If so, then all three prongs are satisfied, the defendants are entitled to immunity, and the court properly dismissed the plaintiffs' lawsuit.

III

At the motion-to-dismiss stage, we examine the "face of the complaint" to determine whether the plaintiffs seek to hold the defendants liable for information provided by another information content provider. *Klayman*, 753 F.3d at 1357. The following analysis addresses the three categories of content that the amended complaint alleges the defendants publish: (1) "third-party websites created by scam locksmith[s] that Defendants know do not exist at the addresses stated thereon," Am. Compl. ¶ 63; (2) "[e]nhanced content that was derived from third-party content, but has been so augmented and altered as to have become new content and not mere editorialization," *id.* ¶ 62; and (3) "original content, created out of whole cloth," *id*.

A

First, the plaintiffs allege that the defendants "publish third-party websites created by scam locksmith[s] that Defendants know do not exist at the addresses stated thereon." Am. Compl. ¶ 63. This category of content published by the defendants --

---

Am. Compl. ¶ 132; Count II, for conspiracy in restraint of trade, faults the defendants for "knowingly publishing fake listings," *id*. ¶ 140; and Count VII, for false advertising, alleges that the "published material at issue . . . misrepresents the geographic origin" of the services in question, *id*. ¶ 173 (internal quotation marks omitted).

the posting of third-party content -- is plainly within the immunity provided by § 230. Indeed, this claim is precisely the kind that Congress passed § 230 to foreclose. *See Bennett*, 882 F.3d at 1166, 1168 (citing *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997)).

The plaintiffs do not seriously contest this conclusion. Before the district court, plaintiffs' counsel conceded that "we don't like the phony websites, but if they got it from somebody else and simply republished it, the [Act] gives them immunity." 12/19/17 Hr'g Tr. 7 (J.A. 54); *see* Recording of Oral Arg. at 7:27-7:54. Nonetheless, the plaintiffs' amended complaint repeatedly suggests that the defendants should be held liable for publishing the content of scam-locksmith websites because they are "on actual notice" that this content is fraudulent and yet have failed to act. *See, e.g.*, Am. Compl. ¶¶ 39, 84, 124-28. But it is "well established that notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech." *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 420 (1st Cir. 2007); *see Bennett*, 882 F.3d at 1166 (noting that § 230 immunity applies regardless of whether the defendant acquired knowledge that the third-party content it published was false (citing *Zeran*, 129 F.3d at 331)). Hence, the amended complaint's allegations regarding the re-publication of content from the scam locksmiths' websites cannot escape the immunity that § 230 confers.

B

Next, the plaintiffs allege that the defendants create "[e]nhanced content that was derived from third-party content, but has been so augmented and altered as to have become new content and not mere editorialization." Am. Compl. ¶ 62. The primary form of "enhanced" content to which the plaintiffs

object is the defendants' creation of map pinpoints that display scam-locksmith locations.

The first question we must address is whether the defendants' translation of information that comes from the scam locksmiths' webpages -- in particular, exact street addresses -- into map pinpoints takes the defendants beyond the scope of § 230 immunity. In considering this question, it is helpful to begin with the simple scenario in which a search engine receives GPS data from a user's device and converts that information into a map pinpoint showing the user's geographic location. The decision to present this third-party data in a particular format -- a map -- does not constitute the "creation" or "development" of information for purposes of § 230(f)(3). The underlying information is entirely provided by the third party, and the choice of presentation does not itself convert the search engine into an information content provider. Indeed, were the display of this kind of information not immunized, nothing would be: every representation by a search engine of another party's information requires the translation of a digital transmission into textual or pictorial form. Although the plaintiffs resisted this conclusion in their briefs, *see* Locksmiths' Reply Br. 3 (declaring that the "location of the inquiring consumer . . . is determined entirely by the search engines"), they acknowledged at oral argument that a search engine has immunity if all it does is translate a user's geolocation into map form, *see* Recording of Oral Arg. at 12:07-12:10.

With this concession, it is difficult to draw any principled distinction between that translation and the translation of exact street addresses from scam-locksmith websites into map pinpoints. At oral argument, the plaintiffs could offer no distinction, and we see none. In both instances, data is collected from a third party and re-presented in a different format. At best, the plaintiffs suggested that a line could be drawn between

the placement of "good" and "bad" locksmith information onto the defendants' maps. *See id.* at 12:43-12:58 (accepting that, "to the extent that the search engine simply depicts the exact information they obtained from the good locksmith and the consumer on a map, that appears to be covered by the [Act]"). But that line is untenable because, as discussed above, Congress has immunized the re-publication of even false information.

The next question is whether the translation of somewhat less-exact location descriptions is protected by the Act. This requires somewhat more discussion. The plaintiffs describe a situation in which the defendants create a map pinpoint based on a scam locksmith's website that says the locksmith "provides service in the Washington, D.C. metropolitan area" and "lists a phone number with a '202' area code." Locksmiths' Br. 8; *see also* Locksmiths' Reply Br. 4-5. According to the plaintiffs, the defendants' search engines use this information to "arbitrarily" assign a map location within the geographic scope indicated by the third party. Locksmiths' Br. 8.

We conclude that these translations are also protected. First, as the plaintiffs do not dispute, the location of the map pinpoint is derived from scam-locksmith information: its location is constrained by the underlying third-party information.[4] In this sense, the defendants are publishing

---

[4] *See* Am. Compl. ¶ 61B ("These businesses . . . have tricked Google into displaying them as physical stores in their neighborhoods, when in reality, they're ghosts."); *id.* ¶ 103 ("Defendants' algorithms organize their organic results by factoring in the geographic proximity of each search result to the [querying] user, with the same geographically restrictive result as an outright map search."); *id.* ¶ 111 ("Defendants' algorithms organize, rank, categorize, correlate, and display results for organic, map, and paid results."); *see also* Recording of Oral Arg. at 14:30-14:55 (plaintiffs' counsel) ("Let's say

"information provided by another information content provider." *Cf. Kimzey v. Yelp!, Inc.*, 836 F.3d 1263, 1270 (9th Cir. 2016) (holding that Yelp's star rating system, which is based on receiving customer service ratings from third parties and "reduc[ing] this information into a single, aggregate metric" of one to five stars could not be "anything other than user-generated data"). It is true that the location algorithm is not completely constrained, but that is merely a consequence of a website design that portrays all search results pictorially, with the maximum precision possible from third-party content of varying precision. *Cf. Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1125 (9th Cir. 2003) ("Without standardized, easily encoded answers, [Matchmaker.com] might not be able to offer these services and certainly not to the same degree.").[5]

Second, and also key, the defendants' translation of third-party information into map pinpoints does not convert them into "information content providers" because defendants use a

---

the scammer represents that it provides service throughout the D.C. metropolitan area. The search engine will arbitrarily put a pinpoint, and often actually assign an arbitrary address, to the scammer somewhere in the D.C. area."); David Segal, *Fake Online Locksmiths May Be Out To Pick Your Pocket, Too*, N.Y. TIMES (Jan. 30, 2016) (referenced in Am. Compl. ¶ 61B) (explaining that scammers "game Google's algorithm" by inputting their misleading location information into two Google "platforms: Google My Business . . . and Map Maker").

[5] To be clear, we do not hold that § 230 protects all information derived from third-party information. Because the defendants' map pinpoints hew to the third-party information from which they are derived -- and because, as we discuss below, the pinpoints are derived neutrally as well as algorithmically -- today we need not decide precisely when an entity that derives information can be considered to have "creat[ed] or develop[ed]" it. 47 U.S.C. § 230(f)(3).

neutral algorithm to make that translation. We have previously held that "a website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online." *Klayman*, 753 F.3d at 1358; *accord Bennett*, 882 F.3d at 1167; *see Kimzey*, 836 F.3d at 1270 (holding that Yelp's "star-rating system is best characterized as the kind of neutral tool[] operating on voluntary inputs that . . . [does] not amount to content development or creation" (internal quotation marks omitted) (citing *Klayman*, 753 F.3d at 1358)). And the Sixth Circuit has held that the "automated editorial act[s]" of search engines are generally immunized under the Act. *O'Kroley v. Fastcase, Inc.*, 831 F.3d 352, 355 (6th Cir. 2016).

Here, the defendants use automated algorithms to convert third-party indicia of location into pictorial form. *See supra* note 4. Those algorithms are "neutral means" that do not distinguish between legitimate and scam locksmiths in the translation process. The plaintiffs' amended complaint effectively acknowledges that the defendants' algorithms operate in this fashion: it alleges that the words and numbers the scam locksmiths use to give the appearance of locality have "tricked Google" into placing the pinpoints in the geographic regions that the scam locksmiths desire. Am. Compl. ¶ 61B. To recognize that Google has been "tricked" is to acknowledge that its algorithm neutrally translates both legitimate and scam information in the same manner. Because the defendants employ a "neutral means" and an "automated editorial act" to convert third-party location and area-code information into map pinpoints, those pinpoints come within the protection of § 230.[6]

---

[6] The same is true of the streetscape photos and driving directions about which the plaintiffs also complain. *See* Am. Compl. ¶¶ 94, 173E. These are a function of the map pinpoints that the defendants' algorithms generate from the location information provided by the

C

Finally, the plaintiffs allege that the defendants publish "original content" devoid of any third-party origination at all. Am. Compl. ¶ 62. We have addressed some of this allegedly "original content" in the previous section. For example, the amended complaint frequently alleges that the defendants create "false" or "fictitious" addresses. *See, e.g.*, *id*. ¶¶ 64, 174. But those allegations refer to the map pinpoints that the search engines generate in neutral fashion based on third-party information like area codes, and we have already concluded that the pinpoints are covered by § 230 immunity.

Elsewhere in the amended complaint, the plaintiffs allege that the defendants go further. According to the plaintiffs, the defendants "manually alter their own algorithmic results to maximize profitability," untethered from either the information the locksmiths provide or the algorithms the defendants employ. *Id.* ¶ 116. But the plaintiffs do not discuss this allegation in their appellate briefs, and they have therefore forfeited it. *Williams v. Romarm, SA*, 756 F.3d 777, 783 (D.C. Cir. 2014); *see* FED. R. APP. P. 28(a)(8)(A).

Finally, the plaintiffs maintain that the defendants' algorithms place the same scam locksmith's map pinpoint in different locations, depending upon a consumer's location, in order to make that locksmith appear to be nearby. This allegation has the mirror-image problem of the allegation just discussed: it is made in the plaintiffs' briefs, *see, e.g.*, Locksmiths' Br. 18; Locksmiths' Reply Br. 5, but is not made in their amended complaint. It is therefore not relevant in reviewing the validity of the district court's dismissal of that

---

locksmiths' websites. *See Baldino's Lock & Key Serv.*, 285 F. Supp. 3d at 281.

complaint. *See Hurd v. District of Columbia*, 864 F.3d 671, 678 (D.C. Cir. 2017) ("In determining whether a complaint fails to state a claim, [the court] may consider only the facts alleged in the complaint, any documents either attached to or incorporated in the complaint and matters of which [the court] may take judicial notice." (internal quotation marks omitted)).

IV

We close by noting that, although we find § 230 immunity warranted in this case, that immunity is not limitless. In this vein, we reject the defendants' remarkable suggestion at oral argument that they would enjoy immunity even if they did in fact entirely fabricate locksmith addresses. *See* Recording of Oral Arg. at 37:27-38:20. That assertion is plainly inconsistent with the scope of the immunity that Congress has conferred. If the defendants were to fabricate addresses, those addresses would not be "information provided by another information content provider." 47 U.S.C. § 230(c)(1). And the defendants would not be entitled to immunity.

For the foregoing reasons, the district court's dismissal of the complaint as barred by § 230 of the Communications Decency Act is

Affirmed.