No. 21-1333

IN THE
Supreme Court of the United States

REYNALDO GONZALEZ, ET AL.,
Petitioners,

v.

GOOGLE LLC,
Respondent.

On Writ of Certiorari to the
U.S. Court of Appeals
for the Ninth Circuit

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF NEITHER PARTY

ALAN BUTLER
Counsel of Record
JOHN DAVISSON
MEGAN IORIO
THOMAS MCBRIEN
GRANT FERGUSSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

December 7, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1]

EPIC regularly participates as *amicus* in this Court and other courts in cases concerning privacy rights and harmful data practices. EPIC also regularly advocates for meaningful government oversight of abusive, exploitative, invasive, and discriminatory data collection systems and algorithms.

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

SUMMARY OF THE ARGUMENT

Section 230 began with a simple purpose: to ensure that internet companies could host and moderate user-generated content without being held liable for harmful information the users post. Over the decades, the provision has been contorted to grant internet companies unprecedented immunity from civil liability for their own harmful conduct. This Court now has the opportunity to bring Section 230 back to its original meaning.

We agree with Petitioners that "treated as the publisher or speaker" must be read in the context of the informational tort cases that led to Section 230's adoption. Under some informational tort theories of liability, information is not harmful, and thus not actionable, until it is published to a third party. Here, "published" means communicated, either orally or in writing. The original speaker of the harmful information is both the publisher and speaker and is liable for the informational tort. Others who participate in communicating the harmful information can also be held liable to varying degrees. Traditional media, such as newspapers, that print harmful information are "treated as the publisher or speaker" for liability purposes because the editorial control they exert enables them to discover the harmful nature of the information before they re-publish it. Thus, they are just as liable as the original speaker when they do re-publish harmful information. What it means to be "treated as the publisher or speaker," then, is to be liable for an informational tort to the same degree as the original speaker or publisher of the harmful information.

A simple test for when an interactive computer service is "treated as the publisher or speaker" of user-

provided information is to ask whether the claim can also be brought against the original speaker or publisher, whom Section 230 calls the "information content provider." In informational torts like defamation, the same claim can be brought against the original publisher of a tortious statement and any subsequent re-publishers. Section 230 bars this kind of claim. If a claim can be brought against the interactive computer service but cannot be brought against the information content provider, then it seeks to hold the service provider liable for their own harmful conduct, which is not akin to treating them as a publisher or speaker of the third-party information.

We believe that this one rule can resolve the dispute in this case as well as many other cases involving harmful online design and misuse of information. In some cases, it will be possible to bring a claim against both the interactive computer service and the information content provider. In such cases, the interactive computer service would have to make two additional showings for a successful Section 230 defense: one, that the claim requires proving that the interactive computer service published or spoke information; and two, that the interactive computer service was not itself a provider, creator, or developer of the information that led to the harm.

This Court's interpretation of Section 230 will have wide-ranging impacts on people's ability to obtain redress for harms caused by internet companies. Social media sites employ sophisticated algorithms that segment, target, and control users in often harmful ways. The allegations in this case—that Google matches ISIS content to users who are profiled to be most susceptible to the group's messaging—represent

one subset of these algorithmic harms. Many internet companies that deploy harmful products use Section 230 as a shield instead of making their products safer, exactly the opposite of what Section 230's drafters intended. Other companies collect and publish people's personal information without a care for the accuracy of the information or for individual privacy rights because they believe Section 230 protects them. Unless Section 230 is returned to its original meaning and courts are given a clear way to apply immunity, internet companies will continue to act with impunity—to all our detriment.

ARGUMENT

I. An interactive computer service is "treated as the publisher or speaker" when it is held liable for harmful information in the same way as the information content provider could be held liable.

In Section 230, "treat[ing]" an interactive computer service "as the publisher or speaker of any information provided by another information content provider" has a specific legal meaning: holding an interactive computer service as liable as its user for the harm the users' words cause. This meaning comes not from the ordinary use of the phrase but from its meaning under defamation law, where publishers and speakers face the same liability for communicating harmful information. Recognizing this, the Court should adopt a simple test for determining whether an interactive computer service qualifies for Section 230 immunity: an interactive computer service is "treated as the publisher or speaker of any information provided by another information content provider" when

the claim (1) could be brought directly against the information content provider; (2) requires proving that the interactive computer service published or spoke harmful information; and (3) does not allege that the interactive computer service provided, created, or developed the harmful information in whole or in part.

A. Congress enacted Section 230 to change the rule on defamation liability.

Congress enacted Section 230 in response to a defamation suit that held an interactive computer service provider liable as a publisher of defamatory material that a user posted to its service. See *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 14 (2020) (Thomas, J., statement respecting denial of certiorari) (discussing *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710, at *3–4 (N.Y. Sup. Ct. May 24, 1995)). Section 230 was meant to specifically limit the kind of publisher liability imposed in *Stratton Oakmont*. 141 Cong. Rec. H8469–70 (daily ed. Aug. 4, 1995) (statement of Rep. Christopher Cox); S. Rep. No. 104-230, at 194 (1996). When a "word is obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it." *Stokeling v. United States,* 139 S. Ct. 544, 551 (2019) (internal citation and quotation marks omitted). In *Stratton Oakmont* and the defamation context more generally, to "treat [an interactive computer service] as the publisher or speaker" means to hold the company liable for the same harm and to the same degree as the user that originally posted the harmful information. Thus, Section 230 only blocks claims that could be brought directly against the information content provider.

The question in *Stratton Oakmont* was whether an internet service, Prodigy, should be treated, for liability purposes, as a publisher or as a distributor of defamatory material posted to its service. *Stratton Oakmont*, 1995 WL 323710, at *3. The term "publisher" has a different meaning under defamation law than its ordinary meaning. Defamation requires "publication to a third party." Restatement (Second) of Torts § 558(b), at 155 (Am. L. Inst. 1965). To "publish" means to communicate words to someone other than the person defamed. Publish, Black's Law Dictionary (11th ed. 2019). Thus, the person who originally communicated the defamatory statement is both the speaker and the original publisher. Anyone who repeats or further communicates defamatory information is also liable for defamation. A "re-publisher" is "subject to liability as if he had originally published [the defamatory statement]," Restatement (Second) of Torts § 578 (Am. L. Inst. 1977), while a "distributor" who merely "delivers or transmits" defamatory information is liable "if, but only if, he knows or has reason to know of its defamatory character," *id.* § 581. Since a re-publisher and the original publisher were held liable to the same degree, the terms "re-publisher" and "publisher" have often been used synonymously under defamation law. The tort of false light also places a re-publisher in the same shoes as the original publisher when assigning liability. *See, e.g.*, *Flowers v. Carville*, 310 F.3d 1118, 1132 (9th Cir. 2002) (false light).

In determining whether to apply publisher or distributor liability to Prodigy, the *Stratton Oakmont* court referred to these traditional defamation terms and the different degrees of responsibility and liability that apply to each category of actors. The court noted that a "publisher" "is subject to liability as if he had

originally published [the libel]," while a "distributor" "will not be found liable in the absence of fault." *Id.* Publishers face greater liability than distributors because "[t]he choice of material to go into a newspaper and the decisions made as to the content of the paper constitute the exercise of editorial control and judgment and with this editorial control comes *increased liability*." *Id.* (internal citations omitted) (emphasis added). The court found that Prodigy should be treated as a publisher because, through its content-moderation practices, it "exercised sufficient editorial control over its computer bulletin boards to render it a publisher with the *same responsibilities as a newspaper*." *Id.* (emphasis added). This was in contrast to other internet companies, which should only be treated as distributors of the harmful information users provided because they were mere "passive conduit[s]". *Id.*

Fearing that the rule in *Stratton Oakmont* would discourage internet companies from moderating their services, Congress passed Section 230 to replace the common law defamation liability standard. 141 Cong. Rec. H8469–70 (daily ed. Aug. 4, 1995) (statement of Rep. Christopher Cox); S. Rep. No. 104-230, at 194 (1996). Under Section 230, interactive computer services are not to be treated as publishers or speakers of the information their users post. All that means is that the interactive computer service should not be put in the same shoes as an information content provider when assigning liability for harmful information the information content provider posted. Section 230 does not bar claims based on the interactive computer service's own harmful conduct just because that conduct was somehow tied to a user's harmful information.

B. An interactive computer service is not treated as the publisher or speaker of an information content provider's content if it faces a claim that the information content provider could not face.

A simple way to determine whether a claim puts an interactive computer service in the shoes of another information content provider is to ask whether the claim could be brought directly against the information content provider. Because the information content provider is the original publisher and speaker of the information, any claim that seeks to hold an interactive computer service liable for publishing or speaking information provided by an information content provider could also be brought directly against that information content provider. Claims that cannot be brought against the information content provider either seek to hold the interactive computer service liable to a lesser degree than the information content provider or seek to hold the company liable for its own harmful conduct.

Many cases implicating Section 230 can be resolved by applying this rule. For example, most products liability claims cannot be brought against the information content provider. Yet, courts have repeatedly granted Section 230 immunity for products liability claims merely because the publishing of third-party content was a fact along the causal chain that led to the harm. *See* Section II, *infra*.

The prevailing interpretations of Section 230 run into difficulty when an information content provider posts harmful information *and* the interactive computer service engages in additional harmful conduct. By looking at each claim and asking whether the

claim can be brought against the information content provider, the rule offered here helps separate the claims that are barred because they are based on the publishing or speaking of the harmful content and those claims that should not be barred because they target the interactive computer service's own harmful conduct. For example, in a case where an individual alleges that a third-party user has posted their private images on an online forum in violation of a state non-consensual intimate imagery law and has also requested that the online forum delete the offending post under a state privacy law, any claims brought by the individual against the online forum for violating the privacy law deletion right should not be barred because they target the company's own allegedly harmful conduct and could not be brought against the third-party user.

C. A claim that does not include publishing or speaking information as an element does not treat an interactive computer service as a publisher or speaker.

If a claim against an interactive computer service could also be brought against the information content provider, the next question is whether proof of the publication of harmful third-party content is a necessary element of the claim against the interactive computer service. In some areas of tort law, multiple defendants can be held liable for the same harm, as with defamation. Many products liability causes of action allow a plaintiff to impose joint and several liability on any party in the product distribution chain. These claims do not generally seek to hold the defendant liable *as a publisher*, but instead as the seller of a defective product. This is true even if the company may

have published harmful information about the product at some point.

For example, in *Erie Insurance v. Amazon*, 925 F.3d 135, 138 (4th Cir. 2019), customers sued Amazon after they purchased a headlamp from its website that spontaneously ignited and set fire to their home. The plaintiffs alleged that Amazon was the legal seller of a defective product because it fulfilled and shipped the order, which was originally posted by a third-party seller. *Id.* Amazon claimed Section 230 immunity, arguing that the claim sought to impose liability on Amazon for a product that a third party placed on its website. *Id.* The Fourth Circuit disagreed, holding that the plaintiffs' design defect claim did not treat Amazon "*as a publisher of speech* . . . [but] as the seller of a defective product." *Id.* at 140 (emphasis in original). This should be the outcome in most products liability suits against interactive computer services because the claims fault what the defendants did in creating their product, not what information another posted to their site.

D. When an online service provider is held liable for its own contributions to harmful content, it is treated as the publisher or speaker of its own information, not that of another.

If a claim against an interactive computer service could also be brought against an information content provider and an element of the claim is publishing or speaking harmful information, Section 230 will still not bar the claim if it alleges that the interactive computer service provided, created, or developed any part of the harmful information. Section 230 provides immunity only if the interactive computer service does

not "creat[e] or develop[ ]" the information "in whole or in part." *See* 47 U.S.C. § 230(f)(3). Claims that target an interactive computer service for its role in encouraging, soliciting, or contributing illegal content are not barred by the statute. A prototypical example would be *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008). In that case, the plaintiffs sued the defendants alleging that they had violated the Fair Housing Act, 42 U.S.C. §§ 3601 *et seq.*, by (1) requiring users to disclose protected characteristics such as sex, family status, and sexual orientation in order to enable discrimination against them, (2) generating user profiles that display these protected characteristics computer service, and (3) allowing potential landlords to filter and search for prospective tenants based on these protected characteristics computer service. 521 F.3d at 1166–67. The Ninth Circuit explained that Roommates.com could not escape the suit on Section 230 grounds because it became a developer, at least in part, of information transmitted by others by "requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers." *Id.* at 1166.

E. An overly broad interpretation of Section 230 does not serve the statutory purposes.

A properly scoped interpretation of Section 230 would better effectuate Congress's intent to achieve two basic goals: "to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene materials." *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003) (internal citations and quotation marks omitted). Overly broad interpretations of Section 230

have done the opposite, disincentivizing interactive computer services from implementing content monitoring or moderation policies that would remove harmful content. *See, e.g.*, *Herrick v. Grindr, LLC*, 765 F. App'x 586, 590–91 (2d Cir. 2019) (holding that Section 230 immunizes company from claim that it ignored the way its product design harmed users); *Dennis v. Mylife.Com, Inc.*, 2021 WL 6049830, at *6–7 (D.N.J. Dec. 20, 2021) (holding that broad immunity means credit reporting agency can ignore statutory duties to ensure it is using and communicating accurate information about people).

A properly scoped Section 230 would still promote the free exchange of information and ideas over the internet because it would immunize internet companies from most claims that could be brought against them for hosting others' speech. Internet companies would be immune to defamation, false light, intentional infliction of emotional distressful, and other torts that could be brought against the information content provider.

Unmeritorious cases can still be dealt with at the motion to dismiss stage even without Section 230 immunity. Plaintiffs must still get past a motion to dismiss phase that is very defendant-favorable given heightened pleading standards, *see Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007), and standing analyses, *see Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016); *TransUnion LLC v. Ramirez*, —— U.S. ——, 141 S. Ct. 2190, 2214 (2021). And plaintiffs must still state a claim. For example, products liability plaintiffs will still have the burden of establishing that there was a reasonable alternative design for an interactive

computer service's product, *see* Restatement (Third) of Torts § 2 Products Liability cmt. f (1998), and that the interactive computer service can be properly characterized as a seller, *e.g.*, *Erie Insurance*, 925 F.3d at 142–43 (dismissing the plaintiff's claim on the basis that Amazon did not sell the defective headlamp).

To the extent there is concern that a properly cabined Section 230 would chill certain types of speech because interactive computer services would over-police content, the problem lies with the underlying liability statutes, not Section 230. For example, those who fear chilling the communication of information about abortion as states begin to prohibit this type of speech are concerned about the statutes that would impose liability for abortion-related speech. These kinds of liability statutes are suspect under the First Amendment and would likely not survive a First Amendment challenge. While this Court should carefully consider the repercussions of a narrow interpretation of Section 230, Section 230 should not be stretched to solve the problem of overbroad liability statutes—the overbroad liability statutes must be challenged themselves.

II. Section 230 does not bar claims based on the design of an interactive computer service's platform and algorithms.

Most online services today do much more than simply host third-party content; these interactive computer services curate and customize what users see and how they interact with the service in ways that sometimes go far beyond simply hosting content. For example, when someone posts a public video on YouTube, that video is simultaneously published on their personal profile; filtered by YouTube's algorithm

to identify and limit the spread of content that violates—or comes close to violating—YouTube's community guidelines, *see* Christos Goodrow, *On YouTube's Recommendation System*, YouTube Official Blog (Sept. 15, 2021),[2] disseminated to other users based on their viewing behavior and the viewing behavior of similar viewers, *id.*, and analyzed to provide performance insights to information content providers that post on the platform, YouTube Creators, *Analytics in YouTube Studio*, YouTube (Apr. 28, 2020).[3] These actions are meaningfully different from each other: some, like publishing the video on a YouTube profile, are akin to publishing or speaking under defamation law, while others, like YouTube's data analytics and user segmenting services, are distinct from publishing and speaking third-party information.

Courts should be wary of attempts to muddle the distinction between publishing and speaking third-party information and other conduct. Section 230 immunity should not extend to the latter set of claims. This section highlights two such claims that fall outside the scope of Section 230: claims based on harmful platform design and claims based on harmful algorithmic design.

---

[2] https://blog.youtube/inside-youtube/on-youtubes-recommendation-system/.

[3] https://youtu.be/J1t34uTT0iA.

A. Claims alleging harmful platform design do not treat an interactive computer service as the publisher or speaker of third-party content.

A few recent cases have involved claims alleging that interactive computer service providers should face products liability for designing their platforms in ways that harm users. These products liability claims seek to hold a company liable for the harm it caused as the designer, manufacturer, marketer, or seller of a harmful product, not as the publisher or speaker of information. The basis for liability in a product liability claim is not the specific content posted by a user of the service, but the harmful design of a product (design defect), the harmful manufacturing of a product that was properly designed (manufacturing defect), or the harmful failure to warn of the dangers a product poses even if designed and manufactured properly (marketing defect or failure to warn). W. Page Keeton et al., *Prosser and Keeton on Law of Torts* 695 (5th ed. 1984); Restatement (Third) of Torts § 2 Products Liability (1999). Under the test laid out above, products liability claims do not seek to treat the interactive computer service as the publisher or speaker of an information content provider's content because (1) the claims could not be brought against the information content provider; and (2) publishing and speaking are not essential elements of a product liability cause of action.

Some courts have not appreciated this distinction because they have relied on a colloquial understanding of what it means to treat an internet company as a publisher. For example, in *Herrick v. Grindr*, 765 F. App'x at 588–89, the plaintiff sued Grindr, the company behind the eponymous web-based dating

application ("app"), for claims including defective design and defective marketing (also known as failure to warn). Herrick alleged that Grindr was liable for defectively designing its app because it failed to implement features that are commonly used by similar apps to protect users from harassment, abuse, impersonation, and stalking. Compl. ¶¶ 82–86, 100–107, *Herrick v. Grindr*, 765 F. App'x 586 (2d Cir. 2019). Because Grindr lacked these features, Herrick's ex-boyfriend was able to use the app to make fake dating profiles impersonating Herrick, match with men in Herrick's area, and send an average of 16 men per day to Herrick's home and work over a six-month period, many falsely expecting that Herrick wanted surprise "rape fantasy" sex and that he would give them drugs in return. *Id.* ¶¶ 50, 51, 62, 63, 66. Grindr ignored more than 100 requests to take down impersonating profiles and a temporary restraining order issued by New York state court ordering it to remove offending profiles, claiming it did not have the technology to do so, *id.* ¶ 75, even though similar apps did so easily, *see* Carrie Goldberg, *Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must be Fixed*, Lawfare.com (Aug. 14, 2019).[4]

Herrick's suit should have survived a Section 230 defense because it sought to hold Grindr liable for its role in violating its distinct duty to design a reasonably safe product. If Herrick had inadvisably tried to bring a harassment or defamation claim against Grindr based on the content of his ex-boyfriend's posts, Section 230 would clearly prohibit the claim for treating Grindr as the publisher and speaker of the

[4] https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed.

information content provider's impersonation accounts and messages. But Herrick instead focused on the independent harms imposed by Grindr's harmful design of its product, such as its willful refusal to block IP addresses of people confirmed to be using the site to abuse others.

Despite this, the Second Circuit held that Section 230 barred the claim because Grindr's hosting of the impersonation profiles was the but-for cause of Herrick's claim. According to the Second Circuit, the suit was barred because Herrick would never have brought it if his ex-boyfriend had not posted harmful third-party content. *See Herrick*, 765 F. App'x at 590–91. But that ignores the legal definition of treating an interactive computer service as a publisher or speaker. Just because third-party content is harmful does not mean that an interactive computer service is immune from all claims that relate to that harm. It is only immune from claims that seek to impose direct liability on the interactive computer service for a third party's harmful content.

Other courts have recognized that Section 230 would not bar claims based on the negligent design of an interactive computer service's platform. In *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1093 (9th Cir. 2021), parents of car crash victims sued Snap, the provider of a popular photo and video sharing phone application, on the theory that Snap negligently designed a speed filter on its application to encourage dangerous driving. The Ninth Circuit held that Section 230 immunity did not apply because the plaintiffs' claims sought to hold Snap liable for negligently providing a product that carried an unreasonable risk of harm to users, rather than for publishing or speaking any third-party

content. *Id.* at 1091–93. And although the Ninth Circuit found that, like the publication of impersonation profiles in *Herrick*, 765 F. App'x at 590–91, Snap's decision to publish photographs of users attempting to reach 100 miles-per-hour with Snap's speed filter was a but-for cause of the victims' injuries, it denied Section 230 immunity because the plaintiffs' negligent design claim did not "seek[] to hold Snap responsible in its capacity as a 'publisher or speaker.'" *Lemmon*, 995 F.3d at 1092–93. The "duty to design a reasonably safe product" extends even to interactive computer services whose business model revolves around third-party content because an interactive computer service's product design choices are "fully independent" from publishing or speaking third-party content under Section 230. *Id.* at 1093.

B. Claims alleging harmful algorithmic design need not treat an interactive computer service as the publisher or speaker of third-party content.

Like platform design claims, products liability claims alleging harmful algorithmic design choices do not necessarily implicate Section 230 immunity. Claims alleging harmful algorithmic design may come in the form of a products liability claim or a statutory claim under laws like the Fair Housing Act, 42 U.S.C. §§ 4601 *et seq.*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and similar state law provisions.

Algorithms can cause harm independent of any harmful underlying content. In 2018, for example, LinkedIn revealed that it would redesign its LinkedIn Recruiter algorithm, which matches job applicants with potential jobs, after discovering that the

algorithm favored men over women. Sheridan Wall & Hilke Schellmann, *LinkedIn's Job-Matching AI Was Biased. The Company's Solution? More AI.*, MIT Tech. Rev. (June 23, 2021).[5] Even though LinkedIn's algorithm purposely excluded protected characteristics like gender and race from its calculations, the algorithm nevertheless detected differences in user behavior between men and women (e.g., men applied to more jobs without having the necessary qualifications) and adjusted its job recommendations to give men more senior job postings. *Id.* Similar to the speed filter in *Lemmon*, the original LinkedIn Recruiter algorithm was designed in a way that caused user harm independent from any third-party content; users were harmed not because of any job posting or user profile, but because of an algorithmic design choice that facilitated hiring discrimination.

Thus far, no court has ruled on whether Section 230 bars products liability claims based on the design of recommendation algorithms,[6] and legal scholars disagree on how to apply products liability to algorithmic design. *Compare, e.g.*, Karni A. Chagal-Feferkorn, *Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers*, 30 Stan. L. & Pol'y Rev. 61, 66 (2019) (arguing for only

---

[5] https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-ziprecruiter-monster-artificial-intelligence/.

[6] At least 28 plaintiffs have *initiated* products liability litigation against major interactive computer services like Google regarding the addictive design of their recommendation algorithms. *See In Re Soc. Media Adolescent Addiction/Pers. Inj. Prods. Liab. Litig.*, 2022 WL 5409144, at *1–2 (J.P.M.L. 2022).

limited negligent products liability for algorithms) *with* Allison Zakon, *Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act*, 2020 Wis. L. Rev. 1107, 1110 (2020) (advocating strict products liability for recommendation algorithms). However, algorithms like the LinkedIn Recruiter algorithm showcase that interactive computer services can and have designed recommendation algorithms in ways that cause harm independent from the act of publishing third-party content. As in *Lemmon*, the mere fact that third-party content is involved does not eliminate an interactive computer service's duty to design reasonably safe products, including products supported by algorithms.

Discriminatory advertising claims under statutes like the Fair Housing Act, 42 U.S.C. § 3604—which may involve the publication of advertisements—also do not necessarily treat an interactive computer service as the publisher or speaker of "information provided by another [information content provider]." 47 U.S.C. § 230(c)(1). In *Roommates.com*, the Ninth Circuit held that, even under a broad interpretation of Section 230, an interactive computer service could not claim Section 230 immunity because it became a co-developer of discriminatory content when it "requir[ed] subscribers to provide [discriminatory preferences] as a condition of accessing its service, and by providing a limited set of pre-populated answers." 521 F.3d at 1166; *see also* Compl., *Nat'l Fair Hous. All. et al. v. Facebook, Inc.*, No. 1:18-cv-02689-JGK (S.D.N.Y. 2018) (alleging Meta violated Fair Housing Act by soliciting specific discriminatory preferences as part of its targeted advertising service). Interactive computer services provide targeted advertising services by

surveilling and segmenting their users: they collect nuanced user data; divide their users into distinct market segments based on demographics, topic interests, and geolocation, among other traits; then sell access to those user segments for targeted advertising.[7] When an interactive computer service provides user segments that reflect protected characteristics like race and solicits targeting preferences based on those characteristics, it acts not only as an interactive computer service, but also as an information content provider co-developing the illegal aspects of discriminatory housing advertisements. *See Roommates.com*, 521 F.3d at 1166. In other words, discrimination facilitated by targeted advertising does not rely on the content of any advertisement provided by an information content provider, but rather on the way that the interactive computer service segments users. Even if the advertisement was removed, the cause of the harm—the advertisement targeting service—would remain.

Lastly, Section 230 would not bar claims seeking to hold interactive computer services liable for harmful "dark patterns"—algorithmic and platform design practices that "trick or manipulate users into making choices that they would not otherwise have made and that may cause harm," Fed. Trade Comm'n, *Bringing Dark Patterns to Light* 2 (2022)—under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or similar state laws prohibiting unfair and deceptive business practices. Today's interactive computer services design sophisticated algorithms with the intent for these algorithms to influence how users experience online platforms and interact with each other. These design

---

[7] https://support.google.com/youtube/answer/2454017?hl=en.

decisions can trap users within harmful patterns without regard to any ICP content. For example, a 2021 report by Mozilla and Simply Secure found that YouTube gave users very little control over what recommendation they saw—even content in violation of YouTube's own content policies. Jesse McCrosky & Brandi Geurkink, Mozilla, *YouTube Regrets: A Crowdsourced Investigation into YouTube's Recommendation Algorithm* 8–23 (2021); *see also* Kelsey Smith et al., *Dark Patterns in User Controls: Exploring YouTube's Recommendation Settings*, Simply Secure (Nov. 30, 2021).[8] Some content settings were false or missing such that users could not make changes, while other settings were restricted to limited reactive feedback after viewing content and hidden behind a labyrinth of buttons and pages. Smith et al., *supra*. These design decisions, which are made by YouTube before and without regard to user-generated content, *see* Pauline Trouillard, *Social Media Platforms Are Not Speakers*, Ohio St. Tech. L.J. (forthcoming 2023) ("When [companies like Google] write their algorithms, they cannot know the messages to be conveyed using their processes—the algorithms are written before the users' posts are even created."), deceive users into believing they control what content they view while perverting the way that its recommendation algorithm learns and functions—and by limiting negative user feedback while allowing positive feedback, *see* Smith et al., *supra*. Claims based on YouTube's deceptive user control

[8] https://simplysecure.org/blog/dark-patterns-in-user-controls-exploring-youtubes-recommendation-settings/.

options and similar "dark patterns" target YouTube's own representations about its products and services, rather than the publication of any third-party content, and would not be barred by Section 230.

III. Section 230 does not bar claims against an interactive computer service simply because the company used third-party information to cause harm.

Internet companies have sometimes been able to use Section 230 as a shield when they use third-party information in harmful ways. For example, companies have repeatedly tried (with some success) to use Section 230 to escape liability for violating fair credit reporting requirements and for misappropriating a plaintiff's name or likeness to sell access to the interactive computer service. In most situations, these claims cannot be brought against another information content provider. Any reasonable interpretation of Section 230 should forestall immunity in such cases. To the extent that these types of claims treat companies as publishers or speakers at all, they treat companies as the publishers or speakers of information they created or developed, in whole or in part—that is, the company is the information content provider of the harmful information. The Court should clean up the mess left by lower courts and restore the original meaning of Section 230.

A. Section 230 does not bar Fair Credit Reporting Act claims that cannot be brought against the information content provider.

In recent years, companies that sell information about ordinary individuals through online databases have tried to use Section 230 to shield themselves from immunity for various claims under the Fair Credit Reporting Act ("FCRA"). Companies that assemble or evaluate information on consumers to furnish consumer reports to third parties are considered consumer reporting agencies ("CRAs") and are subject to certain legal obligations under the FCRA. 15 U.S.C. § 1681a(f). Companies like MyLife and The Source for Public Data ("Public Data") collect background information on millions of individuals, assemble the information into consumer reports, and even create scores that indicate a person's trustworthiness, such as MyLife's Reputation Score. These companies have faced lawsuits alleging that, among other things, they fail to maintain proper procedures to ensure accurate information as required by the FCRA. Compl. ¶ 87, *Dennis v. Mylife.Com, Inc.*, 2021 WL 6049830 (D.N.J. Dec. 20, 2021); *Henderson v. Source for Public Data, L.P.*, 53 F.4th 110, 125 (4th Cir. 2022). The companies have tried (with some success) to use Section 230 to avoid liability.

The courts should have swiftly rejected Section 230 immunity for the FCRA claims in these cases. The only entities that have responsibilities under the FCRA are CRAs, not their information content providers, and the information content providers cannot face any liability under the FCRA. Because FCRA claims cannot be brought directly against the information content providers, they do not treat the CRA as the

publisher of the information content providers' information. To the extent that a FCRA claim treats the CRA as a publisher or speaker at all, it treats the CRA as the publisher or speaker of its own information: a consumer report. Indeed, the whole point of the FCRA is to regulate consumer reports and the companies that assemble and furnish them because of the harm that credit reports—particularly inaccurate ones—can cause. *See* 15 U.S.C. § 1681 (explaining the reasons for regulating credit reporting). Certain FCRA claims, such as reasonable procedures claims, arguably do not treat a CRA as a publisher or speaker at all because a plaintiff need not allege publication to state such a claim.

But the district courts in both the MyLife and Public Data cases found that all claims against the companies were barred by Section 230. In *MyLife*, the court did not analyze each individual claim but found that, in general, the plaintiffs treated MyLife as a publisher because they sought to hold MyLife liable for the "exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter [a third party's] content." *MyLife*, 2021 WL 6049830, at *6. The court also found that plaintiffs sought to hold MyLife liable for information created by third parties because MyLife created its reports based on information the company gathered from other sources. *Id*. The court even found that the reputation scores could not be the basis of a claim because "the reputation scores appear to derive solely from information generated by third parties." *Id.*

The district court in the Public Data case similarly found that the plaintiff sought to hold Public Data liable for publishing third-party information

because the company "do[es] not produce the content of the reports at issue in this litigation." *Henderson v. Source for Public Data,* 540 F. Supp. 3d 539, 549 (E.D. Va. 2021). The Fourth Circuit reversed and came to the right outcome in this case, but it is not clear that the court would come to the right outcome in other cases. The court found that Public Data had "materially contributed" to the inaccurate content by omitting and summarizing information, making it the information content provider of the improper information. *Henderson*, 53 F.4th at 128. But it should not matter whether a CRA alters information in a consumer report to make it inaccurate; all that should matter is that the CRA assembled third-party data into a new information form, a consumer report, without having reasonable procedures for ensuring the accuracy of the data it used. In other words, the CRA's creation of a consumer report and its failure to have reasonable procedures are the basis of liability under the FCRA, not the third-party information on its own. That is why the claim cannot be brought against the information content provider and why Section 230 does not bar the claim.

Finally, the *Henderson* court acknowledged that the FCRA's reasonable procedures provisions do not, on their face, treat a CRA as a publisher or speaker because they do not require dissemination of information or that the information be improper. 53 F.4th at 125. But the court noted that a plaintiff would have to allege that the information was published to satisfy Article III standing. *Id.* at 126 (citing *TransUnion*, 141 S. Ct. at 2214). The court opined that this might indicate that the reasonable procedures claims "functionally depend on Public Data disseminating inaccurate information to a third party." *Id.* The court is

essentially saying that Section 230 bars any lawsuits that could not have been brought if defendants had not published harmful information. But a claim does not treat an interactive computer service as a publisher or speaker merely because publishing harmful content was a but-for cause of the eventual harm. What matters is whether the claim seeks to hold the interactive computer service liable as the publisher or speaker by holding them liable for the information content provider's tortious words. Standing has nothing to do with whether and to what extent a defendant is liable. Standing is jurisdictional; it only bears on whether the plaintiff can bring the claim in federal court. What a plaintiff must allege to show standing should not affect Section 230 immunity.

B. Section 230 does not bar misappropriation and other privacy tort claims that cannot be brought against the information content provider.

Companies that sell access to people's personal information online can face numerous privacy tort claims, such as misappropriation and public disclosure of private facts. Misappropriation claims often arise when these companies use pieces of people's personal information, like a teaser profile or a photo, to entice others to buy access to their database.

One recent suit alleged that Ancestry.com collected the yearbook photos of a group of plaintiffs and used the photos, without plaintiffs' consent, to entice people to subscribe to the company's service. The plaintiffs also alleged that Ancestry was liable for intrusion upon seclusion and unjust enrichment from its sale of plaintiffs' personal information.

The district court granted Ancestry immunity from all claims under Section 230. The court did not look at each individual claim but rather rejected them wholesale because the company "did not create the underlying yearbook records and instead obtained them from third parties." *Callahan v. Ancestry.com Inc.*, No. 20-CV-08437-LB, 2021 WL 783524, at *5 (N.D. Cal. Mar. 1, 2021). The court rejected plaintiffs' argument that Ancestry transformed the yearbook data into an advertisement, opining that "Ancestry did not transform data and instead offered data in a form . . . that did not alter the content. Adding an interactive button and providing access on a different platform do not create content. They just add functionality." *Id.* at *6 (citations omitted); *see also Callahan v. Ancestry.com Inc.*, No. 20-CV-08437-LB, 2021 WL 2433893, at *5 (N.D. Cal. June 15, 2021) (dismissing plaintiffs' amended complaint for the same reasons as it dismissed the previous complaint.). The court did not consider that the information that gave rise to the misappropriation claim was the *advertisement*, which Ancestry created, not the yearbook data on its own.

Several other courts have considered the same or similar issues as *Callahan* and come to the opposite conclusion, but much like *Henderson*, it is not clear that the analyses offered in these cases would always lead to the right outcome. For example, in *Fraley v. Facebook*, 830 F. Supp. 2d 785, 802–03 (N.D. Cal. 2011) (citation omitted), a district court in California correctly decided that a right of publicity claim against Facebook for transforming user "likes" into endorsements was not eligible for Section 230 immunity because Facebook's actions "go beyond 'a publisher's traditional editorial functions[,] such as deciding whether to publish, withdraw, postpone or alter content.'" Such

a test invites courts to analyze the extent to which an interactive computer service changes the third-party information. When the change is clear, such as in *Fraley*, the test may lead to the right outcome. But it is worth noting that *Callahan* applied *Fraley* and concluded that Ancestry did not meet the test precisely because the misappropriation was more subtle. *Callahan*, 2021 WL 2433893, at *7.

IV. Section 230 should not be read so broadly as to limit the enforcement of data privacy laws.

In recent years, several states have passed laws to regulate the collection, maintenance, sale, and use of user data. For example, five states—California, Colorado, Connecticut, Utah, and Virginia—have enacted comprehensive data privacy bills that limit the personal data interactive computer services can use and permit users to access, correct, and demand the deletion of their personal data held by those services. Cal. Civ. Code §§ 1798.100 *et seq.*; Colo. Rev. Stat. §§ 6-1-1301 *et seq.* (effective July 1, 2023); S.B. 6, 2022 Gen. Assemb., Feb. Sess. (Conn. 2022) (effective July 1, 2023); S.B. 227, 64th Leg., 2022 Gen. Sess. (Utah 2022) (effective Dec. 31, 2023); S.B. 1392, X, 161st Gen. Assemb. 2021 Special Sess. (Va. 2021) (effective Jan 1, 2023). These data privacy laws, as well as similar state and federal bills that have yet to pass, *see, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); S.B. 5062, 67th Leg., 2021 Reg. Sess. (Wash. 2021); H.B. 2969, 58th Leg., 2d Sess. (Okla. 2022), impose civil legal obligations onto interactive computer services that do not treat them as the publisher or speaker of third-party content.

When internet companies face data privacy obligations, including complying with deletion requests, processing limitations, retention limits, and other obligations, they are not being treated as publishers or speakers of third-party content. Rather, data privacy laws target harms caused by internet companies' own conduct—data retention, processing, and deletion—distinct from publishing or speaking activity under defamation law. As a result, neither state nor federal data privacy laws would be barred under Section 230. *See* 47 U.S.C. § 230(e)(3) (permitting state law enforcement "consistent with" the statute). By restoring the original meaning of Section 230, as discussed in Section I, *supra*, this Court would avoid needless confusion regarding legitimate state and federal regulatory interests and ensure that data privacy laws are properly enforced.

CONCLUSION

For the above reasons, *amicus* EPIC respectfully asks this Court to reverse the judgment of the U.S. Court of Appeals for the Ninth Circuit.

Respectfully submitted,

ALAN BUTLER
JOHN DAVISSON
MEGAN IORIO
THOMAS MCBRIEN
GRANT FERGUSSON

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
butler@epic.org

December 7, 2022