No. 18-396

IN THE
UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

MATTHEW HERRICK

Plaintiff-Appellant,

-against-

GRINDR, LLC, KL GRINDR HOLDINGS INC., and GRINDR HOLDING COMPANY,

Defendants-Appellees.

On Appeal from an Order of the United States District Court for the Southern District of New York

PLAINTIFF-APPELLANT'S PETITION FOR REHEARING *EN BANC*

Carrie A. Goldberg
Adam Massey
C. A. Goldberg, PLLC
16 Court Street
33rd Floor
Brooklyn, NY 11241
t. (646) 666-8908
carrie@cagoldberglaw.com

Tor B. Ekeland
Tor Ekeland Law, PLLC
195 Montague Street
14th Floor
Brooklyn, NY 11201
t. (718) 737-7264
tor@torekeland.com
docketing@torekeland.com

Table of Contents

Table of Contents

Cases

Other Authorities

Initial Statement

This is a case of exceptional importance to victims of violence targeted through the internet. Petitioner Matthew Herrick seeks rehearing *en banc* because the Panel's Summary Order endorses the dangerous status quo that multi-million- and billion-dollar internet companies are entitled to blanket immunity from liability for their intentional, knowing, and negligent facilitation of real-world violence and harassment. The danger posed to the public safety by Apps like Grindr is a question of exceptional importance that merits *en banc* review.

Grindr intentionally, knowingly, and negligently facilitated the targeting, stalking, and assault of Herrick by a user of its App. Herrick's fact pattern is not unique, and the numbers of people who suffer real world damage from internet stalking is only growing. The National Center for Victims of Crime estimates that stalkers target 7.5 Million Americans annually.[1] In this day and age, almost all stalking is aided by technology. The Panel's Summary Order ("Summary Order") affirming the District Court's dismissal holds that victims of internet violence have

---

[1] *See*, Chanta Da Silva, *Police Fined This 19-Year Old For Wasting Their Time With Stalking Complaints - Then She Was Killed*, Newsweek, April 10, 2019, available at https://www.newsweek.com/police-fined-19-year-old-wasting-their-time-stalking-complaints-then-she-was-1392114.

no recourse when an internet company, often the only one capable of stopping the harm, refuses. Law enforcement often isn't a recourse, due to overburdened law enforcers' inability to deal with sophisticated crimes involving tech and anonymity. And the Summary Order says the courts aren't a resource for victims either.

Grindr was in the exclusive position of control to stop the attack its App directed at Herrick. Grindr's competitors quickly did spring to action to help when their Apps were also used against Herrick. But Grindr did nothing, even after Herrick desperately pleaded for help approximately 50 times. The Summary Order is an endorsement of Grindr's inaction.

The rapid spread of the Internet of Things (IOT), where interactive computer services have intimate access to every aspect of our private and professional lives is only going to worsen this threat. Already, interactive AI devices like Alexa are finding their way into our homes and soon to follow, self-driving cars into our garages. The Court should grant *en banc* review because of the seriousness of this growing threat.

En banc review is also warranted because the Summary Order conflicts with *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016). Consideration by the full court is necessary to secure and maintain uniformity with *LeadClick* and reconcile the summary order with other circuits. Thus, this case satisfies the

criteria laid out in Federal Rule of Appellate Procedure 35(b) for a rehearing *en banc*.

Introduction

Every one of us is a moment away from crossing paths with somebody hell-bent on our destruction. The anonymity, convenience, accessibility and force-multiplying nature of the internet makes it simple to attack somebody else remotely. The Summary Order endorses an overbroad reading of the Communications Decency Act § 230 (CDA) that allows internet companies to escape accountability when they intentionally, knowingly, or negligently facilitate stalking, rape, and murder. At all times in this case, Grindr had control over its App and could have stopped the harm. But it ignored all pleas for help from Herrick whose life was constantly interrupted – as many as 23 times a day -- by strangers coming in-person expecting to have sex with him. Grindr only finally responding when sued, but even then claimed it lacked the ability to stop malicious use of its product even though its competitors quickly could and did.

The threat to the public safety posed by Apps like Grindr, which users have successfully, indisputably used to commit domestic violence, stalking, rape, murder, and child molestation is an issue of exceptional importance that warrants *en banc* review by this Court. Rehearing *en banc* is justified because, among other reasons:

1. The threat to the public safety posed by Apps like Grindr is a question of exceptional importance

2. The Summary Order conflicts with this Court's precedents and other circuits' decisions, and
3. The Summary Order gets facts wrong.

The Summary Order reduces everything to third party content - without elucidating any clear theory of why this is so - and avoids difficult questions. But human beings are not content, and the violence that Apps and companies like Grindr knowingly and negligently facilitate against women, men, and members of the LGBTQ community is real. This Court should grant rehearing *en banc* given the seriousness of this public safety threat.

I. The Threat to the Public Safety Posed by Apps that Facilitate Violence is a Question of Exceptional Importance

An *En Banc* rehearing is appropriate because of the exceptional importance of the question whether internet companies enjoy immunity for acts of stalking, rape, and murder they intentionally, knowingly or negligently facilitate through products and services they exclusively control. Under the Summary Order's reasoning, immunity under the CDA is absolute and covers all causes of action. The question of whether the CDA grants *de facto* absolute immunity for internet companies for real world violence facilitated by their products and services is one of exceptional importance because it's a matter of life and death for many.

But even if this Court believes that the very real, growing harm to victims of internet targeted physical violence isn't a question of exceptional importance to the

public safety, rehearing *en* banc is warranted by the Summary Order's conflict with its decision in *FTC v. LeadClick*.

II. The Summary Order Conflicts with *FTC v. LeadClick*

A. Under FTC v LeadClick Knowing Control of a Deceptive Harm Eliminates CDA Immunity

In 2016, this Court eliminated CDA §230 immunity for defendants who knowingly fail to exercise control over deceptive content on their platforms when they have control.[2]

LeadClick was an internet company that sold advertising space on fake news web sites.[3] When the FTC sued LeadClick for its deceptive advertising, appellant LeadClick argued that CDA §230 shielded it from liability because it was third parties – and not LeadClick – that created the deceptive content. This Court rejected that argument, eliminating CDA limited immunity not just for the original creators of deceptive content, but also for those who knowingly control the deceptive content:

> [W]e conclude that a defendant acting with knowledge of deception who either directly participates in that deception or has the authority to control the deceptive practice of another, but allows the deceptions to proceed,

---

[2] *See FTC v. LeadClick Media, LLC*, 838 F.3d 158 (2d Cir. 2016),
[3] *Id*. at 162-66.

> engages, *through its own actions,* in a deceptive act or practice that causes harm to consumers.[4]
> (emphasis in original).

LeadClick emphasizes that a defendant with authority to control deceptive activity on its platform can be held liable for the harms resulting from that deception. *LeadClick* held that the failure to exercise control over known deceptive content or conduct renders an interactive computer service (ICS) an information content provider (ICP) as to the deceptive content it controls, and therefore it is not entitled to CDA limited immunity.[5]

The Summary Order doesn't explain why the *FTC v LeadClick* holding doesn't apply to Herrick. Just like LeadClick, Grindr was fully aware of the deceptive and malicious use they facilitated with their App. Herrick told them almost 50 times. Grindr was in control of a situation it knew about and could easily end. And instead did nothing.

The Summary Order conflicts with *LeadClick's* reasonable, common sense interpretation of the scope of CDA limited immunity by recognizing that those with authority to control an online platform are responsible for the harm if, as here, they instead looked the other way when the could have easily stopped it.

---

[4] *Id.* at 170.
[5] *Id.* at 176.

Disregarding *LeadClick,* the Summary Order adopts the District Court's view that "[w]hile the creation of the impersonating profiles may be sufficiently extreme and outrageous, Grindr did not create the profiles."[6] That may or not be true, there's been no discovery or expert testimony in this case, but it misses the point. Grindr controlled its App -- there is nothing in the Complaint that alleges otherwise -- and it knowingly and negligently facilitated a harm that it was on notice of and that it could easily stop. The Summary Order conflicts with *LeadClick* because, among other things, it fails to acknowledge *LeadClick* holding that control over a real world, non-publication tort harm moves a case outside the realm of CDA limited immunity.

In *LeadClick* the non-publication tort harm was essentially consumer fraud.[7] Likewise, in Herrick's case, the claims relate to product liability, intentional torts, negligence, and deceptive business practices. This Court should grant rehearing *en banc* because the Summary Order conflicts with *LeadClick*.

B. The Summary Order Doesn't Follow LeadClick's Analysis

LeadClick rejects guaranteed immunity for an internet company simply because "it 'enabled computer access by multiple users to a computer server by

---

[6] *Herrick v. Grindr, LLC,* 306 F.Supp.3d 579, 594 (S.D.N.Y. 2018).
[7] *LeadClick* 838 F.3d at 176.

routing consumers" from one place to another.[8] Instead, *Leadclick*, among other things, looks at the purpose and use of an online product or service and how that squares with congressional intent. Does it live up to Congress' desire to promote the "'the availability of educational and informational cultural resources to our citizens' and to offer a forum of true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity[?]"[9] Stalking, rape, and murder are notably absent from this list.

When Congress passed the CDA, it only intended to empower simple websites and bulletin boards to moderate passive content on their site without getting sued all the time for defamation because of trash talk, or for exercising control over uploaded porn.[10] Two decades ago Congress didn't foresee the danger that Apps like Grindr loaded with geolocating and targeting functionality posed to the public. In 1995, Congress wasn't considering computer functionality that causes violence in the real world. For this reason alone the Court should grant *en banc* review to give this serious issue the careful consideration it merits.

---

[8] *LeadClick* 838 F.3d at 174.
[9] *Id.*at 176.
[10] *See* Appellants Opening Brief ("AOB"), at pp. 25-27 (Appeal Dkt. 53) (discussing the legislative intent of the CDA).

Additionally, under *LeadClick*, a defendant has the burden of establishing its ICS status, something Grindr never has done.[11] And *LeadClick* recognizes that a computer product or service may be an ICS in some contexts but not others.[12] The Summary Order doesn't analyze any of this.

Thus, this Court should grant rehearing *en banc* to resolve the conflict between the Summary Order and *LeadClick*.

C. The Summary Order Doesn't Address that CDA Immunity is an Affirmative Defense

CDA limited immunity is an affirmative defense for which the defense carries the burden of proof.[13] Dismissing well pleaded claims on the basis of CDA limited immunity is only proper if the defense is plain from the face of the complaint.[14] The Summary Order doesn't analyze the law on this point despite the

---

[11] *See Leadclick* 838 F.3d at 175-76. (discussing Leadclick's failure to show it was an ICS).
[12] *Id.*
[13] *See, e.g., id.*; *Doe v. GTE Corp.*, 347 F.3d 655, 657 (7th Cir. 2003) (holding that CDA limited immunity is an affirmative defense and that "[a]ffirmative defenses do not justify dismissal under Rule 12(b)(6); litigants need not try to plead around defenses."); AOB at 18.
[14] *See Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (2d Cir. 2015) ("Although "[p]reemption under the Communications Decency Act is an affirmative defense, . . . it can still support a motion to dismiss if the statute's barrier to suit is evident from the face of the complaint.").

fact this was Herrick's lead argument in his opening brief. [15] And given that both the CDA's text and the case law are clear that CDA limited immunity does not apply to non-publication torts, it makes sense that it should be an affirmative defense.[16] Because the factual questions are complex, and are not all reduceable to third party content under some unarticulated theory of distinguishing first party content from third party content from conduct, and non-publication torts from publication torts. The complexity of the factual issues is improper for the motion to dismiss stage, and the Court should grant rehearing *en banc* to explain where the procedural law stands when it comes to the exceptionally important question of whether CDA immunity is an affirmative defense. Because the consequences of granting CDA limited immunity at the motion to dismiss stage instead of as an affirmative defense leads to courts getting facts wrong because they don't have the benefit of discovery and adversarial proceeding below. The result is plaintiffs with profound harms are deprived of their day in court. And that's what happened here.

---

[15](S*ee* AOB at pp.18 – 21.).

[16] *See, e.g., Doe v. Internet Brands, Inc.*, 824 F.3d 846, 854 (9th Cir. 2016) (discussing failure to warn claims); *City of Chicago v. StubHub!, Inc.*, 624 F.3d 363, 366 (7th Cir. 2010), ("[S]ubsection (c)(1) does not create an 'immunity' of any kind. It limits who may be called the publisher of information that appears online" (citations omitted).); *McDonald v. LG Elecs. USA, Inc.*, 219 F. Supp. 3d 533, 537 (D. Md. 2016) (stating the CDA 230 does not immunize defendants from all product liability claims.).

D. The Summary Order Gets Facts Wrong

The Summary Order relies on mistaken facts not in the record. Herrick alleges in his Complaint that in November 2015, he "removed his Grindr profile because the relationship had become more serious and exclusive." The Panel and the District Court both assume that Herrick "deactivated" his account and never used the App again.[17] This is mistaken. "[R]emoving a profile" from view on one's phone and "deactivating an account" are different things. One can remove an App from a phone, without deleting an account.

Herrick never alleges – because it isn't true – that he'd stopped using Grindr before the abuse began and never used it again. Identifying, monitoring, and reporting the impersonating accounts required that he use a Grindr account. Grindr's own attorneys said the best way for Grindr to observe the problem was for a user to flag the problem account(s), an impossibility for a non-user.[18]

This mistaken factual speculation renders much of the Summary Order's reasoning problematic because it depends on this assumption. The Summary Order's proximate cause analysis assumes that Herrick stopped using Grindr in

---

[17] Summary Order at 8; District Court Order at pp. 2, 23 (Joint Appendix ("JA") at pp.191, 212. (Appeal Dkt. 43.)).
[18](Tr. of TRO Hearing (S.D.N.Y. Feb. 22, 2017) (JA at p. 150.).

2015.[19] And it used this assumption as a basis for affirming the dismissal of Herrick's claims for: fraud, negligent misrepresentation, promissory estoppel, deceptive business practices, and false advertising.[20]

The Summary Order states:

> It is uncontested that Herrick was no longer a user of the app at the time the harassment began; accordingly, any location information was necessarily provided by Herrick's ex-boyfriend.[21]

This is problematic not only because it overlooks that Herrick was basically coerced into using the App to plead with Grindr for help. It ignores the real possibility that readily available geo-location "spoofing" software was used to target Herrick. Geo-spoofing is a common and well-known phenomena, and both Apple's App Store and Google's Play store contain Apps that can be downloaded for this purpose to work with Grindr.[22] Grindr knew, or should have known, about this danger, yet did nothing to prevent it.

---

[19] (Summary Order at 7 (Appeal Dkt. 156)).
[20] (*Id.*).
[21] (*Id.* at 5).
[22] *See* Tim Fisher, *How to Fake a GPS Location on Your Phone*, Lifewire.com Feb. 9, 2019, available at https://www.lifewire.com/fake-gps-location-4165524 (last visited April 10, 2019).

This highlights crucial questions as to whether Grindr is defectively designed because it permits known dangers such as Geo-Spoofing, and also demonstrates why Herrick's failure to warn, and other claims should never have been dismissed on speculative facts not in the record relating to when Herrick was and was not using Grindr. Ultimately, these claims don't all turn on whether Herrick was using Grindr at a given time, but rather if Herrick was a victim of a dangerous product whose manufacturer who had a duty to protect against known dangers under its control. This puts Herrick's case squarely under the rubric of such cases like the Ninth Circuit's *Doe v. Internet Brands*, 824 F.3d 846 (9th Cir. 2016).

If this case had proceeded to discovery, and was before this Court on an appeal of a Summary Judgement, the Court would have been aware of the fact that Herrick had to report Grindr's facilitation of his stalking, and attempt to stop it, by downloading Grindr for the sole purpose of pleading with Grindr for help.[23] But it granted a Summary Order affirming a grant of CDA limited immunity at the motion to dismiss stage. And in so doing, it made mistaken factual assumptions on a matter of life and death to victims of internet targeted violence. That the Summary Order is premised on mistaken factual assumptions warrants *en banc*

---

[23] *See* AOB at p. 12 ("[f]rom November 2016 through January 2017, Mr. Herrick reported the impersonation and stalking approximately 50 times to Grindr".).

review because the threat to public safety this case involves is a question of exceptional importance.

Conclusion

Millions of Americans are stalked annually. It is a question of exceptional importance whether internet companies enjoy absolute immunity when they knowingly facilitate stalking, harassment, and violence that they can easily stop with the exclusive control their platforms have over these targeted crimes. The Summary Order conflicts with this Court's precedent in *FTC v. LeadClick Media, LLC.* And the Summary Order can't be reconciled with all the decisions that hold CDA limited immunity is an affirmative defense. Finally, the Summary Order is premised on mistaken factual assumptions. Thus, the Court should grant rehearing *en banc.*

April 10, 2019

C.A. Goldberg, PLLC

By: */s/ Carrie A. Goldberg*
Carrie A. Goldberg
Adam G. Massey
C.A. Goldberg, PLLC
16 Court Street
33rd Floor
Brooklyn, NY 11241
t. (646) 666-8908
carrie@cagoldberglaw.com

Attorneys for Appellant
Matthew Herrick

Tor Ekeland Law, PLLC

By: */s/ Tor B. Ekeland*
Tor B. Ekeland
Tor Ekeland Law, PLLC
195 Montague Street
14th Floor
Brooklyn, NY 11201
t. (718) 737-7264
tor@torekeland.com

Attorneys for Appellant
Matthew Herrick

CERTIFICATE OF COMPLIANCE

Counsel for Plaintiff-Appellant Matthew Herrick certifies under Federal Rules Of Appellate Procedure 35 that the above Petition contains 3522 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f), according to the Word Count feature of Microsoft Word.

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface in 14-point font of Times New Roman.

April 10, 2019

By: */s/ Tor B. Ekeland*

Tor B. Ekeland
Tor Ekeland Law, PLLC
195 Montague Street
14th Floor
Brooklyn, NY 11201
t. (718) 737-7264
tor@torekeland.com

Attorneys for Appellant Matthew Herrick

CERTIFICATE OF SERVICE

Counsel for Plaintiff-Appellant Matthew Herrick certifies that on April 10, 2019, a copy of the attached Petition for Rehearing *En Banc* was filed with the Clerk through the Court's electronic filing system.

I certify that all parties required to be served have been served.

April 10, 2019 By: */s/ Tor B. Ekeland*

Tor B. Ekeland
Tor Ekeland Law, PLLC
195 Montague Street
14th Floor
Brooklyn, NY 11201
t. (718) 737-7264
tor@torekeland.com

Attorney for Appellant
Matthew Herrick