Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must be Fixed

By Carrie Goldberg, Wednesday, August 14, 2019, 8:00 AM

For two and a half years, I've been fighting for the gay dating app Grindr to bear responsibility for the harms my client Matthew Herrick endured because of its defective product. Last week, Matthew, my co-counsel Tor Ekeland and I petitioned the Supreme Court for a writ of certiorari in Matthew's case against Grindr.

The question is whether the immunity provided to platforms by Section 230 of the Communications Decency Act has any meaningful limits at all. As discussion of Section 230 has become more frequent and mainstream in the last several months, with solemn events—like 8chan apparently hosting the suspected murderer's racist screed in the El Paso shooting and Facebook being painfully slow to remove the live-streamed Christchurch massacre—forcing the U.S. to rethink liability for third-party platforms, it is important that this conversation not be conducted in fuzzy abstracts. Rather, everyone involved in the discussion must look at the stories of real individuals who have been deeply wounded, their lives upended, because of platforms turning a blind eye or willfully ignoring injuries their products facilitate. In all cases involving a Section 230 immunity defense, there are two stories—the story of the individual and the story of the litigation. This is Matthew's story.

Herrick v. Grindr is a civil lawsuit born from the urgent need for immediate help in a life or death situation. While the goal of most Section 230 cases—and litigations in general—is financial compensation for past injuries, Matthew's suffering was ongoing. Matthew's ex-boyfriend, Oscar Juan Carlos Gutierrez, was impersonating him on Grindr and sending men to Matthew's home to have sex with him.

It all started one evening in late October 2016, right before Halloween. Matthew had been sitting on the front stoop of his New York City apartment, smoking a cigarette, when a stranger called to him from the sidewalk and started heading up the steps toward him. The stranger's tone was friendly and familiar. But Matthew had never met this guy before. "I'm sorry," he said. "Do I know you?"

The stranger raised his eyebrows and pulled his phone from his back pocket. "You were just texting to me, dude," he replied, holding out his phone for Matthew to see. On the screen was a profile from the gay dating app Grindr, featuring a shirtless photo of Matthew standing in his kitchen, smiling broadly. Matthew recognized the picture right away. He'd posted it on his Instagram account a few weeks earlier. But the Grindr profile wasn't his. "I wasn't talking to you," Matthew explained. "That's not my account."

They went back and forth for a while. The stranger kept holding up his phone, insisting Matthew had invited him over for sex. But Matthew knew the profile wasn't his. Finally, the stranger became exasperated and left. "Fucking liar!" he shouted in Matthew's direction as he walked away. "You're an asshole!"

Rattled, Matthew went back inside. A few minutes later, he heard his buzzer ring. It was another man insisting that he, too, had made a sex date with Matthew. Two more men showed up that day. And three others came calling the next. "Matt!" they'd holler from the sidewalk, or they'd lean on the buzzer expecting to be let in. At first the strangers only went to his apartment, but by the end of the week a steady stream of men was showing up at the restaurant where Matthew worked as well. Some were in their 20s, others much older. A few arrived in business suits, as though on the way to the office. Others

were twitchy and sweaty, looking like they'd been up all night getting high. They'd stalk him at work and at home, all hours of the day and night, each one convinced Matthew had invited him over for sex.

He was pretty sure he knew who was behind the attack: Gutierrez, his ex. The pair had met more than a year prior, on Grindr, and dated for 11 months. As time wore on, Gutierrez became increasingly jealous and clingy, accusing Matthew of cheating and doing things like showing up at Matthew's job and refusing to leave. Eventually, Matthew couldn't take it anymore; the pair broke up. The week after he ended his relationship with Gutierrez, strange men began showing up at Matthew's door.

The impersonating profile sent men for fisting, orgies and aggressive sex. They were told that if he resisted, that was part of the fantasy. They should just play along. It seemed clear to me that Gutierrez was endeavoring to do more than harass and frighten Matthew. He appeared to be trying to recruit unwitting accomplices to perpetrate sexual assaults.

Like many of my clients, before coming to see me Matthew had tried everything he could to take care of the problem on his own. He filed more than a dozen complaints with his local police precinct. The officers dutifully took down his information but didn't seem to understand the danger he was in. "One guy rolled his eyes," Matthew recalled. "I think they figured since I'm a big guy, and I look like I should be able to take care of myself, that I should just go beat him up or something. I guess to them I don't look like a 'victim.' " Another officer suggested Matthew pack up his belongings and "find a new place to live."

By the time Matthew came to me for help, the Manhattan district attorney opened an investigation and he'd gotten a family court "stay away" order, but neither was stopping the traffic of strangers coming to his home and work for sex. He also did everything he could to get the imposter profiles taken down. He directly contacted Grindr and its competitor Scruff, which Matthew's ex was also using to impersonate him, and begged the companies to remove the fake profiles from their platforms. In their terms of service, both companies explicitly prohibit the use of their products to impersonate, stalk, harass or threaten. Scruff, the smaller of the two companies, responded to Matthew immediately. It sent him a personal email expressing concern, took down the fake accounts, and blocked Gutierrez's IP address, effectively banning him from the app. When Gutierrez started impersonating Matthew on Jack'd, yet another gay dating app, that company also banned Gutierrez from using its platform to harass Matthew. But Grindr took a different approach: It did absolutely nothing.

"I emailed and called and begged them to do something," Matthew told me, the frustration rising in his voice. His family and friends also contacted Grindr about the fake profiles—in all, about 50 separate complaints were made to the company, either by Matthew or on his behalf. The only response the company ever sent was an automatically generated email: "Thank you for your report."

All in all, more than 1,400 men, as many as 23 in a day, arrived in person at Matthew's home and job over the course of 10 months.

Grindr is a wildly successful company. In 2018, the dating app reportedly had more than three million users in 234 countries. Like most social media companies, Grindr operates, in large part, as an advertising platform. The free content and services these platforms provide—porn, photo sharing, direct messaging, emailing, shopping, news, dating—are really just lures to get people to show up so the companies can collect data about what users buy, who they're friends with and where they're going,

and use that information to advertise. Grindr prides itself on its state-of-the-art geolocative feature, which can pinpoint a user's exact location, allowing users to match with others in their vicinity. This is how they rake in advertising revenue—by customizing the ads that users see based on nearby businesses.

Even though Grindr's terms of service state that Grindr can remove any profile and deny anybody the use of their product at the company's discretion, they refused to help. After Matthew's approximately 50 pleas to Grindr for help were ignored, we sued Grindr in New York State Supreme Court, New York County, and obtained immediate injunctive relief requiring that Grindr ban Gutierrez.

It's not clear exactly how Gutierrez was exploiting Grindr to send the strangers to Matthew—it might have been through a spoofing app that worked with Grindr's geolocation software or something more technical. But the strangers who came to Matthew said they were sent through the Grindr app and would show Matthew the fake profiles with his pictures, geolocation maps showing how far away they were from Matthew, and direct messages telling them which buzzer to ring and what kind of sex Matthew was eager to have.

I didn't need to explain on a technical level how Grindr was being used against Matthew at this stage of the litigation; that's what discovery is for. What we knew is that Grindr was in an exclusive role to help stop Matthew's hell, given law enforcement was too slow and Gutierrez had been deterred by neither arrests nor orders of protection.

I knew from the start that Grindr would claim it was immune from liability pursuant to Section 230 of 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." Section 230 was originally conceived to shield internet companies that ran online message boards—where the majority of user-generated content appeared online—from legal action traditionally lodged against publishers, like defamation and obscenity claims. Today, of course, the internet looks very different than it did in 1996, when the law was passed. Tech companies today wield unimaginable power and influence and offer services that didn't even exist in 1996, like direct messaging and geolocating. Yet internet companies not only use Section 230 to shield themselves from liability for anything users post on their platforms; they also think that immunity extends to cover any and all decisions they make about how their products operate—even if those decisions cause users harm.

So I made sure not to sue Grindr for traditional publication torts like defamation. That is, I was not suing them for any words that Gutierrez said on the profiles or communications he'd made on the app. Instead, I tried something new—I sued Grindr using traditional product liability torts. I argued that Grindr is a defectively designed and manufactured product insofar as it was easily exploited—presumably by spoofing apps available from Google and Apple—and didn't have the ability, according to the courtroom admissions of Grindr's own lawyers, to identify and exclude abusive users. For a company that served millions of people globally and used geolocating technology to direct those people into offline encounters, it was an arithmetic certainty that at least some of the time the product would be used by abusers, stalkers, predators and rapists. Failing to manufacture the product with safeguards for those inevitabilities, I argued, was negligent.

On Feb. 8, 2017, Grindr filed a notice of removal from state court to the Southern District of New York. Our temporary restraining order requiring that Grindr ban Gutierrez from its services expired as a

matter of law 14 days after the removal—but when we moved to extend the order, Judge Valerie Caproni denied the extension. Judge Caproni felt our underlying case lacked merit because she suspected Grindr was immune from liability pursuant to the Communications Decency Act, arguing that our claims depended on information provided by another information content provider. If not for Matthew's ex using the app, she reasoned, none of this would have happened to Matthew. She reduced all the harm as flowing from Gutierrez's actions, not Grindr's, and therefore reasoned that the company was immune from liability and had no obligation to Matthew. In April and May of 2017, Grindr and its holding companies filed motions to dismiss our claims. At the time, Matthew's ex was continuing to relentlessly use the app to send strangers to his home and job—a fact the court knew. However, it was not until the following year that the court ruled on the motion to dismiss. By this time, Tor Ekeland had joined me representing Matthew.

We argued in our opposition papers that because we were suing Grindr for its own product defects and operational failures—and not for any content provided by Matthew's ex—Grindr was not eligible to seek safe harbor from Section 230. To rule against Matthew would set a dangerous precedent, establishing that as long as a tech company's product was turned to malicious purposes by a user, no matter how foreseeable the malicious use, that tech company was beyond the reach of the law and tort system.

Nevertheless, on Jan. 25, 2018 Judge Caproni dismissed our complaint entirely. All but a copyright claim was dismissed with prejudice, meaning that even if Matthew learned new information to support his claims, he could not amend his complaint.

Matthew's case was thrown out before we'd even gotten our foot in the door—even though dismissal at the motion to dismiss stage is supposed to be reserved for situations where a complaint is defective on its face, while ours was a detailed, thorough 43 pages and well-pleaded. The judge relied on Grindr's immunity under Section 230.

Usually, to benefit from an affirmative defense like Section 230, a defendant has the burden of proving it satisfies the elements of that defense. Grindr would have needed to serve an answer claiming it was immune under Section 230 and allege all three of the statute elements for the company to get the enormous benefit of immunity—that it was (1) "an interactive computer service" (2) being "treated as a publisher" of (3) "information provided by another information content provider." Instead, contrary to procedural rules but nevertheless common in Section 230 cases, the judge saved Grindr that step by dismissing the case before Grindr had filed a single pleading.

On Feb. 9, 2018, we filed a Notice of Appeal with the U.S. Court of Appeals for the Second Circuit. The case was scheduled to be heard on Jan. 7, 2019. By then, it had become one of the most closely watched Section 230 cases in the country. It had been covered widely in the media, with attention paid to our novel product liability approach. Plus, because of a string of bad press for tech companies—major data breaches by Facebook, the Cambridge Analytica scandal, stilted testimony by Facebook CEO Mark Zuckerberg to Congress, and the use of major platforms to disseminate fake news aimed at altering the course of U.S. elections—many people were waking to the idea that Big Tech might not be quite so trustworthy. At the same time, the Communications Decency Act became a major topic of mainstream conversation. Producers at Netflix planning a new show with comedian Hasan Minhaj put together a widely viewed episode on the legislation.

To our disappointment, on March 27, the Second Circuit issued a summary order affirming the district court's dismissal of the complaint. On April 11, we filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc.* On May 9, that too was denied.

Which leads me to this moment—our filing on Aug. 7, a petition for a writ of certiorari from the Supreme Court of the United States. We are presenting the court with two questions:

1. Does the Communications Decency Act Section 230(c)(1), which protects interactive computer services from liability for traditional publication torts when they publish third-party content, prevent well-pleaded causes of action for non-publication torts—such as product liability, negligence, fraud and failure to warn—as a matter of law?

2. Whether Section 230(c)(1) is an affirmative defense and therefore inappropriate for resolution at the motion to dismiss stage.

The Supreme Court has never ruled on the proper scope of Section 230. As Matthew's case demonstrates, this is a matter of life or death for victims of stalking and violence caused and exacerbated by computer technologies unimagined when Congress passed the law in 1996. Decades ago, lawmakers had this pie-in-the-sky idea that internet companies would monitor content their users uploaded to protect the rest of us. What's become painfully apparent, and arguably should have been obvious, is that without the threat of legal liability hanging over their heads, companies like Grindr really don't care about who gets hurt.

This debate is muddied by the fact that the federal and state court decisions in this country lack clarity and are often contradictory as to the Communications Decency Act's proper scope, which has led many courts to create an almost absolute immunity for internet companies for their tortious conduct. Courts do this, as the lower courts did in our case, with overbroad definitions of what constitutes an "interactive computer service" and what constitutes information provided by a different "information content provider." These are, or should be, fact-intensive inquiries, but if cases are dismissed on motions to dismiss for failure to state a claim, as ours was—before discovery and without defendants even needing to plead Section 230 immunity—plaintiffs will never have a chance.

This case is not only about justice for Matthew. We are fighting for future victims' rights to sue any tech company that knowingly, or recklessly, aids their abusers and causes victims harm. What's more, determining the scope of the Communications Decency Act is a crucial component of society's current debate about the responsibility internet companies bear for the harm their technologies arguably propagate. This could be no truer than this moment when mass shooters are radicalizing and posting propaganda on the likes of 8chan, mentally ill people with restraining orders are murdering with weapons purchased from online gun sellers, and individuals with warrants out for their arrests are killing people they match with on dating apps and torturing individuals they meet in the back seats of pooled rideshares.

Most industries would also like to be free from liability for harms their product, services or staff could cause their customers. But the reality is, legal responsibility for one's products and services is the cost of doing business and drives safety innovation. Other business owners purchase liability insurance and—for the sake of reputation, low insurance premiums and morality—run businesses that don't harm customers or the general public.

All in all, Section 230 is a government subsidy to the industry least in need and least deserving of it. It's time to fix 230—and if the Supreme Court won't do it, legislators must act.