18-396-cv

United States Court of Appeals

for the

Second Circuit

MATTHEW HERRICK,

Plaintiff-Appellant,

– v. –

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

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF SANCTUARY FOR FAMILIES, INC., CYBER SEXUAL ABUSE TASK FORCE, DAY ONE, DOMESTIC VIOLENCE LEGAL EMPOWERMENT & APPEALS PROJECT, HER JUSTICE, LEGAL MOMENTUM, MY SISTER'S PLACE, NEW YORK LEGAL ASSISTANCE GROUP AND SAFE HORIZON AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANT

STACEY J. RAPPAPORT
NICOLE C. NIELSON
MILBANK, TWEED, HADLEY & MCCLOY LLP
Attorneys for Amici Curiae
28 Liberty Street
New York, New York 10005
(212) 530-5000

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici curiae* make the following statement of disclosure:

The *amici curiae* are Sanctuary for Families, Inc., Cyber Sexual Abuse Task Force, Day One, Domestic Violence Legal Empowerment and Appeals Project, Her Justice, Legal Momentum, My Sister's Place, New York Legal Assistance Group, and Safe Horizon.

The *amici curiae* certify that none of the *amici curiae* has a parent corporation or publicly held corporation that owns ten percent or more of its stock or membership interests.

Dated: May 31, 2018

MILBANK, TWEED, HADLEY, & McCLOY LLP

By: /s/ *Stacey J. Rappaport*

Stacey J. Rappaport
28 Liberty Street
New York, New York 10005-1413
Phone: (212) 530-5000
Fax: (212) 822-5347
srappaport@milbank.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Rules

Other Authorities

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

Sanctuary for Families, Inc. ("Sanctuary") is the largest non-profit in New York dedicated exclusively to serving victims of domestic violence, sex trafficking, cyber abuse, and related forms of gender violence. Every year, Sanctuary offers legal, shelter, clinical and economic empowerment services to over 15,000 survivors. Sanctuary also engages in extensive community outreach, education, and training, and advocates for policies and legislation designed to protect survivors.

The Cyber Sexual Abuse Task Force ("CSATF") is a coalition of survivors, advocates, and professionals in New York who work with victims of gender-based violence. With the ubiquity of the internet and related technology, members of the CSATF are seeing an onslaught of cyber sexual abuse, including "revenge porn," hacking, impersonating, stalking, spoofing, harassment, identity theft, and others. The CSATF seeks to change that by (i) advocating for criminal and civil laws prohibiting the nonconsensual dissemination of sexual images and supporting victims of cyber sexual abuse; (ii) supporting advocates and attorneys representing victims of cyber sexual abuse by providing trainings, resources, and best practices;

[1] Pursuant to Local Rule 29.1, *amici curiae* inform the Court that all parties have consented to the filing of this brief. *Amici curiae* also confirm that (i) no counsel to any party authored this brief, in whole or in part; (ii) no party or party's counsel contributed money that was intended to fund preparing or submitting this brief; and (iii) no person — other than *amici*, their members, or their counsel — contributed money that was intended to fund preparing or submitting the brief.

and (iii) raising awareness about cyber sexual abuse and victims' rights through community and public outreach and education.

Day One is a New York–based organization that partners with youth to end dating abuse and domestic violence through community education, supportive services, legal advocacy and leadership development.

The Domestic Violence Legal Empowerment and Appeals Project ("DV LEAP") makes the law work for survivors of domestic violence by helping overturn unjust trial court outcomes, advancing legal protections for victims and their children through expert appellate advocacy, training lawyers, psychologists and judges on best practices, and spearheading domestic violence litigation in the Supreme Court. DV LEAP works to ensure that federal and state courts understand the realities of domestic violence and the law when deciding cases with significant implications for domestic violence litigants. DV LEAP has co-authored *amicus* briefs in numerous state courts and in the United States Supreme Court, on domestic violence, cyber abuse, and many related issues. DV LEAP is a partnership of the George Washington University Law School and a network of participating law firms.

Since 1993, Her Justice has been dedicated to making a real and lasting difference in the lives of low-income, underserved, and abused women by offering them legal services designed to foster equal access to justice and an empowered approach to life. Her Justice recruits volunteer attorneys from New York City's law

firms to stand side-by-side with women who cannot afford to pay for a lawyer, giving them a real chance to obtain legal protections that transform their lives. Approximately ninety percent of the women Her Justice serves receive full representation from a volunteer attorney, while the balance are represented by Her Justice staff attorneys. Her Justice provides legal services to over 3,000 women every year in all five boroughs of New York City. Informed by its work, Her Justice also promotes policies that make society more responsive to the legal issues confronting the women it serves.

Legal Momentum, the Women's Legal Defense and Education Fund, is the nation's oldest legal advocacy organization for women, www.legalmomentum.org. Legal Momentum advances the rights of all women and girls by using the power of the law and creating innovative public policy. For example, Legal Momentum was the leading advocate for the landmark Violence Against Women Act and its subsequent reauthorizations, which seek to redress the historical inadequacy of the justice system's response to domestic violence. Legal Momentum also represents victims of domestic violence who suffer housing and employment discrimination related to the violence. Legal Momentum has long been concerned with judicial decision-making in custody and visitation cases involving domestic violence. Legal Momentum has a particular interest in ensuring that the judicial system adequately protects the rights of victims of sexual domestic violence and their children.

My Sister's Place ("MSP") is a multi-disciplinary non-profit organization based in Westchester County, New York, that provides legal, counseling, and shelter services to survivors of domestic violence and human trafficking and their children. MSP's Center for Legal Services represents hundreds of clients every year in contested family law proceedings in Family Courts in White Plains, Yonkers, and New Rochelle, involving orders of protection, custody, visitation, and child support. In addition to these direct services, MSP's community advocacy program educates thousands of teens every year about healthy relationships.

Founded in 1990, the New York Legal Assistance Group ("NYLAG") is a not-for-profit organization dedicated to providing free civil legal services to New York's low income families. The Matrimonial & Family Law Unit of NYLAG provides legal consultation and representation to victims of domestic violence on a priority basis. In addition to obtaining orders of protection, NYLAG provides victims with representation in child protection, custody, visitation, child and spousal support, and both contested and uncontested matrimonial matters. NYLAG has particular expertise in complex child custody matters, including relocation and jurisdictional disputes. NYLAG has further demonstrated its commitment to promoting legal services for victims of domestic violence through its Domestic Violence Clinical Center ("DVCC"). The DVCC is an innovative program administered and supervised by NYLAG attorneys, which offers law students the

opportunity to learn the substantive and litigation skills necessary to provide exceptional representation to battered women. As such, NYLAG has a special degree of knowledge and expertise in litigating jurisdictional disputes and domestic violence matters.

Safe Horizon is the leading non-profit victim services agency in the United States. It touches the lives of more than 250,000 children, adults, and families affected by crime and abuse throughout New York City each year. It provides compassionate and expert trauma-informed programs and services for people who have experienced domestic violence, child physical and sexual abuse, rape, sexual assault, human trafficking, stalking and other forms of crime and abuse. Safe Horizon partners with governmental and other community agencies and also advocates for policies on a local, state, and national level on behalf of those affected by violence and abuse.

STATEMENT OF CASE AND SUMMARY OF ARGUMENT

Perpetrators of intimate partner violence are increasingly using online platforms or other digital technologies to exploit, harass, and threaten their victims. This type of abuse—sometimes referred to as "cyber abuse"—encompasses an array of harassment including, but not limited to, hacking, stalking, spoofing,[2] identity

[2] "Spoofing" is the disguising of a sender's identity so that the recipient believes the sender is someone else.

theft, impersonation, sexual extortion, and the dissemination of explicit images and videos. Perpetrators of cyber abuse, like many other forms of abuse, range from strangers to intimate partners. The harms caused by cyber abuse are pervasive and persistent, and can bleed into every aspect of a victim's life, seriously impairing the person's physical, emotional and economic well-being.

This case exemplifies the range and extent of harm that abusers using technology and online platforms can impose on their victims—harm that goes well beyond the online universe and has serious consequences for the safety and well-being of victims. Over a period of five months, Plaintiff-Appellant Matthew Herrick ("Herrick") was subject to an onslaught of dangerous harassment and stalking arising from a series of fake online profiles of Herrick created and posted by Herrick's former boyfriend (herein referred to as "JC"). The fake profiles of Herrick were developed and distributed (without Herrick's involvement or consent) on a popular, mobile dating application for gay, bisexual and queer men (the "Grindr App") owned and operated by Appellee Grindr, LLC. Grindr App users develop profiles communicating their age, height, weight, ethnicity, and photographs. Accessed on mobile "smart" phones, the key feature of the Grindr App is GPS technology that displays the profiles of other users in close geographic proximity to each other. Every one of the approximately 426,000 Grindr App users in the New York metropolitan area had the opportunity to view and potentially communicate

with the fake Herrick profiles posted by JC. First Amended Complaint, *Herrick v. Grindr, LLC*, No. 17-CV-00932 (VEC) (S.D.N.Y. Mar. 31, 2018), ECF No. 34 ("Am. Compl.") ¶ 29, Joint Appendix ("JA") 58. In the fake profiles, which appeared to the unknowing observer to have been created and posted by Herrick, JC repeatedly and falsely described Herrick as interested in rape fantasies, bondage, and other fetishes. Hundreds of Grindr App users who viewed the fake profiles and subsequently communicated with JC (pretending to be Herrick), sought to meet Herrick in person in order to pursue these interests. For months, Herrick's work and personal life became a living hell as at least 1,100 Grindr App users, directed by JC and the Grindr App, arrived at Herrick's home and his workplace demanding the as-advertised (by JC impersonating Herrick) sex. Am. Compl. ¶ 49, JA-65; *see also* Am. Compl. ¶¶ 54-62, JA-67-69. Herrick, and others on his behalf, made at least 100 complaints to Grindr, LLC, identifying the fake profiles and the harm they were causing Herrick. Grindr, LLC failed to meaningfully respond to or address these complaints. In contravention of its own published policies, Grindr, LLC did not remove the fake Herrick profiles, nor did it implement any safeguards to prevent new fake Herrick profiles from appearing. Am. Compl. ¶¶ 81, 83-86, JA-72-74. Had Grindr, LLC simply followed its own policies as advertised to Grindr App users, the months of dangerous and life-destroying harassment that Herrick suffered could have been avoided.

Given Grindr, LLC's lack of response, Herrick turned to the courts for relief. In November 2016, he filed for and received an Order of Protection against JC in Family Court prohibiting JC from harassing Herrick or impersonating him online. JC violated the Order of Protection repeatedly, and despite Herrick's reporting of these violations to the authorities, JC maintained his campaign of abuse, facilitated by the Grindr App. On January 27, 2017, Herrick filed suit against Grindr, LLC, along with its two corporate parents, KL Grindr Holdings, Inc. and Grindr Holding Company (collectively, "Grindr"), in New York state court, *Herrick v. Grindr, LLC*, No. 150903/2017 (Sup. Ct. N.Y. Cty. Jan. 27, 2017), alleging negligence, deceptive business practices, false advertising and numerous other torts. The court issued an *ex parte* temporary restraining order ("TRO") against Grindr, requiring Grindr to "immediately disable all impersonating profiles created under Plaintiff's name or with identifying information related to Plaintiff, Plaintiff's photograph, address, phone number, email account or place of work, including but not limited to all impersonating accounts under the control [of Plaintiff's malefactor]." TRO at 2, JA-42. Instead of complying with the TRO, Grindr ignored the court's order, removed the case to the Southern District of New York and moved to dismiss Herrick's complaint pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. The District Court granted Grindr's motion. *Herrick v. Grindr, LLC*, No. 17-CV-00932

(VEC), 2018 WL 566457 (S.D.N.Y. Jan. 25, 2018). Herrick appeals the District Court's order dismissing his complaint.

Technology companies have a unique role in the facilitation of abuse by perpetrators like JC. Grindr ignored multiple complaints about the abuse, failed to install safeguards to ward against it, allowed a known abusive user to maintain and create fake accounts for the purpose of harassing and stalking his victim, and facilitated the harassment and stalking through its geolocation feature. JC could not have perpetrated this campaign of abuse without Grindr's participation and knowing inaction. Accordingly, Grindr and technology companies like it have an obligation to prevent or stop the abuse perpetrated on their technology platforms.

ARGUMENT

I. TECHNOLOGY ENABLES NEW FORMS OF INTIMATE PARTNER VIOLENCE

A. Technological Abuse Comes in Various Forms and Causes Devastating Harms

Abusive intimate partners deploy technology in many different ways to exploit, harass, threaten, and stalk their victims. This conduct encompasses a range of activities, including (but not limited to) cyber sexual abuse,[3] monitoring an intimate partner's online activity, impersonating, spoofing, and creating and

[3] Cyber sexual abuse is a form of sexual exploitation and/or harassment that occurs on online platforms or through other digital technologies.

disseminating deep fakes.[4] As technology develops to make the internet more accessible and easier to navigate, it also provides abusers with the tools to engage in new and creative forms of abuse to terrorize their victims. For example, one increasingly common form of technological abuse is the nonconsensual disclosure, or threat of disclosure, of nude or sexually explicit images or videos via the internet or other technologies.[5] Perpetrators of this type of abuse often include personally identifying information (*e.g.*, full name, address, phone number) next to images of their victim that creates physical vulnerability. Publication of these details creates opportunities for untold numbers of others to stalk, harass, or assault victims in the real world as well as online.[6]

Online abuse is a particularly malignant form of abuse because of the lasting nature of digital images and content on the internet. Once published on the web,

[4] The term "deep fake" refers to digital manipulation of sound or images to impersonate another person and make it appear that the impersonated person did something, often of a sexual nature, that he or she did not actually do. Deep fakes are perpetrated in a manner that appears so realistic, an unaided observer cannot detect the fake.

[5] Mary Anne Franks, *Drafting An Effective "Revenge Porn" Law: A Guide for Legislators* (Sept. 22, 2016) at 2, https://www.cybercivilrights.org/wp-content/uploads/2016/09/Guide-for-Legislators-9.16.pdf (hereinafter "Revenge Porn Law"); Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L.R. 345, 346 (2014) (hereinafter "Criminalizing Revenge Porn").

[6] *Power in Numbers*, Cyber Civil Rights Initiative (Jan. 3, 2014), https://www.cybercivilrights.org/revenge-porn-infographic/ (hereinafter "CCRI Powers in Numbers") (of the victims CCRI surveyed, 59 percent reported their full name was published to websites, 49 percent their social network information, 26 percent their email address, 20 percent their phone number, 16 percent their physical home address, 14 percent their work address, and 2 percent their social security number). This practice of posting personal identifying details is known as "doxxing."

digital content is nearly impossible to completely remove.[7] Even if content is removed from one website, there is a high likelihood that it has already migrated elsewhere on the web, or was captured for posterity by "caching."[8] In addition, any number of third-party individuals can take screenshots to preserve the content or repost it elsewhere, making it virtually impossible for a victim to track down all the digital footprints of the abusive content.[9] Images or posts containing explicit or otherwise harmful material successfully removed from all websites retain another persistent harm: dead URLs[10] and links often remain online and available to search engines and search results.

Cyber abuse has a devastating impact on victims' mental health and emotional well-being, and affects people of all gender identities and sexual orientations.[11] One

---

[7] *See* Mitchell J. Matorin, *In the Real World, Revenge Porn Is Far Worse Than Making It Illegal*, TPM Media (Oct. 18, 2013, 2:00 AM), http://talkingpointsmemo.com/cafe/our-current-law-is-completely-inadequate-for-dealing-with-revenge-porn (explaining that civil litigation may provide compensation to revenge porn victims but it "won't remove the photos from the Internet or Google").

[8] "Caching" refers to hardware or software components that capture internet usage data. Future requests use the captured data in order to increase the speed of user access.

[9] Erica Souza, *"For His Eyes Only": Why Federal Legislation Is Needed to Combat Revenge Porn*, 23 UCLA Women's L.J. 101, 107 (2016).

[10] "URL" stands for Uniform Resource Locator. It is the protocol for specifying internet addresses. A URL is also known as the "link" to an internet page.

[11] Cyber abuse can be considered a form of cyberbullying, which has received national attention due to its immense impact on young people, particularly LGBT youth. Joseph G. Kosciw, Emily A. Greytak, Mark J. Bartkiewicz, Madelyn J. Boesen & Neal A. Palmer, *The 2011 National School Climate Survey: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth in Our Nation's Schools* (GLSEN, 2012).

survey by the Cyber Civil Rights Initiative shows just how harmful cyber abuse can be:

- Over ninety percent of victims experience severe emotional distress and anxiety;
- Fifty-seven percent of victims suffer anxieties about their professional reputation and employment prospects due to the abuse; and
- More than fifty percent of victims experience thoughts of suicide.[12]

By its nature, technology has the ability to accelerate harm rapidly, but the risk of perpetual harm from abuse via technology is the most sobering.[13] Cyber abuse victims experience repetitive trauma of the loss of personal dignity and respect of family, friends, and community, and they continuously suffer potential economic harm from adverse impact on their employment or employment prospects.[14]

---

[12] *See End Revenge Porn: A Campaign of the Cyber Civil Rights Initiative, Inc.*, Cyber Civil Rights Initiative (Dec. 2014), https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf (hereinafter "CCRI December 2014 Statistics"). *See also Online Reputation in a Connected World*, 1, 3, 8 (Jan. 2010), https://www.job-hunt.org/guides/DPD Online-Reputation-Research_overview.pdf (finding that nearly 80 percent of employers consult search engines to collect intelligence on job applicants, and, about 70 percent of the time, they reject applicants due to their findings). *See also* CCRI December 2014 Statistics (finding that 51 percent of victims have suicidal thoughts).

[13] *See* Asia A. Eaton, Holly Jacobs, & Yanet Ruvalcaba, *2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration*, Cyber Civil Rights Initiative (June 2017), at 24, https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf (hereinafter "CCRI 2017 Nationwide Online Study").

[14] *See* Charlotte Alter, *'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn*, Time.com, June 13, 2017, http://time.com/4811561/revenge-porn/.

B. Perpetrators of Intimate Partner Violence Often Employ Technology to Increase the Impact of Their Abuse

Often, as is the case here, intimate partners or former intimate partners, use technology to magnify their ability to stalk and harass their victims. By manipulating online applications and/or social media sites, abusers can reach vast numbers of people and use them as weapons against their victims. *Amici curiae*, who serve tens of thousands of intimate partner violence victims every year, have seen a rapid increase in perpetrators harnessing technology to use against their clients—this brand of abuse is a powerful new tool in the arsenal of intimate partner violence perpetrators. Just like other tactics typically used by perpetrators, abusers like JC use technology as a weapon to exert power and control, intimidate, humiliate, scare, coerce, harass, and threaten their victims.

For example, perpetrators of intimate partner violence often threaten online publication of intimate images in order to prevent their partners from leaving the relationship, reporting abuse and/or pursuing their legal rights in court.[15] Studies have found that at least ten percent of abusive ex-partners have threatened their victims with distribution of nude photographs or sexual content; sixty percent of those who make such threats follow through.[16]

[15] Criminalizing Revenge Porn, *supra* note 5, at 351.

[16] *CCRI Power in Numbers*, *supra* note 6.

Individuals who identify as lesbian, gay, or bisexual ("LGB") are more likely to have experienced cyber abuse than those who do not identify as LGB. Statistics from the Data & Society Research Institute and the Center for Innovative Public Health Research reveal that seventeen percent of LGB internet users in the U.S. have experienced threats or actual non-consensual image-sharing.[17] Women, too, are more likely to be victimized by cyber abuse, with one in ten women under the age of thirty reporting threats of cyber abuse.[18]

Amici curiae continue to observe the myriad ways that intimate partner abusers wield technology to control their victims. For example, the ex-boyfriend of one Sanctuary for Families client created fake Facebook accounts using the client's photo and name. The client did not have a Facebook account and so she was unaware and unable to monitor the impersonating accounts. Her abuser "friended"[19] the client's friends and family members, and proceeded to share intimate and sexually explicit photographs of her. In another matter for a different Sanctuary for Families client, the physically abusive husband of the client threatened that if she ever left the

[17] Amanda Lenhart, Michelle Ybarra & Myeshia Price-Feeney, *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of "Revenge Porn"*, Data & Society Research Institute & Center for Innovative Public Health Research (Dec. 13, 2016), https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf (hereinafter "Data & Society").

[18] *Id.*

[19] To "friend" in this context means to use a social media platform to reach and connect with other users.

husband, the husband would send intimate photos of her to her co-workers, family, and friends. When she escaped her husband, she did not escape his cyber abuse: he carried out his threat, and posted several naked images of her across social media. The publication of the images threatens not only the viability of her future employment, but also her privacy from such intimate exposure to friends and family, including her own children. She has no way of knowing where the images may have migrated. She lives in fear of who will find the images and what will happen when they do.[20]

II. PREVENTION AND PROTECTION AGAINST MODERN INTIMATE PARTNER DOMESTIC VIOLENCE TACTICS REQUIRE TECHNOLOGY COMPANIES LIKE GRINDR TO BE HELD RESPONSIBLE FOR FAILURES TO PROTECT USERS

A. As Technology Advances, It Is Increasingly Used to Control Victims of Intimate Partner Violence in New Ways

Abusers, unfortunately, will always exist; technology is just another weapon to use against their victims. The kind of abuse and stalking through Grindr that Herrick experienced is among the most accessible forms of abuse available—perpetrators of cyber abuse do not need to be physically violent nor do they need to be particularly skilled at using technology. All they need is an internet connection.

[20] Sanctuary for Families, Letter to Dr. Dubravka, Special Rapporteur on Violence against Women (Nov. 2, 2017).

Cyber harassment and abuse have expanded their reach as internet usage has become an integral part of daily life. In a 2014 Pew Research Center Study, seventy-three percent of adult internet users reported that they had witnessed cyber harassment. That same study found that forty percent of adult internet users had themselves experienced online harassment.[21] The number of internet users continues to rise, and studies have shown that the risks posed by cyber abuse have not diminished. In fact, a 2016 survey by the Data and Society Research Center found that approximately one in twenty-five Americans (approximately 10.4 million people) has experienced threats that an image will be posted without consent; one in ten American women under the age of forty has had someone post an image without permission, or threaten to do so.[22]

Many, if not most, technology companies with a business model based on web-based application platforms have the informational and structural capacity to either facilitate cyber abuse or to prevent and stop its occurrence. As discussed *infra*, other technology companies, faced with cyber abuse reports by Herrick, stopped the use of their platform to perpetrate abuse. Technology companies must be held accountable to their own terms of service which pledge to police inappropriate use of their technology when a user of their services is victimized.

---

[21] *See* Maeve Duggan, *Online Harassment*, Pew Research Center, Oct. 22, 2014, http://www.pewinternet.org/2014/10/22/online-harassment/.

[22] Data & Society, *supra* note 17.

B. Individual Victims Should Not and Cannot Address Technological Abuse Alone

Traditional recommendations that victims clear their phone data, delete their social media profiles, or simply just not take or share intimate photographs misconstrue the issue, and do not curb the problem of cyber abuse. Any person with a camera can edit an image to make it appear that a desired victim posed for an explicit picture, and any person with an email address and phone number can impersonate someone on a dating website. In addition, these types of "remedies" can increase the costs of cyber abuse. A victim's removal of his or her profile on social media platforms like Facebook, LinkedIn, and Twitter can impair his or her ability to obtain employment.[23] Further, without social media accounts, victims may have less ability to monitor whether their images or information are being used inappropriately.

The cooperation of technology companies in investigating, locating, and removing abusive content is critical to addressing cyber abuse; victims lack the tools to stem the spread of abuse, and they cannot do it alone.

Without technology companies' compliance with their own policies, even law enforcement is hamstrung in achieving justice for victims. The ease with which cyber abuse campaigns can be conducted, coupled with the complexity of forensic

[23] Seth Stevenson, *Popularity Counts*, Wired, May 2012, at 120, 122.

challenges in compiling evidence, mean that too often, law enforcement resources are insufficient to investigate and develop the evidence needed to charge and prosecute these crimes. Here, Herrick filed numerous police reports to no effect, and many months passed before JC was finally arrested and his egregious abuse halted. Consolidated Memorandum of Law in Opposition to Grindr LLC's, Grindr Holdings, Inc.'s & Grindr Holding Company's Motions to Dismiss, No. 17-CV-00932 (VEC) (S.D.N.Y. June 14, 2017), ECF No. 54, at 2 (hereinafter "Grindr Memo"). During those months, moreover, Herrick suffered substantial harm—harm that could have been avoided had Grindr just followed its own policies.

III. GRINDR FACILITATED INTIMATE PARTNER VIOLENCE ON ITS PLATFORM

A. The Grindr App Played a Critical Role in Facilitating Violence Against Herrick

The Grindr App actively generates mapping information and directs individuals toward one another for offline meetings. *See* Am. Compl. ¶¶ 3, 23-24, 31, JA-53, 57, 59. Here, pretending to be Herrick, JC used the Grindr App to create numerous impersonating profiles and interact with hundreds of users.

Grindr was of critical importance in facilitating and perpetuating violence against Herrick. Am. Compl. ¶¶ 52-62, JA-67-69. Once JC uploaded Herrick's pictures and various identifying information, the Grindr App connected JC's "Herrick" to hundreds of its users who could locate, harass, and abuse the real

Herrick. *See* Am. Compl. ¶¶ 49, 52-53, JA-65, 67. Grindr's algorithms led to the continuous display of JC's "Herrick," causing hundreds of Grindr App users—as many as 16 per day—to go to Herrick's home and his workplace, where they approached Herrick with the expectation of sex. Am. Compl. ¶¶ 5, 54, JA-54, 67. Given the advertisements of rape fantasies and fetishes, the online connections fostered by Grindr had significant potential to quickly (and all too easily) result in physical and sexual abuse. In fact, Herrick was stalked and harassed for months, his acting and modelling career prospects were doomed, and his roommate was assaulted by a "suitor" who refused to leave their apartment building. *See* Am. Compl. ¶¶ 64, 68-69, 94-95, JA-69-70, 75.

Grindr's participation took at least two forms: first, Grindr was negligent in creating a platform without safeguards for abuse; and second, Grindr inexplicably refused to respond to hundreds of complaints or heed a TRO, violating its own policies that, if followed, would have shut down abuse of this nature. *See* Grindr Memo, at 31. The functionality of the Grindr App and Grindr's willingness to ignore numerous complaints, and refusal to comply with a TRO and its own published policies, enabled JC to abuse Herrick in ways he could not have otherwise done as a single actor.

B. Grindr Had the Capacity to Prevent and Stop the Abuse

Given the numerous complaints made by Herrick and others, Grindr was on clear notice that Herrick was being abused by JC through the impersonating accounts on its platform, and that Herrick was in imminent and ongoing danger. Grindr chose to allow the abuse to continue and did nothing in response to the numerous complaints Herrick and others made through the Grindr App's complaint interface. Nor did Grindr respond to the complaints Herrick's counsel made directly to Grindr's counsel. Am. Compl. ¶¶ 8, 68-69, 81, JA-54-55, 70, 72.

Grindr's negligence did not stop there. As with its choice to ignore complaints by Herrick and others, Grindr also failed to maintain its content on the Grindr App in a way that demonstrates any reasonable or ordinary standard of care. As the operator of the Grindr App, Grindr provides content in the form of its geolocation algorithms. Am. Compl. ¶ 52, JA-67. These algorithms collect information from its millions of users (including 426,000 and growing in New York City alone) and connect various users based on location and other information in their profiles. Am. Compl. ¶¶ 29, 31, JA-58-59. It was these geolocation algorithms that allowed JC to stalk Herrick by sending a stream of third-party Grindr App users to Herrick's home and workplace.

Grindr, like many other technology companies, has the capacity to design (or purchase) and implement software to identify abusive content, allow anyone who

comes across an abusive post to report it, and suspend accounts of users who post prohibited content. For example, Twitter removes media when a victim complains, and will even remove images that victims may not yet be aware exist (*i.e.*, upskirt photos and hidden webcams). Once Twitter identifies the original poster of non-consensual nudity, that user is suspended immediately.[24] Twitter is not alone. Facebook also has policies to safeguard its users on all its platforms from cyber abuse.[25]

Grindr, too, has the ability to flag and remove prohibited or harmful content. There are a variety of available safety protocols like PhotoDNA technology, geofencing, and duplicate-detection software. Am. Compl. ¶¶ 79-85, JA-72-74. Similarly situated platforms have routinely blocked abusers like JC to protect the safety of victims. Am. Compl. ¶ 45, JA-64. In fact, in addition to his use of Grindr as a platform for abusing Herrick, JC used another app called "Scruff." On Scruff, JC also impersonated Herrick and arranged sexual encounters. When Herrick contacted Scruff (much the same as he contacted Grindr), Scruff's operators immediately and effectively handled the situation. Within 24 hours, Scruff located

[24] @TwitterSafety, *A Calendar of Our Safety Work* (updated Nov. 17, 2017), https://blog.twitter.com/official/en_us/topics/company/2017/safetycalendar.html.

[25] Niraj Chokshi, *Facebook Announces New Ways to Prevent "Revenge Porn*," N.Y. Times, Apr. 5, 2017, https://www.nytimes.com/2017/04/05/us/facebook-revenge-porn.html (reporting on Facebook's announcement to use artificial intelligence tools designed to keep nonconsensual explicit posts off all of its platforms, including Facebook, Instagram and Facebook chat).

and removed the offending profiles, and banned the IP addresses as well as the specific devices from which the profiles originated. Complaint, dated January 27, 2017, ¶ 26, JA-18. Grindr, absurdly, has taken the position that it, a larger and more widely used platform than Scruff, does not have the capacity to protect its users in these ways—or in any way—at all. *See* Am. Compl. ¶¶ 82, 86, JA-73-74.

The Grindr App generates ample profits that are more than sufficient to enable Grindr to install protections against abuse, which the Grindr App's policy specifically purports to provide. *See* Am. Compl. ¶¶ 27, 35-36, 40-43, JA-57, 60, 62-64. Moreover, other cyber platforms that function in the same marketplace as Grindr employ staff to respond to user complaints, identify offending users and within 24 hours are able to locate and remove offending profiles, ban IP addresses, and even ban specific devices from creating new profiles. Am. Compl. ¶ 45, JA-64. If smaller companies can safeguard users from abuse, so too, can Grindr. *See id.*

CONCLUSION

For the reasons stated above and by Herrick, *amici curiae* respectfully urge the Court to reverse the order of the court below dismissing Herrick's claims.

Dated: May 31, 2018

Respectfully submitted,

MILBANK, TWEED, HADLEY, & McCLOY LLP

By: /s/ *Stacey J. Rappaport*

Stacey J. Rappaport
Nicole C. Nielson
28 Liberty Street
New York, New York 10005-1413
Phone: (212) 530-5000
Fax: (212) 822-5347
srappaport@milbank.com

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT TYPEFACE REQUIREMENTS, AND TYPE-STYLE REQUIREMENTS

1. This document complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f):

   ☒ this document contains 4,523 words

2. The document 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 document has been prepared in a proportionally-spaced typeface using Microsoft Word 2013 in 14-point Times New Roman.

Dated: May 31, 2018

MILBANK, TWEED, HADLEY, & McCLOY LLP

By: /s/ *Stacey J. Rappaport*

Stacey J. Rappaport
28 Liberty Street
New York, New York 10005-1413
Phone: (212) 530-5000
Fax: (212) 822-5347
srappaport@milbank.com

Counsel for Amici Curiae