

Law, Privacy, and Online Dating: “Revenge Porn” in Gay Online Communities

Ari Ezra Waldman

Nonconsensual pornography, commonly known as “revenge porn,” is the dissemination of another’s sexually explicit images or videos without their consent. This article explores this phenomenon in gay and bisexual male online communities. The first part reviews the current sociological and legal literature on online dating, gay culture on the Internet, and revenge porn. Then, based on a survey of gay and bisexual male dating app users, ethnographic interviews, and an analysis of platform content moderation policies, the next part makes three related points. First, it shows that gay and bisexual men who use geosocial dating apps are more frequently victims of revenge porn than both the general population and the broader lesbian, gay, and bisexual community. Second, it shows that geosocial dating apps create powerful norms of disclosure that make sharing personal information all but required. And third, it describes how gay and bisexual male users engage in privacy navigation techniques with the goal of building trust and enhancing safety. The final substantive section then shows how inadequate protections for online privacy and inadequate legal incentives for safe platform design contribute to the problem of revenge porn. The article concludes with a summary and avenues for future research.

INTRODUCTION

4 percent of US Internet users—nearly 10.4 million people—have been threatened with or victimized by the nonconsensual distribution of sexually explicit images in which they are identifiable, a phenomenon commonly known as “revenge porn” or “nonconsensual pornography.”¹ The problem is worse among sexual minorities. According to the Data & Society Research Institute, 15 percent of lesbian, gay, and bisexual (LGB) Internet users report that someone has threatened to share their explicit images; 7 percent say someone has actually done it (Lenhart, Ybarra, and Price-Feeny 2016).

Ari Ezra Waldman is a Professor of Law and Director of the Innovation Center for Law and Technology at New York Law School. He is also an Affiliated Fellow at the Information Society Project at Yale Law School. You can reach him at ari.waldman@nyls.edu.

The author would like to thank Danielle Keats Citron, Mary Anne Franks, Andrew Santa Ana, Elisa D’Amico, Luke Boso, Scott Skinner-Thompson, Kate Klonick, Amanda Levendowski, and Paul Schwartz. Maverick James provided essential research assistance. This article was presented as the 11th Deirdre G. Martin Memorial Lecture on Privacy at the University of Ottawa, Faculty of Law. The research was supported by a New York Law School Summer Research Grant and was approved by the New York Law School IRB.

1. The terms “revenge porn” and “nonconsensual pornography” are sometimes used interchangeably, although the former is more popular. The latter is more accurate because not all nonconsensual sharing of sexually explicit media is done out of revenge (Franks 2015; Waldman 2017). Because this article does not focus on nomenclature, it follows the lead of the scholarly literature and uses both “revenge porn” and “non-consensual pornography.”

Evidence on the ground points to a growing problem, particularly among gay and bisexual men who use geosocial dating apps, where much image sharing occurs. In May 2017, for example, two North Carolina high school students created a fake profile on Grindr, the popular gay-oriented geosocial app. They solicited nude photographs from one of their teachers and distributed the pictures throughout the school. The teacher was first suspended and then transferred elsewhere in the district (Towle 2017). Matthew Herrick, an openly gay man living in New York City, alleged in a recent lawsuit that an ex-boyfriend stole his intimate images, impersonated him on an app, shared his photos with other men, and ultimately sent 1,100 of those men to Herrick's home and workplace looking for sex (O'Brien 2017; *Herrick v. Grindr*, Opinion and Order, 17-CV-932 (VEC) (S.D.N.Y. Jan. 25, 2018)). And in ongoing ethnographic research over the last two years, many of the thirty-seven gay men and eighteen lesbians to whom I have spoken who use geosocial apps also report striking stories of extortion for explicit images, race-based sexual harassment, impersonation (also known as "catfishing"), and revenge porn.

These stories raise important research questions as yet unanswered in the sociolegal literature. Are LGB users of geosocial dating apps more likely than the general population or other LGB individuals to be victims of revenge porn? If so, why do users share graphic or explicit images in the first place, and how do they navigate their privacy in disclosure-heavy environments like dating apps? And what can this data tell us about the role of law and platform design in online safety?

This article begins to answer these questions. A survey of 917 mostly gay male and bisexual² users of geosocial dating apps and follow-up ethnographic research offers new insight into our understanding of nonconsensual image sharing and privacy management in one subset of queer communities. These data show that gay and bisexual male users of geosocial apps are more than twice as likely as LGB persons generally to be victimized by revenge porn. Despite this, and a recognition of the risks inherent in disclosure, users still frequently share graphic or explicit images of themselves because the norms of the platforms demand it. In such contexts, users deploy several privacy navigation techniques, including anonymizing photos, developing a rapport through conversation, reciprocal sharing, and mutual surveillance, in an attempt to organically build trust and enhance safety.

But self-help can only go so far. Revenge porn occurs frequently on gay male-oriented dating apps despite sophisticated efforts on the part of users to identify trustworthy social partners. Based on survey and ethnography data, an analysis of geosocial app rules and reporting procedures, and interviews with app executives, I argue that no matter how sophisticated privacy navigation techniques become, gaps in the ecosystem of privacy and Internet law, including privacy tort law, copyright law, criminal law, and the law of platform responsibility governed by section 230 of the Communications Decency Act, fail to incent privacy-enhancing platform design, thus making revenge porn a feature, not a bug, of online social spaces.³

2. This project began with the intent to study lesbian, gay, and bisexual male and female users of geosocial dating apps. The final data set did not include a sufficient number of lesbians and bisexual women to include in the quantitative analysis. This is an area for future research that will require more nuanced research design to reach these, as well as transgender and self-identifying queer, populations.

3. I use the term "design" broadly, to capture the technological architecture, user interface, aesthetics, and internal policies and reporting procedures of a social platform. This definition is based on a long history

There is no perfectly safe place online. Even comprehensive federal and state laws and private ordering cannot always account for bad social behavior. But in a modern social world in which sharing is, if not mandatory, expected, law and design have a role to play in making digital spaces safe for everyone.

ONLINE SOCIAL SPACES: THEORETICAL LITERATURES AND NEW TECHNOLOGIES

As multiactor information-sharing environments (Goffman 1959), online dating apps are uniquely modern social spaces. They can be physical or face-to-face, as Goffman presumed, or digital (Cohen 2000, 2008; Gibbs, Ellison, and Heino 2006; Bullingham and Vasconcelos 2013). Social spaces can be big or small, and they can involve the exchange of words or body language (Siegman and Feldstein 1987; Mondada 2016). At their most basic, though, social spaces are constructed by persons engaged in information exchange. Online dating apps involve the exchange of a variety of pieces of information, including basic demographic data, sexual interests, and, at times, graphic or revealing images. Though shared in specific contexts for specific purposes (Nissenbaum 2010), some of those images are further disseminated without the individual's consent.

It is, therefore, worth studying online dating apps as sites of revenge porn for several reasons. First, geosocial dating platforms are widely used. Three-fifths of Americans think the Internet is a good way to meet people (Smith and Anderson 2016), a number likely higher today. Fifteen percent of American adults have used online dating Web sites or mobile apps, with use among young adults ages eighteen to twenty-four tripling in the two years between 2013 and 2015 (Smith 2016). And, as of 2014, more than 50 million people had Tinder profiles (Bilton 2014). Much of the growth in online dating over the past few years has been in the mobile app sector, or platforms designed to be used on smartphones. In 2013, only 5 percent of eighteen- to twenty-four-year-olds reported using mobile dating apps; by 2015, that number had jumped to 22 percent (Smith and Anderson 2016). All of these numbers are likely to grow.

A second reason to study dating apps from a sociolegal perspective is that they are designed to promote and facilitate the free disclosure of intimate images and other personal information. On some apps, users answer basic questions about their age, physical attributes, and preferences, and write the profile themselves. On others, like Tinder, user profiles are populated by linking to a valid Facebook account. Some apps go further than a brief profile paragraph. OkCupid “ask[s] interesting questions to get to know you on a deeper level.” The platform then uses a “super-smart algorithm” to match compatible users based on the answers to those questions. But personal images are the bread and butter of geosocial dating apps. Sometimes presented in a grid based on proximity or as a single picture that fills most of the smartphone screen, photos are the first, and sometimes only, thing other users see. Although all platforms allow users to add information to their profiles, including name, age, physical characteristics, and

of design literature, including Norman (1988), and the more recent privacy by design scholarship, including Hartzog (2018).

“About Me” notes, pictures are at the center of these profiles. As is sharing pictures over and above the profile image. Beyond the first picture, platforms are designed to allow users to upload at least six photos, with some including space for hundreds of images.⁴

Third, by incorporating geolocation technology (hence the portmanteau “geosocial”) to not only identify potential matches nearby, but also to tell users their relative proximity to those matches—“Dave is 1,500 feet away,” for example—these apps remind us that our embodied, phenomenological social experiences are simultaneously digital and physical (Cohen 2007, 2012). This is true in several ways. Apps like Tinder and OkCupid are overtly predicated on transferring to the physical world a social connection that originated online. Otherwise, there would be no difference between a dating app and an anonymous chat room; the point is to chat online, develop a rapport, and then meet in person. Geosocial apps also invite digital interactions, but move with their users in physical space, allowing users to see the relative distance between them and their prospective matches and giving users different matches depending on their location. Users can, therefore, find community nearby in the physical world or classify potential matches based on their locations. And the technology arguably impacts the quality of social interaction in the physical world. Some social scientists argue that geosocial technologies commodify intimacy, making it a transactional, repetitive experience involving “swiping,” texting, and sex (Bauman 2003; Badiou 2012). The social scientist Sherry Turkle (2011) has also warned that digital technologies, generally, are transforming lives in peculiar and compulsive ways: smartphones that give us constant access to e-mail are often the first things we pick up and the last things we put down at night. Despite these concerns, geosocial dating apps represent an important microcosm of modern social life, particularly with respect to the ways in which technology mediates our interactions with others. It makes sense, then, to join scholars of the sociology of technology (Cowan 1987; Woolgar 1990; Wajcman 1991; Kline and Pinch 1996; Bijker, Hughes, and Pinch 2012) to study these new technologies and their place in a rapidly evolving social space.

A fourth reason to study dating apps is that individuals who identify as gay and bisexual frequently deploy these apps to meet others who share their identities. There are hundreds of gay-oriented dating apps.⁵ According to one study, dating app users who identified as heterosexual opened their apps eight times per week and used them for seventy-one seconds at a time. Gay and bisexual men, on the other hand, averaged twenty-two times per week for ninety-six seconds at a time. One app, Grindr, reported that in 2013, more than 1 million users logged in to the app every day and sent more than 7 million messages and 2 million photos (Groves et al. 2014). There may be several reasons for this, not the least of which is that digital spaces offer social opportunities when stigma and discrimination make face-to-face interaction difficult (Stein 2003). Social engagements on these apps are also expressions of sexual and romantic

4. This number was determined by selecting the most popular queer-oriented geosocial dating apps in three categories—for gay men, for lesbians, and for both—and setting up mock profiles in each. The apps selected were Tinder, OkCupid, Chappy, Grindr, Scruff, Jack’d, Hornet, HER, JustShe, LesbianPersonals, and Hinge. Most of these platforms allowed users to upload up to six pictures.

5. A keyword search of “gay dating” on App Annie, an app analytics service, revealed 1,500 relevant apps. That number is likely overinclusive.

freedom after decades of marginalization. Some even argue that they facilitate a form of self-pornography and eroticism (Tziallas 2015).

Indeed, there is a vast social science literature investigating gay experiences with digital dating. For example, scholars have studied why gay men start and stop using geosocial apps (Brubaker, Ananny, and Crawford 2016). Others have studied how users manage their presentation and develop impressions about others based on their profiles (Blackwell, Birnholtz, and Abbott 2015; Miller 2015a). Still others have studied the impact of traditional gender roles on the kinds of images gay men share and their judgments of others (Albury and Byron 2014). There is also a large related literature about how to leverage LGB uses of these platforms for public health purposes, like stopping the spread of HIV (Wohlfeiler et al. 2013; Whitfield 2017). None of this scholarship appears to focus on revenge porn. Therefore, studying privacy invasions on these apps, all of which are designed to encourage, facilitate, and sometimes require the sharing of images and personal information, will not only add to a growing interdisciplinary research agenda, but also help scholars understand how marginalized populations may face unique privacy burdens (Gilliom 2001; Bridges 2011; Citron 2014; Skinner-Thompson 2015).

Users of dating apps already face heightened privacy risks. Grindr shared its users' HIV status with third parties for years (Ghorayshi and Ray 2018). Farnden, Martini, and Choo (2015) found that Grindr sends all profile images unencrypted across its network. User locations are also sent from devices to the Grindr server with country and city data as well as exact longitude and latitude of the users. The researchers noted that combining this information with a time stamp could allow someone to track users in real space. On Badoo, which is identical to the Blendr app, the researchers were able to collect profile names, chat histories, nearby users, profile information, and device information. And on Tinder, the most popular dating app in the United States, researchers retrieved exact user locations, profile images, and all message history. The potential dissemination of this kind of information could uniquely harm queer populations, especially those in need of the protection of anonymity or the closet (Stern 2016).

Finally, dating apps and revenge porn sit at the intersection of several relevant and overlapping scholarly literatures in law, privacy, and sociolegal theory. Nonconsensual image sharing implicates at least four areas of law. Privacy tort law operates when personal information is disseminated widely or obtained via a breach of implied trust (Waldman 2017). Copyright law gives photographers the rights to stop the reproduction of their images and to force platforms to take down pictures uploaded without their consent (Levendowski 2014). The criminal law has been increasingly deployed by states and localities to address nonconsensual pornography (Citron and Franks 2014). And the prospect of moderating third-party conduct uploaded to Web sites implicates the law of platform liability (Klonick 2018) and section 230 of the Communications Decency Act, which immunizes online platforms from the tortious conduct of third-party users (Citron and Wittes 2017). These regimes can either work together to help eradicate revenge porn or fail to operate to protect victims at all.

Revenge porn also highlights basic questions about how we conceptualize privacy in the digital age. Some scholars understand privacy to be about separating from the prying eyes of others (White 1951; Shils 1966; Bok 1983; Rosen 2001). Others argue that privacy is about choice, autonomy, or control over our information (Westin 1967;

Fried 1968; Inness 1992; Cohen 2001; Matthews 2010). There are many other conceptions of privacy.⁶ But revenge porn challenges the strength and staying power of many traditional theories of privacy. Victims often freely and voluntarily shared their intimate photos with another person, but many of them also did so with the expectation that those images would not be further disseminated. Traditional conceptualizations of privacy, however, often struggle to recognize that a privacy interest can exist after such disclosure. Solove (2004) calls this the “secrecy paradigm,” and it is forcing scholars to rethink privacy in a world where digital technology makes revenge porn possible. In that context, social conceptions of privacy make more sense (Post 1989; Strahilevitz 2005; Nissenbaum 2010) and, in particular, an approach to privacy based on trust, where trust facilitates disclosure by mitigating the vulnerabilities inherent in sharing (Waldman 2018a), may protect victims of revenge porn most effectively. The breadth and timeliness of applicable legal and philosophical questions speaks to the need for lawyers, policy makers, and legal scholars to understand the phenomenon of revenge porn and identify the best way to deploy law to combat it.

GAY AND BISEXUAL MALE ONLINE COMMUNITIES AND NONCONSENSUAL IMAGE SHARING: QUANTITATIVE AND QUALITATIVE RESEARCH

More specifically, in light of the prevalence of geosocial dating apps in gay communities, the salient role that personal photos play on those apps, and the need for data-driven law and policy to combat online harassment, it is worth studying whether widely reported anecdotal evidence of nonconsensual image sharing on gay-oriented apps is backed by hard evidence. If it is, we can then learn from the experiences of these geosocial app users to help create safe social spaces online.

Research Questions

First, are gay and bisexual male users of geosocial dating apps more frequently threatened with or victimized by nonconsensual image sharing than either the general population or other LGB persons? Data show that roughly 3 percent of Americans who use the Internet have had someone threaten to post their intimate photos online; 2 percent have actually had someone do it. Those numbers jumped to 15 percent and 7 percent, respectively, among LGB persons (Lenhart, Ybarra, and Price-Feeney 2016). Given the frequency with which gay and bisexual men share intimate images on geosocial apps, it stands to reason that the rate of victimization may increase among similarly situated geosocial app users.

Second, why do individuals share intimate images on these platforms? What are the social forces that encourage sharing on these apps, despite the risks involved? Understanding when and why individuals share personal information with others is part of a larger research agenda that suggests, among other things, that context matters when

6. There are many other approaches to privacy. For summaries of those theories, see Solove (2010), Waldman (2018a).

making disclosure decisions (Grimmelmann 2009; John, Acquisti and Loewenstein 2011; Acquisti, John, and Loewenstein 2012). The disclosure norms of gay-oriented geosocial dating apps, however, have been inadequately studied.

Third, if geosocial app users share much personal information, how and to what end do they mitigate the vulnerabilities associated with disclosure? Answering these questions may give us insight into privacy navigation techniques among a community with high disclosure norms and tendencies. It may also show, as I argue later, that platform design and law have important roles to play in making online social spaces safe for sharing.

Research Design and Methodology

To answer these and related research questions, I designed a survey with a yes/no, Likert scale and open-ended questions. The survey is attached as [Exhibit A](#). I followed up that survey with semistructured interviews with selected participants and included data from interviews I previously conducted with other gay, lesbian, and bisexual users of geosocial apps.

A Facebook advertisement was purchased to disseminate the survey. The ad was targeted to Facebook users around the world who identified as lesbian, gay, bisexual, transgender, or queer using various focusing techniques. The survey also made clear that it was only to be completed by queer users of geosocial dating apps. The ad ran for one week, received 137,545 impressions, and reached 87,167 people, which resulted in 387 responses. To grow the sample set, a link to the survey was also placed on a series of LGB-oriented Web sites. A total of 834 valid responses were included in the final analysis.

The survey first asked participants for basic demographic information, including sex, gender identity, sexual orientation, age, relationship status, education level achieved, and location. The survey then listed some of the most popular queer-oriented geosocial dating apps and asked participants to check which, if any, they use. Survey participants also noted their primary purposes for using the apps they chose; their options ranged from chatting and making friends to relationships and sex. The survey then asked for participants' experiences with sharing photos on these platforms. Because personal perceptions of what words like "graphic" or "explicit" mean could vary among respondents, the questions made clear that one was asking about "nude" photos and the other was asking about shirtless or otherwise "revealing" but not explicit photos. Several questions asked about users' perceptions and expectations when they share photos, including perceptions of trust, whether they care about further dissemination of their photos, and whether they feel compelled to share. An open-ended question followed that allowed participants to explain their answers in more detail. The final section of the survey asked about participants' revenge porn experiences, including threats and actual posting or dissemination.

At the end of survey, participants were given the option to include their e-mail addresses for follow-up questions. Thirty participants who provided some responses to open-ended questions were chosen for follow-ups. This was not a random sample; it was not intended to be. These conversations, which included a guarantee of anonymity

or pseudonymity, were intended to tease out more detail about the particular responses these participants had already given. Rather than generalizing from these interviews to entire populations, the interviews clarified and expanded upon particular themes already identified in the quantitative data.

These interviews supplemented similar semistructured interviews I conducted with LGB geosocial app users over the last two years. Some of the questions, which mirrored some of the questions in the survey, are attached at Appendix B. The interviews did not, however, include only these questions; follow-up questions were asked based on responses. Interviewees were identified in various ways: first by standing at popular street corners in LGBTQ-friendly neighborhoods in New York City, San Francisco, and Los Angeles and soliciting participants during midday (12:00 p.m. to 2:00 p.m.) on several weekdays; then, by setting up a researcher profile on several of the apps and both soliciting participants and receiving inquiries; and finally, through respondent-driven sampling (Heckathorn 1997; Gile and Handcock 2010). Efforts were made to ensure diversity on age, race, and gender metrics.

Data and Discussion

The survey received 936 total responses. Three were excluded because they were incomplete. A further sixteen were excluded as duplicates, leaving 917 valid responses. Of those, 834 identified as male ($n = 834$), two respondents identified as “non-binary” (including genderqueer or gender fluid), and one participant answered “prefer not to say.” Because of the small sample size of lesbian or bisexual women ($n = 80$), this analysis focuses on the experiences of gay and bisexual men. Additional research is still necessary to better understand the experiences of lesbians and bisexual women on geosocial dating apps. That said, quantitative analysis based on a large sample set of gay and bisexual men nevertheless adds to a literature on nonconsensual image sharing that has to date mostly ignored queer communities. Exactly 80.9 percent of the entire sample ($n = 834$) identified as cisgender; the vast majority of the balance (18.9 percent) did not identify as transgender, but rather chose not to respond. There were 804 gay men and 29 bisexual men in the sample studied. One respondent identified as “queer.” Age ranges reflected a roughly normal distribution. The sample was also highly educated: 685 (82.1 percent) graduated college, attended some graduate or professional school, or graduated with an advanced or professional degree. Respondents resided predominantly in the United States, Europe, and Canada, with a small minority in South America. The survey did not classify respondents by city or geography (Hardy and Lindtner 2017).

Research Question 1: Gay and Bisexual Male Experiences with Nonconsensual Image Sharing on Geosocial Dating Apps

As presented in Table 1, among respondents who identified as male ($n = 834$), including gay and bisexual men, 14.5 percent report that someone on a geosocial dating app has distributed or made public their sexually revealing or explicit photos without

their consent. That is approximately double the rate of revenge porn incidents reported by LGB persons in general (Lenhart, Ybarra, and Price-Feeney 2016). Notably, logistic regression reveals no statistically significant correlation between demographics like age and education level, on the one hand, and reporting being a victim of nonconsensual image sharing, on the other.

TABLE 1.
Nonconsensual Image Sharing among LGB Persons
on Geosocial Mobile Dating Apps (% of respondents)

	Threats	Distribution
Men	5.8	14.5

Gay and bisexual men report having their intimate images distributed without their consent at far higher rates than they report receiving revenge porn threats: 14.5 percent and 5.8 percent, respectively. The latter number is more than half the rate of the general LGB population (Lenhart, Ybarra, and Price-Feeney 2016). But traditionally, threats of revenge porn are more frequent than actual nonconsensual image sharing. According to Elisa D'Amico, a partner at the law firm K&L Gates and founder of the Cyber Civil Rights Legal Project, the firm's in-house revenge porn clinic where she has litigated seven years of revenge porn cases, threats are common because "perpetrators of revenge porn usually want something: money, to stay in a relationship, or more photos. And some do it out of passion or anger."⁷ That means that these results could be aberrations; as with all social science research based on relatively small sample sets, these results should be verified with subsequent surveys.

It is also possible that higher rates of actual revenge porn may speak to the unique experiences of gay men on geosocial dating apps. As Eduard R., a gay male geosocial app user who was told by a friend that his intimate photos were posted on Tumblr, a multimedia microblogging platform, said, "There are so many images just sent around, I think guys feel willing to take them just as easily. Why bother threatening it? I don't think the guy that did it had any personal vendetta against me. He saw a body he liked and, like an asshole, spread it around."⁸ Thomas P., another gay male victim of revenge porn, said that he thinks "gay men have a pretty lax approach to shirtless pics or nudes. It doesn't occur to some of them that someone with a great body would not want it all over the internet."⁹ This sentiment—that someone with an attractive physique who shares intimate photos either wants or should have no problem with the further spread of his photos—was echoed by ten other interviewees. If generalizable beyond this specific group of respondents, this suggests that some gay men who use geosocial dating apps do not understand the privacy invasion inherent in sharing graphic images without consent, whatever the images' subjects look like (Citron and Franks 2014; Waldman

7. Elisa D'Amico (Partner, K&L Gates), interview by Ari Ezra Waldman, January 18, 2018, via phone.

8. Eduard R., interview by Ari Ezra Waldman, December 27, 2017, via phone.

9. Thomas P., interview by Ari Ezra Waldman, January 3, 2018, via phone.

TABLE 2.
Sharing Images on Geosocial Mobile Dating Apps
 (% of respondents)

	Explicit	Revealing
Men	87.4	93.4

TABLE 3.
Predictors of Sharing Images on Geosocial Apps

	Explicit	Nonexplicit
Expectations of Confidentiality	1.7*	2.0*
Sharing Necessary	1.8*	1.7*

*Sig. < .005

2017). Later I address some of the ways in which law and the platforms themselves contribute to this problem.

Research Question 2: Gay and Bisexual Male Disclosure Behavior on Geosocial Dating Apps

Approximately 87.4 percent of survey participants ($n = 834$) have shared “graphic, explicit, or nude photos or videos” of themselves on geosocial dating apps; 93.4 percent have shared “shirtless or otherwise revealing” photos of themselves. This data is displayed in Table 2. It is clear that a substantial amount of intimate image sharing happens on these platforms. Such disclosures happen in the context of specific norms and expectations. For example, 89.7 percent agreed or strongly agreed that they share images with the expectation that they will not be shared further. Exactly 82.6 percent of survey participants either agreed or strongly agreed with the statement: “Sharing photos is pretty much a necessary part of the process of meeting people on these apps.”

A logistic regression analysis was also performed to determine the effect of user expectations on sharing behavior. Those who agreed with the statement that they share images with the expectation that they will not be shared with others were 1.7 times more likely to share explicit images and 2.0 times more likely to share nonexplicit but revealing images than others. Similarly, those who felt that sharing images was necessary to use geosocial apps and meet other people were 1.8 times more likely to share explicit images and 1.7 times more likely to share nonexplicit but revealing images than those who disagreed.¹⁰ These results, all of which were statistically significant, are reported in Table 3.

10. For explicit image sharing, the model was statistically significant ($p < .005$), explained 17 percent (Nagelkerke R^2) of the variance in sharing behavior, and correctly classified 89.1 percent of the cases. For nonexplicit image sharing, the model was also statistically significant ($p < .005$), explained 20 percent (Nagelkerke R^2) of the variance in sharing behavior, and correctly classified 94.2 percent of the cases.

Responses to open-ended survey questions¹¹ and interviews with gay and bisexual male users of geosocial apps teased out four common and sometimes overlapping explanations for such high levels of sharing on these platforms. First, many agreed with survey respondents that sharing intimate or explicit images is impliedly necessary. Stephen P., a gay app user from Boston, noted that “if you don’t share photos, you can’t really participate.”¹² A respondent who chose not to be identified said the same thing: “If I don’t [send], then I don’t get a response.” Matt N., who met his husband on Scruff, a gay geosocial app, stated that “there’s an expectation; gays want to see what you’re offering.”¹³ Put another way, as Adam A. saw it, “We’re basically peacocks showing our plumage so that the other person will be interested in us. It’s pretty basic.” Eleven other responses to the survey reiterated this point. A related series of responses suggested users were resigned, almost nihilistic, about the cultural norms among gay and bisexual men that encourage explicit image sharing. Jason R. admitted that “it’s the culture; [it’s] hard to avoid.” “It’s just what’s done,” another said. Ted S. responded similarly: “Sharing photos seems to be essential to maintaining interest. I wish it weren’t the case, but whatever.” Resignation to sharing intimate photos ran through ten responses and five other interviews of gay and bisexual men.

Second, sharing verifies identity, especially on platforms that only allow users to see one picture of others. As one user who chose to remain anonymous noted, “chatting with people necessarily involves a visual component, and indeed chatting online (and potentially over long distances) doesn’t alter people’s desire to engage with one another by ‘knowing’ who they’re taking to by seeing them.” Another anonymous respondent stated that “sending my photos and receiving the photos from the person I’m chatting with helps reduce the chance that someone is misrepresenting or impersonating someone else.” Another stated that “photos help prove that you are who you say you are.” One respondent felt that sharing photos “is part of the game, so to speak. I’m not comfortable meeting people who don’t have pictures. We are all on devices that have cameras, not using them makes meeting the person seem ‘risky.’” Twenty-nine others said something similar. Therefore, although some users are resigned to the importance of image sharing, others see picture exchange as a safety mechanism when interacting online.

Third, if users want to see what others look like, they have to share first. “I share,” J.P. responded, “because I want to receive [their] photos back.” There is a social dance on many of these apps with respect to image sharing. As discussed *infra*, many gay men try to mitigate the risks associated with sharing intimate pictures by waiting for the other user to share first. As Ryan D. colorfully stated on the survey, social interaction on geosocial apps is the “same . . . as when we were little boys. I’ll show you mine if you show me yours.” Too much of that strategy would make sharing stop. Sharing continues, these interviews suggest, because the reciprocity norm remains strong. Eighteen respondents agreed with J.P.’s assessment.

11. Any statements not directly cited to an interview refer to survey participant responses to open-ended questions. The survey made clear that there was a possibility these responses would be used in publication. All respondents have been pseudonymized or anonymized, per their preference.

12. Stephen P., interview by Ari Ezra Waldman, August 11, 2015, San Francisco.

13. Matt N., interview by Ari Ezra Waldman, December 12, 2017, via phone.

Seven participants described a fourth reason for sharing intimate images: body positivity and sexual freedom, echoing the work of Phillips (2015) and Miller (2015b). Neil F. said, “I am absolutely not ashamed of my body, so I’m happy to share it. I may not look like what ‘society’ thinks I should look like, but that’s everyone else’s problem.” J.M. said, “skin is just skin.” Jared K., who says he used many different dating and “hook up” apps over the last five years, stated that “almost all of them allow gay men to explore their sexuality. We can be safe and we can be open and positive about who we are and what we want. Given what previous generations of queer men and women went through, there is exactly nothing wrong with that.”¹⁴ Sexual empowerment and the desire for sex, among other factors, likely also contribute to user disclosure behavior, and it is worth studying the relative impact of each of these and other factors that influence sharing. But these data suggest that many of these forces work together to create powerful organic disclosure norms that pervade gay dating app culture.

Research Question 3: Privacy and Risk Mitigation Strategies on Geosocial Dating Apps

Despite these powerful forces encouraging disclosure and despite accepting that sharing intimate pictures is a necessary part of social interaction on geosocial apps, most gay and bisexual male users are nevertheless concerned about their privacy. More than 68 percent of respondents care if their images are shared with others. Moreover, just under 70 percent agreed or strongly agreed with the statement that they share photos “with the expectation that the person I send them to will not share them with anyone else.” As G.M. noted, echoing Erving Goffman (1959), “sharing these photos is a calculated risk.” They balance the benefits of sharing—conformance to norms, social connection, sexual exploration, and so forth—against the vulnerability and risks that attend intimate image sharing (Palen and Dourish 2003; Richards and Hartzog 2016). Recognizing those risks, most users seek to mitigate them. Interviews and answers to open-ended questions suggest that these participants use four strategies to reduce risk inherent in sharing personal information.

First, thirty-eight respondents reported that they anonymize their photos. In particular, many send intimate images without their faces or without identifying characteristics, at least initially. Or they will send identifiable nonintimate pictures, but only cropped explicit photos. Or they will only send photos that they “wouldn’t be embarrassed by if [they] were made public.” This strategy reduces the risk of harm if the pictures are shared or posted online. Second, twenty-two respondents only share photos, graphic or otherwise, after “chatting with the other person” for some time—ranging from a few hours to a few weeks—sufficient to “develop a rapport” or, as Jared S. responded, “feel somewhat comfortable with the other person.” At some point, one anonymous respondent noted, “you begin to trust the person and let your guard down.” Third, as noted above, several respondents only share intimate photos after another user has shared with them, maintaining power in a social exchange for as long as possible and relying on reciprocity and mutual vulnerability to reduce the likelihood of bad behavior (Berg, Dickhaut, and McCabe 1995;

14. Jared K., interview by Ari Ezra Waldman, October 15, 2017, via phone.

Brin 1999; Kahan 2003). As Ben Z. noted, “reciprocity is the norm, but I like to be the one to reciprocate. It makes me feel more comfortable because the other person has already put himself out there. He’s more at risk than I am, right?” And then, after reciprocation, users rely on a form of mutually assured surveillance. “I’m sharing photos of myself, some with my shirt off that I wouldn’t necessarily want to get home to nana. But, so is he. He’s in it just as deep as I am.” Fourth, some rely on the comfort and familiarity in an app’s exclusive queer-ness. Stephen P. said: “[Y]ou go on Grindr and you trust that everyone realizes we’re all in this together. We’re all gay, all of us looking for companionship.”¹⁵ John H. noted, unintentionally echoing Max Weber’s (1946) argument that a common religion allowed for trustworthy contracting in the early American republic and Talcott Parsons’ (1978) argument that cultural similarity inspires trust, that “someone who is also gay, also about the same age, also single, also lonely, also looking for the same thing you’re looking for, just seems less likely to hurt you than someone else who doesn’t share the same personal narrative.” Thirty-eight survey respondents made similar comments. Not all of these mitigation strategies are successful. But their use suggests a high level of privacy sophistication in an environment with powerful disclosure norms.

One tool for mitigating the risks associated with sharing intimate images—platform surveillance and punishment—was largely absent from participant responses to the survey’s open-ended questions. Follow-up interviews and interviews with app users who did not participate in the survey revealed one potential reason why: in cases where users have been victimized by violations of app terms of service—racism, harassment, or revenge porn, for example—at least some platforms appear virtually absent. Ben Z. stated that an ex-boyfriend of his has been impersonating him on Grindr and that he has “told Grindr . . . at least 5 or 10 times, . . . but they’ve done nothing.” Other interviewees report platforms taking little to no interest in enforcing their rules, particularly about racist profiles. Racism is rampant on gay-oriented geosocial apps (Callander, Holt, and Newman 2012; Callander, Newman, and Holt 2015; Robinson 2015). “I had gotten so used to seeing ‘no Asians’ or even ‘no rice,’” Timothy Y. reported. “But at some point I just started reporting them. Nothing ever happened. I would keep seeing the same white men in my neighborhood with the same racist comments. They were never taken down.”¹⁶ Oliver C. noted that he is “a proud Gaysian. No one can make me not proud to be who I am. But when these apps say they don’t allow racist profiles, but then obviously allow half the white guys in this town to say ‘no chocolate, no rice’ or ‘no fats, no fems, no Asians’, you know what they really care about: numbers, not the rules.”¹⁷ Lack of responses from platforms was a common theme in six of the interviews. Granted, many of these examples involve racism, not revenge porn. However, a platform that tolerates opportunistic, asocial, and hateful behavior creates a welcoming environment for other types of mischief.

Limited Data on Lesbians and Bisexual Women

The data set included too few women to add to the small literature on dating app experiences of lesbians and bisexual women (Murray and Ankersen 2016; Duguay 2017).

15. Stephen P. interview.

16. Timothy Y., interview by Ari Ezra Waldman, August 12, 2015, San Francisco.

17. Oliver C., interview by Ari Ezra Waldman, September 18, 2017, New York.

Nor did the survey reach more “hidden” or hard to reach populations of sexual minorities, including those who identify as transgender, queer, gender fluid, or intersex, among others. Future research can fill this gap, although different survey techniques may be necessary.

That said, of the twelve women in the sample who had met someone on a geosocial dating app who threatened to distribute their sexually graphic images, seven of them were bisexual, six of whom had been threatened by men.¹⁸ A similar pattern held for those victimized by revenge porn: three of the five women were bisexual, and all of their harassers were men.¹⁹ We already know that the vast majority of perpetrators of revenge porn are men, and the majority of victims are women (Eaton 2017; Franks 2017). Although the sample set includes too few women to make strong conclusions, this study lends credibility to the idea that, as with heterosexual women, revenge porn is a gendered phenomenon among bisexual women.

What’s more, gender hierarchies and traditional dynamics may still pervade even apps geared toward those seeking same-sex relationships. Every lesbian interviewed expressed concern about privacy on dating apps. As Jaclyn M. explained, “I’m not showing anything sexual for a while, not until I really trust the person.”²⁰ And one respondent who chose to remain anonymous but identifies as a lesbian on dating apps noted that she “still get[s] messages from men all the time, and they’re harassing messages where they either want pictures of me with another queer woman or say ‘how can you really be a lesbian’ or ‘you don’t like dick, that’s crazy.’ I’ve basically stopped using them.” Although more research is required to determine if these feelings and behaviors are common among lesbians and bisexual women, these limited data points suggest that current platform design inadequately restricts predatory behavior that could harass and silence sexual minorities on geosocial apps.

Limitations

The survey did not classify respondents by self-identified race or ethnic origin, focusing solely on sexual orientation. Surveys that require participants to self-report may be subject to response biases. Survey participants often feel pressure to give answers that are socially acceptable or that they think the survey drafter wants to hear. Response biases may also be more pronounced when dealing with sensitive topics like sharing explicit images online. The conclusions we can draw from the ethnographic portion of this study are necessarily limited. Qualitative interviews with a small subset of survey respondents are not meant to stand in for the entire data set, let alone the population at large. Rather, they can add context to quantitative results and speak to the experiences of the interviewees alone.

18. Stephanie T., interview by Ari Ezra Waldman, November 27, 2017, via phone; Madison B., interview by Ari Ezra Waldman, November 27, 2017, via phone; Sarah M., interview by Ari Ezra Waldman, November 29, 2017, via phone; Maria M., interview by Ari Ezra Waldman, December 6, 2017, via phone; Solara, interview by Ari Ezra Waldman, December 8, 2017, via phone; Karyn P., interview by Ari Ezra Waldman, January 4, 2018, via phone; Helen F., interview by Ari Ezra Waldman, January 4, 2018, via phone.

19. Daniella S., interview by Ari Ezra Waldman, December 27, 2017, via phone; Rebecca T., interview by Ari Ezra Waldman, January 9, 2018, via phone; Alexi N., interview by Ari Ezra Waldman, January 14, 2018, via phone.

20. Jaclyn M., interview by Ari Ezra Waldman, January 10, 2018, via phone.

LAW, TRUST, AND SAFE SOCIAL SPACES

Despite these limitations, these quantitative and qualitative data show that gay and bisexual men who use geosocial dating apps are more likely than the general population and other sexual minorities to have their intimate images taken and shared without their consent. The data also show that powerful, organically derived norms of disclosure make sharing intimate images all but required on these apps. As a result, even though many users trust that their images will not be further disseminated, many simultaneously engage in a series of strategies and tactics that mitigate the risks that come with sharing sexually explicit or otherwise revealing pictures of themselves. But risk mitigation strategies do not always work. Even when they do, the risk of privacy harms remain.

It would be easy to chastise victims themselves for continuing to share in unsafe circumstances: if we do not want our images to be posted to Tumblr—if we do not want to be at risk—we should not share photos we find potentially embarrassing in the first place (Goldman 2013). It would be just as easy to blame online dating as a whole, based as it is on the presentation of self through pictures. Neither argument is fair or persuasive. Victims of nonconsensual image sharing are not asking to have their privacy invaded; they are merely engaging in an important facet of modern social life that is governed, organically and by design, by powerful norms of disclosure. And suggesting that online dating as an institution is itself to blame for revenge porn is just another form of victim blaming (Citron 2013; Franks 2013). Plus, not all users and platforms are the same: among gay and bisexual men, almost every reported incident of nonconsensual image sharing occurred on one platform, Grindr. It is, therefore, neither the victim's fault nor that of online dating itself. Rather, some social spaces are safe, and some are not. I argue that platform design and privacy law play important roles in creating, or undermining, online safety.

Design

The design of built environments powerfully yet subtly influences, restricts, and directs behavior within those environments. This includes the design of everyday places and things (Norman 1988), technology hardware (Woolgar 1990), and online spaces (Cohen 2007; Hartzog 2018), just to name a few. Participants, too, play important roles in the social construction of these environments (Kline and Pinch 1996; Bijker, Hughes, and Pinch 2012).

With respect to geosocial apps, design includes both the back-end coding that operates behind the scenes and the front-end user interface that defines user interactions with the platform. Therefore, design considerations in this context include things like default privacy settings, ephemeral messaging, spaces for photographs, the ease with which users can report hostile profiles, accessibility of legal terms, and any baked-in friction to interaction, like pop-ups, warnings, and in-app purchase requirements, just to name a few. For example, some apps, like Tinder, only allow users to see one person at a time, whereas some gay-oriented geosocial dating apps, like Grindr, are designed to populate the screen with a series of thumbnail images of potential partners based on

their location. An app may design limits to that process by automatically populating only twenty other users, requiring the user to swipe, click, or pay for an upgrade to see more options (Blackwell, Birnholtz, and Abbott 2015). Apps can be designed to categorize users by body type, interests, and sexual preferences. They can be designed in ways to make rules and regulations obvious (pop-ups in plain language, for example) rather than inaccessible, as in a privacy policy only available on an associated Web site. To determine the role of design, I compared two of the more popular platforms among the gay and bisexual men in the survey: Grindr and Scruff. Almost every survey participant that reported either being threatened with or victimized by the nonconsensual distribution of their intimate images noted that the incident happened on Grindr. This makes sense. The two companies' approaches to violations of terms of service diverge.

The platforms' terms of service are roughly identical. Both Grindr and Scruff ban nudity, X-rated pictures, images of sex acts, racist imagery or text, and pictures of anyone underage, among many other things. They ban harassment, abuse, defamation, obscenity, and fraud. They ban commercial uses and advertisements. They reserve the right to ban, both temporarily and permanently, users who violate any of the platforms' rules.

The difference is in design and enforcement. According to its founder, Eric Silverberg, Scruff decided early on to "create a safe space for our members through vigorous content moderation." That is evident in the numbers and in the company's structure. More than half of Scruff's twenty-eight employees sit on its customer support team. That team is diverse, representing different genders, backgrounds, sexual orientations, and geographies. They are trained and updated on new norms and policies. Scruff's policy is to respond to every complaint within forty-eight hours; it almost always responds within twenty-four hours. The company's head of support sits in an office with the engineering team to ensure "a tight feedback loop" and "responsive process without friction," echoing scholarly recommendations that legal and engineering teams must be closely linked to enhance user privacy and safety by design (Waldman 2018b). And the company reacts decisively: "We have a zero-tolerance policy for stealing pictures or impersonating and we show it." Scruff also designs in easy reporting. The button to report violations is obvious and "the entire support ecosystem exists within the app: users do not have to include e-mail addresses on third-party platforms and receive responses within the app."²¹

Scruff is also designed so users can easily flag profiles that are offensive or violate platform rules. And according to Andrew Santa Ana, the Director of Litigation for the nonprofit organization, Day One, and the Faculty Supervisor for the Cyberharassment Clinic at New York Law School,²² flagging can be effective, but only if the platform is responsive. When "a client emails us that some image or video has gone up" without their consent, we assign a team—more than one person—to "flag the item and, if we can, explain why."²³ In her experience representing

21. Eric Silverberg (Founder & CEO, Scruff), interview by Ari Ezra Waldman, January 9, 2018, New York.

22. New York Law School is also the author's home institution.

23. Andrew Santa Ana (Director of Litigation, Day One), interview by Ari Ezra Waldman, January 17, 2018, via phone.

victims of nonconsensual image sharing, Elisa D'Amico has recognized the importance of designing safety procedures to be understandable and user friendly. "It can be difficult for victims or navigate reporting procedures [inside an app]. You have to get to the right screen to trigger removal of a photo, and to do that you need to find the right button to press or right question to answer. Sometimes, those questions are confusing."²⁴ As a result, D'Amico and her team of lawyers handle flagging and reporting for their clients. Santa Ana's and D'Amico's experiences, which they caution are limited with respect to dating apps, nevertheless suggests that companies can design effective reporting tools and respond to complaints to reduce the prevalence of nonconsensual image sharing on their platforms.

Joel Simkhai, the founder of Grindr, did not sit down for an interview. But what we know about Grindr is telling. In follow-up interviews with 10 of the 120 gay and bisexual male survey respondents who stated they were threatened with or victims of revenge porn, six reported notifying Grindr about the offending account, only to never hear back.²⁵ All interviewees reported seeing the offending account still active even after multiple reports and e-mails to Grindr's support team. Grindr's reporting mechanism is also less intuitive and harder to navigate. When trying to report a harassing account, for example, Grindr requires users to write an open-ended explanation, creating friction in the process. This friction, like a speed bump on a road, makes traversing the reporting mechanism more difficult, which makes it less likely that users will report offensive accounts in the first place (McGeeveran 2013). Seven interviewees reported a different experience with Scruff: one called interaction with Scruff's support team "easy and helpful" after a cyberstalking incident;²⁶ another said, "they were great when I found a fake account with my boyfriend's pictures. They took the account down immediately."²⁷

Law

This divergence in enforcement exists because the law allows it. Indeed, the entire ecosystem of privacy and Internet law—including privacy tort law, copyright law, criminal law, and the law of platform liability—fails to protect intimate disclosures online.

Tort Law

Even though revenge porn is, primarily, an invasion of privacy, privacy tort law is mostly incapable of helping. One of the so-called privacy torts (Prosser 1960), the tort of public disclosure of private facts, seems most applicable to revenge porn. It holds

24. Elisa D'Amico (Partner, K&L Gates LLP), interview by Ari Ezra Waldman, January 17, 2018, via phone.

25. Eduard R. Interview; Thomas P. Interview; Daniel M., interview by Ari Ezra Waldman, November 29, 2017, via phone; Steve E., interview by Ari Ezra Waldman, November 30, 2017, via phone; Kevin T., interview by Ari Ezra Waldman, December 1, 2017, via phone; Henry L., interview by Ari Ezra Waldman, December 1, 2017, via phone.

26. Nathan W., interview by Ari Ezra Waldman, October 17, 2017, via phone.

27. Ed. T., interview by Ari Ezra Waldman, October 11, 2017, via phone.

liable anyone who “gives publicity to a matter concerning the private life of another . . . if that matter publicized . . . (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public” (Restatement (Second) of Torts, § 652D). The tort of false light captures those who publicize something false or misleading about another when they know or should have known that the false way in which the victim is portrayed would be highly offensive to a reasonable person (Restatement (Second) of Torts, § 652E). The tort of intentional infliction of emotional distress allows individuals to recover for severe emotional distress caused by another who intentionally or recklessly acted to cause harm in an “extreme and outrageous” way (Restatement (Second) of Torts, § 46). There is also the tort of breach of confidentiality. This tort holds liable those who, without consent, disseminate information disclosed to them in a context they knew or should have known included expectations of confidentiality, discretion, and trust, thus harming the victim (Waldman 2017).

Although they sound promising, these causes of action are inadequate. Practically, civil litigation is expensive, making it inaccessible to all but a few victims. And court interpretations of the public disclosure tort in particular make it difficult to deploy. Many courts equate the tort’s “private life” requirement with secrecy, thus putting the tort out of reach for revenge porn victims who took the photos themselves and voluntarily shared them with another person. Scholars have discussed and critiqued the approach at length (Solove 2004; Strahilevitz 2005; Waldman 2018a; Hartzog *forthcoming*). But privacy tort law and privacy constitutional law are rife with it (*Gill v. Hearst Pub. Co.*, 253 P.2d 441, 444 (Cal. 1953); *United States v. Miller*, 425 U.S. 435, 443 (1976); *Smith v. Maryland*, 442 U.S. 735, 744 (1979); *Florida Star v. B.J.F.*, 491 U.S. 524, 527 (1989)). The victim, the argument goes, not only shared her picture with someone else, making the photograph no longer private, but also the act of sharing constituted consent for others to see it (Citron and Franks 2014). Moreover, as Scott Skinner-Thompson (*forthcoming*) has showed, the public disclosure tort has been used to greater effect by people of privilege than by plaintiffs from marginalized groups. It is, therefore, not clear that a public disclosure claim can consistently support the search for justice for gay and bisexual male victims of revenge porn.

The tort of false light is likely inapplicable to nonconsensual image sharing. Perpetrators may publicize something about another person, but it is hard to argue that sharing an identifiable photograph of another, even one that invades their intimate privacy, portrays them in a way that is false (Levendowski 2014). And although nonconsensual pornography may undoubtedly cause a victim to experience severe emotional distress, proving such harm to a court is difficult. The false light tort also misses revenge porn cases where the perpetrator’s goal was sex or money, not emotional harm. Moreover, the tort of breach of confidence in the United States has traditionally been restricted to just a few special relationships, including doctor-patient and bank-customer relationships (*Peterson v. Idaho First Nat’l Bank*, 367 P.2d 284, 290 (Idaho 1961); *Alberts v. Devine*, 479 N.E.2d 113, 120 (Mass. 1985)). This ecosystem of civil liability claims is, therefore, ill-equipped to support organic trust and address the problem of revenge porn on geosocial apps.

Copyright Law

A second legal regime that offers inadequate support for necessary trust norms on geosocial dating apps is copyright law. Nonconsensual image sharing is also a copyright violation. As one scholar has noted, “[c]opyright establishes a uniform method for revenge porn victims to remove their images, target websites that refuse to comply with takedown notices and, in some cases, receive monetary damages” (Levendowski 2014, 426). And several leading practitioners have used copyright law to take down images of their clients from revenge porn Web sites (Goldberg and D’Amico 2015). If the image distributed was a “selfie,” that is, taken by the victim herself, copyright law gives her the same exclusive rights it gives all photographers—namely, the rights, in relevant part, to prevent the reproduction, public display, and public distribution of that image without her consent. In addition, the notice-takedown-and-counter-notice procedure outlined in section 512 of the Copyright Act should provide a “clear, step-by-step pathway for removing revenge porn from the Internet, the result victims often want the most.”²⁸

Like privacy tort law, however, copyright law is an incomplete response to nonconsensual image sharing: not all distributed images are selfies; many of the images on geosocial dating apps that become fodder for revenge porn are taken by someone else, including friends and professional photographers. And, as Citron and Franks (2014) argue, copyright law lacks the ability to condemn nonconsensual pornography as morally wrong. Merely conceiving of revenge porn as theft has a limited expressive effect.

Criminal Law

Nor can criminal law help all victims. There is, as yet, no federal revenge porn criminal law in the United States. But even though forty-one states,²⁹ the District of Columbia,³⁰ and the City of New York³¹ (and probably more by this time this article

28. Elisa D’Amico, e-mail exchange with Ari Ezra Waldman, December 19, 2017.

29. Ala. Code § 13A-6-240 (West 2015); Alaska Stat. Ann. § 11.61.120 (West 2015); Ariz. Rev. Stat. § 13-1425 (Supp. 2015); Ark. Code Ann. § 5-26-314 (Supp. 2015); Cal. Penal Code § 647 (West Supp. 2016); Colo. Rev. Stat. Ann. § 18-7-107 (West Supp. 2015); Conn. Gen. Stat. Ann. § 53a-189a (West 2012 & Supp. 2016); Del. Code Ann. tit. 11, § 1335 (2015); Fla. Stat. Ann. § 784.049 (2015); Ga. Code Ann. § 16-11-90 (West Supp. 2015); Haw. Rev. Stat. § 711-1110.9 (2014); Idaho Code Ann. § 18-6609 (West 2016); 720 Ill. Comp. Stat. Ann. § 5/11-23.5 (2015); Iowa Code Ann. § 708.7 (West 2015); Kan. Stat. Ann. § 21-6101(8) (West 2016); Ky. Rev. Stat. § 531.120 (West 2018); La. Rev. Stat. Ann. § 14:283.2 (2004 & Supp. 2016); Me. Rev. Stat. Ann. tit. 17-A, § 511-A (West Supp. 2015); Md. Code Ann., Crim. Law § 3-809 (West Supp. 2015); Mich. Comp. Laws Ann. §§ 145e, 145f (West 2016); Minn. Stat. Ann. § 617.261 (2017); Mo. Rev. Stat. §§ 573.110, 573.112 (West 2018); Nev. Rev. Stat. Ann. § 200.780 (West 2015); N.H. Rev. Stat. Ann. § 644:9-a (West 2016); N.J. Stat. Ann. § 2C:14-9 (West 2015); N.M. Stat. Ann. § 30-37A-1 (West 2015); N.C. Gen. Stat. Ann. § 14-190.5A (2015); N.D. Cent. Code Ann. § 12.1-17-07.2 (Supp. 2015); Okla. Stat. Ann. tit. 1040.13b (2016); Or. Rev. Stat. Ann. Ch. 379 § 1 (2015); 18 Pa. Cons. Stat. Ann. § 3131 (2015); R.I. Gen. Laws ch. 11-64-3 (2018); S.D. Codified Laws § 22-21-4 (West 2015); Tenn. Code Ann. § 39-17 (West 2016); Tex. Penal Code Ann. § 21.16 (West Supp. 2016); Utah Code Ann. § 76-5b-203 (West 2016); Vt. Stat. Ann. tit. 13, § 2606 (West Supp. 2015); Va. Code Ann. § 18.2-386.2 (2014); Wash. Rev. Code Ann. § 9A.86.010 (West 2016); W. Va. Code Ann. § 61-8-28a (West 2016); Wis. Stat. Ann. § 942.09 (2013-2014).

30. D.C. Code Ann. §§ 22-3051–57 (West 2016).

31. N.Y.C. Int. No. 1267 (enacted December 12, 2017).

is published) have passed criminal laws prohibiting revenge porn, many of these laws miss harassing behavior (Franks 2017). For example, twenty-one revenge porn laws require that the act be done with the specific intent to harass or intimidate the victim or for financial gain.³² Maryland requires plaintiffs to prove that their harassers intended to cause “serious emotional distress.”³³ Not only is posting such images with reckless disregard for such harm perfectly legal under the Maryland statute, but proving a specific malicious intent is difficult and misses the point that revenge porn is first and foremost an invasion of privacy. Arkansas’s law only applies to people in relationships.³⁴ Georgia’s law requires that the nonconsensual sharing of explicit content “serve[] no legitimate purpose to the depicted person,” which appears to presume that revenge porn can have legitimate ends.³⁵

Intermediary Liability

There is no intermediary liability for revenge porn on their platforms. Our approach to the legal responsibilities of online platforms is still to some extent governed by the cyberlibertarians who dominated early Internet scholarship (Goldsmith and Wu 2008; Franks 2009) and by the first few online speech cases in the federal courts. Early on, the Internet was seen as a true marketplace of ideas, unencumbered by legal restrictions, antiquated social norms, or even our bodies. John Perry Barlow (1996) called the Internet “a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.” Eugene Volokh (1995) wrote that the Internet would empower end users, allowing them to bypass intermediaries and filters, like Rupert Murdoch and the publisher of the New York Times. Kathleen Sullivan (1998) agreed, arguing that since the Internet was available at home, at cybercafés, or in public libraries, there would be more speakers and more listeners, and more things said and heard.

Congress and the courts cemented these strong free speech norms with passage and subsequent interpretations of section 230 of the Communications Decency Act, which governs platform responsibility law today. The provision, which immunizes Internet platforms from lawsuits associated with third-party content on their sites, was passed to preserve the Internet as “a forum for a true diversity” of views “with a minimum of government regulation,” and to maintain “the vibrant and competitive free market

32. Ala. Code § 13A-6-240(a) (West 2015); Alaska Stat. Ann. § 11.61.120(a) (West 2015); Ariz. Rev. Stat. § 13-1425(A)(3) (Supp. 2015); Ark. Code Ann. § 5-26-314(a) (Supp. 2015); D.C. Code Ann. § 22-3052(a)(3) (West 2016); Iowa Code Ann. § 708.7(1)(a) (West 2015); Kan. Stat. Ann. § 21-6101(a)(8) (West 2016); La. Rev. Stat. Ann. § 14:283.2(A)(4) (2004 & Supp. 2016); Me. Rev. Stat. Ann. tit. 17-A, § 511-A(1) (West Supp. 2015); Mich. Comp. Laws Ann. §§ 145e, 145f (West 2016); Nev. Rev. Stat. Ann. § 200.780(1) (West 2015); N.M. Stat. Ann. § 30-37A-1(A)(1) (West 2015); N.C. Gen. Stat. Ann. § 14-190.5A(b)(1)(a) (2015); Okla. Stat. Ann. tit. 1040.13b(B)(2) (2016); Or. Rev. Stat. Ann. § 163.472(1)(a) (2015); 18 Pa. Cons. Stat. Ann. § 3131(a) (2015); S.D. Codified Laws § 22-21-4 (West 2015); Tex. Penal Code Ann. § 21.16(c) (West Supp. 2016); Vt. Stat. Ann. tit. 13, § 2606(b)(1) (West Supp. 2015); Va. Code Ann. § 18.2-386.2(A) (2014); W. Va. Code Ann. § 61-8-28a(b) (West 2016).

33. Md. Code Ann., Crim. Law § 3-809(C) (West Supp. 2015).

34. Ark. Code Ann. §§ 5-26-302(1)(A), 5-26-314(a)(2) (Supp. 2015).

35. Ga. Code Ann. §§ 16-11-90(b)(1), (b)(2) (West Supp. 2015).

that presently exists for the Internet” (141 Cong. Rec. H8460-01 (August 4, 1995)). Congress’s other purpose was to encourage platforms to take self-regulatory steps to enhance safety. But, in interpreting the clause, federal courts gave Web sites broad immunity, leaving them no legal incentive to police the bad behavior of their users. In *Zeran v. America Online*, 129 F.3d 327, 330 (4th Cir. 1997), for example, the Fourth Circuit noted that lawsuits against providers for third-party content would risk “freedom of speech in the new and burgeoning Internet medium.” The *Zeran* court stated that “Section 230 was enacted, in part, to maintain the robust nature of Internet communication, and accordingly, to keep government interference in the medium to a minimum” (330). This and other broad decisions created an online world where platforms have no legal incentive to stamp out nonconsensual image sharing and where perpetrators do not fear the consequences of their actions (Franks 2017).

Mr. Silverberg, who took on extensive moderation responsibilities for his company, admitted that he did not have to; the law did not require it. Scruff decided on its own to take safety seriously. Online social spaces that benefit from corporate leadership committed to moderation can become safe despite the lack of a strict legal requirement. Kate Klonick (2018) shows that online social networks have market incentives to eliminate hate and harassment from their platforms. Public pressure can make a difference even as we recognize how much power these platforms have over us. But the lack of legal remedies and legal incentives puts users at risk. Gaps in the law have downstream effects, allowing platforms to prioritize numbers over safety and ignore the needs of their users.

Law Reform

A natural response to these gaps in the law is law reform. This can take multiple paths. Legislatures, including the US Congress, should follow Franks (2017) and criminalize revenge porn. Specifically, Franks recommends that such a statute make clear that

[a]n actor may not knowingly disclose an image, [reproduction, or video] of another person who is identifiable from the image itself or information displayed in connection with the image and whose intimate parts are exposed or who is engaged in a sexual act, when the actor knows or recklessly disregards the risk that the depicted person did not consent to the disclosure (1292).

In this context, “disclose” refers to “transferring, publishing, distributing or reproducing.” “Intimate part” should be defined specifically to include “naked genitals, pubic area, anus, or female adult nipple of the person” and “sexual act” includes, but is not limited to, “masturbation; genital, anal, or oral sex; sexual penetration with objects; or the transfer or transmission of semen upon any part of the depicted person’s body” (720 Ill. Comp. Stat. § 5/11-23.5(b)(1)–(3) (2015); Franks 2017).

That said, the prospect of criminalization may raise concerns among queer communities. After all, the criminal law has long been leveraged to subordinate and discriminate against LGBTQ persons and other sexual minorities (Rubin 2011). And laws that criminalized gay male sexual activity also had the effects of both keeping

gay populations hidden and justifying other forms of discrimination and harassment, all of which are tools of subordination (*Bowers v. Hardwick*, 478 U.S. 186 (1986); Eskridge 1997).

Nevertheless, criminalization makes sense for two related reasons. First, revenge porn is one among the many pernicious ways in which sex, intimacy, and physical bodies can be weaponized to subordinate and discriminate against marginalized populations. As Citron (2014) and others (Allen 1988; MacKinnon 1988) have shown, social norms about sexual “modesty,” social and professional environments, structures around gender stereotypes, and online platforms that value the free speech rights of men over the safety and privacy of women, for example, contribute to the subjugation and silencing of women. Leveraging stereotypes of gay men as promiscuous, sex-driven, and predatory marginalizes and otherizes them, as well (Eskridge 2000; Boso 2017). In similar ways, because it transforms otherwise private persons into sexual objects for others, revenge porn makes victims’ public personae one of sexual promiscuity, and thus diminishes, stigmatizes, and subjugates its victims (Citron 2014). Nonconsensual pornography, then, deserves social condemnation, and the criminal law may be the only effective response with the sufficient expressive effect to change society’s expectations about what is and what is not appropriate behavior online (Citron 2009).

Second, the mere fact that the criminal law has been manipulated in the past to reinforce traditional hierarchies and gender norms does not necessarily mean we should give up on the power of criminal sanctions entirely. For example, it is true that the law once allowed husbands to beat their wives (*State v. Rhodes*, 61 N.C. 453 (1868)) and codified stereotypes of women as victims and subservient to their husbands. But modern criminal laws against sexual assault, harassment, and rape, all of which are gender-neutral, do the opposite. They promote the idea that our bodies are our own, and cannot be used sexually without our consent (Citron and Franks 2014).

Modest reform to section 230 immunity can also help. As Danielle Citron and Benjamin Wittes (2017) argue, conditioning platform immunity on reasonable efforts to combat unlawful activity will not “break this Internet.” Privacy tort law can be reinvigorated by discarding the false notion that privacy is the same as secrecy. Rather, if we understood information privacy as protecting relationships of trust—trust between social sharers creating expectations of confidentiality and discretion—it would be relatively easy to recognize that an intimate image shared between sexual partners for a specific purpose on a specific platform is not public or fair game for anyone to see (Waldman 2018a). These changes would facilitate socially beneficial expression in a modern, digital world in great need of it.

Law reform need not exist in a vacuum, of course. Given that gay-oriented geosocial dating apps have already been leveraged for public health campaigns to fight the spread of HIV and sexually transmitted infections (Wohlfeiler et al. 2013; Whitfield 2017), the same tools can be used to fight privacy invasions. As discussed above, some incidents of revenge porn affecting gay and bisexual men occur because perpetrators may not realize that sharing a picture of someone they find attractive is also an invasion of privacy. Public education, in the form of public service advertisements on dating platforms, local government-sponsored online safety campaigns, and school-centered privacy education curricula can, therefore, supplement legal changes that incent safety-enhancing design, thereby creating tools to combat revenge porn from all sides.

CONCLUSION

Not all of us use geosocial dating apps, let alone apps geared toward the gay community. But we all live in a world where social interaction occurs online. And yet, despite digital mediation of our social lives, the law leaves us at risk for bad and opportunistic behavior online. This article explored that phenomenon in detail, using a case study of revenge porn on geosocial dating apps. It showed, first, that gay and bisexual male users of these apps are far more likely than both the general population and other sexual minorities to report that they have been victims of revenge porn. More specifically, quantitative and qualitative research suggested that dating apps maintain powerful norms of disclosure. That research also suggested how dating app users navigate those norms—namely, through organically built trust and risk mitigation techniques.

The empirical and theoretical contributions of this article have implications beyond the narrow world of online dating. The article showed the disconnect between law and platform safety, which affects anyone who uses Facebook, Instagram, or Twitter. It also highlighted the unique burdens faced by gay and bisexual male users of the Internet, many of whom risk surveillance, outing, and loss of control over their identities if personal information shared online in one context is disclosed in another. Although more research is needed, particularly with respect to lesbians, transgender persons, and persons of color not represented in the sample set (McGlotten 2013; Han 2015), this article offers insight into how we are still struggling to respond to technology's impact on personal privacy, how different groups value and experience privacy decision making in different ways, and how law and design can be leveraged to subordinate or empower marginalized populations.

REFERENCES

- Acquisti, Alessandro, Leslie K. John, and George Loewenstein. "The Impact of Relative Standards on the Propensity to Disclose." *Journal of Marketing Research* 49 (April 2012): 160–74.
- Albury, Kathy, and Paul Byron. "Queering Sexting and Sexualisation." *Media International Australia* 153, no. 1 (2014): 138–47.
- Allen, Anita. *Uneasy Access: Privacy for Women in a Free Society*. New York: Rowman & Littlefield Publishers, 1988.
- Badiou, Alain. *In Praise of Love*. New York: The New Press, 2012.
- Barlow, John Perry. "A Declaration of the Independence of Cyberspace." *Electronic Frontier Foundation*. 1996. <https://www.eff.org/cyberspace-independence>.
- Bauman, Zygmunt. *Liquid Love: On the Frailty of Human Bonds*. Cambridge, UK: Polity, 2003.
- Berg, Joyce, John Dickhaut, and Kevin McCabe. "Trust, Reciprocity, and Social History." *Games and Economic Behavior* 10, no. 1 (1995): 122–42.
- Bijker, Weibe, Thomas P. Hughes, and Trevor Pinch, eds. *The Social Construction of Technology Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 2012.
- Bilton, Nick. "Tinder, the Fast-Growing Dating App, Taps an Age-Old Truth." *New York Times*. October 29, 2014.
- Blackwell, Courtney, Jeremy Birnholtz, and Charles Abbott, "Seeing and Being Seen: Co-Situation and Impression Formation Using Grindr, a Location-Aware Gay Dating App." *New Media and Society* 17, no. 7 (2015): 1117–36.

- Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage Books, 1983.
- Boso, Luke. "Dignity, Equality, and Stereotypes." *Washington Law Review* 92, no. 3 (2017): 1119–83.
- Bridges, Khiara M. "Privacy Rights and Public Families." *Harvard Journal of Law and Gender* 34, no. 1 (2011): 113–74.
- Brin, David. *The Transparent Society*. New York: Basic Books, 1999.
- Brubaker, Jed R., Mike Ananny, and Kate Crawford. "Departing Glances: A Sociotechnical Account of 'Leaving' Grindr." *New Media and Society* 18, no. 2 (2016): 373–90.
- Bullingham, Liam, and Ana C. Vasconcelos. "'The Presentation of Self in the Online World': Goffman and the Study of Online Identities." *Journal of Information Science* 39, no. 1 (2013): 101–12.
- Callander, Denton, Martin Holt, and Christy E. Newman. "Just a Preference: Racialised Language in the Sex-Seeking Profiles of Gay and Bisexual Men." *Culture, Health, and Sexuality* 14, no. 9 (2012): 1049–63.
- Callander, Denton, Christy E. Newman, and Martin Holt. "Is Sexual Racism Really Racism? Distinguishing Attitudes toward Sexual Racism and Generic Racism among Gay and Bisexual Men." *Archives of Sexual Behavior* 44, no. 7 (2015): 1991–2000.
- Citron, Danielle Keats. "Law's Expressive Value in Combatting Cyber Gender Harassment." *Michigan Law Review* 108, no. 1 (2009): 373–415.
- . "How to Make Revenge Porn a Crime: Worried about Trampling Free Speech? Don't Be." *Slate*. November 7, 2013. http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/making_revenge_porn_a_crime_without_trampling_free_speech.html.
- . *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press, 2014.
- Citron, Danielle Keats, and Mary Anne Franks. "Criminalizing Revenge Porn." *Wake Forest Law Review* 49, no. 2 (2014): 345–91.
- Citron, Danielle Keats, and Benjamin Wittes. "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity." *Fordham Law Review* 86, no. 2 (2017): 401–23.
- Cohen, Jean L. "The Necessity of Privacy." *Social Research* 68, no. 1 (2001): 318–27.
- . "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52, no. 3 (2000): 1373–438.
- . "Cyberspace as/and Space." *Columbia Law Review* 107, no. 1 (2007): 210–56.
- . "Privacy, Visibility, Transparency, and Exposure." *University of Chicago Law Review* 75 (2008): 181–201.
- . *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press, 2012.
- Congressional Record. 141 Cong. Rec. H8460–01 (August 4, 1995).
- Cowan, Ruth Schwartz. "The Consumption Junction: A Proposal for Research Strategies in the Sociology of Technology." In *The Social Construction of Technological Systems*, eds. Wiebe E. Bijker, Thomas Parke Hughes, and Trevor Pinch. Cambridge, MA: MIT Press, 1987.
- Duguay, Stefanie. "Dressing Up Tinderella: Interrogating Authenticity Claims on the Mobile Dating App Tinder." *Information, Communication & Society* 20, no. 3 (2017): 351–67.
- Eaton, Asia E., et al. "2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration: A Summary Report." 2017. <https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf>.
- Eskridge, Jr. William N. "Privacy Jurisprudence and the Apartheid of the Closet, 1946-1961." *Florida State Law Review* 24, no. 4 (1997): 703–840.
- . "No Promo Homo: The Sedimentation of Antigay Discourse and the Channeling Effect of Judicial Review." *New York University Law Review* 75, no. 3 (2000): 1327–411.
- Farnden, Jody, Ben Martini, and Kim-Kwang Raymond Choo. "Privacy Risks in Mobile Dating Apps." *Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015)* (2015): 1–16, 13–15 August 2015, Fajado, Puerto Rico.
- Franks, Mary Ann. "Unwilling Avatars: Idealism and Discrimination in Cyberspace." *Columbia Journal of Gender and the Law* 20, no. 1 (2009): 224–61.
- . "Adventures in Victim Blaming: Revenge Porn Edition." *Concurring Opinions*. February 1, 2013. <https://concurringopinions.com/archives/2013/02/adventures-in-victim-blaming-revenge-porn-edition.html>.

- . “How to Defeat ‘Revenge Porn’: First, Recognize It’s about Privacy, Not Revenge.” *Huffington Post*. 2015. http://www.huffingtonpost.com/mary-anne-franks/how-to-defeat-revenge-porn_b_7624900.html.
- . “‘Revenge Porn’ Reform: A View from the Front Lines.” *Florida Law Review* 70, no. 4 (2017): 1251–337.
- Fried, Charles. “Privacy.” *Yale Law Journal* 77, no. 3 (1968) 475–93.
- Gibbs, Jennifer L., Nicole B. Ellison, and Rebecca D. Heino, “Self-Presentation in Online Personals: The Role of Anticipated Future Interaction, Self-Disclosure, and Perceived Success in Internet Dating.” *Communications Research* 33, no. 2 (2006): 152–77.
- Gile, Krista J., and Mark S. Handcock. “Respondent-Driven Sampling: An Assessment of Current Methodology.” *Sociological Methodology* 40, no. 1 (2010): 285–327.
- Gilliom, John. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press, 2001.
- Ghorayshi, Azeen, and Dri Ray. “Grindr Is Letting Other Companies See User HIV Status and Location Data.” *BuzzFeed*. April 2, 2018. <https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy>.
- Goffman, Erving. *The Presentation of Self in Everyday Life*. New York: Anchor Books, 1959.
- Goldberg, Carrie, and Elisa D’Amico. “Representing Victims of Revenge Porn.” Presentation at Internet Safety Conference, New York, 2015.
- Goldman, Eric. “What Should We Do about Revenge Porn Sites like Texxxan?” *Forbes*. January 28, 2013. <https://www.forbes.com/sites/ericgoldman/2013/01/28/what-should-we-do-about-revenge-porn-sites-like-texxxan/#1068c2aa7eff>.
- Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford, UK: Oxford University Press, 2008.
- Grimmelmann, James. “Saving Facebook.” *Iowa Law Review* 94, no. 4 (2009): 1137–206.
- Grov, Christian, et al. “Gay and Bisexual Men’s Use of the Internet: Research from the 1990s through 2013.” *Journal of Sex Research* 51, no. 4 (2014): 390–409.
- Han, C. *Winter. Geisha of a Different Kind: Race and Sexuality in Gaysian America*. New York: NYU Press, 2015.
- Hardy, Jean, and Silvia Lindtner. “Constructing a Desiring User: Discourse, Rurality, and Design in Location-Based Social Networks.” Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, Feb. 25– Mar. 1, 2017, Portland, OR.
- Hartzog, Woodrow. *Privacy’s Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press, 2018.
- . “The Public Information Fallacy.” *Boston University Law Review* 99: 98 (forthcoming 2019).
- Heckathorn, Douglas. “Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations.” *Social Problems* 44 (1997): 174–99.
- Inness, Julie C. *Privacy, Intimacy, and Isolation*. Oxford, UK: Oxford University Press, 1992.
- John, Leslie K., Alessandro Acquisti, and George Loewenstein, “Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information.” *Journal of Consumer Research* 37, no. 5 (February 2011): 858–73.
- Kahan, Dan M. “The Logic of Reciprocity: Trust, Collective Action, and the Law.” *Michigan Law Review* 102, no. 1 (2003): 71–103.
- Kline, Ronald, and Trevor Pinch, “Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States.” *Technology and Culture* 37, no. 4 (1996): 763–95.
- Klonick, Kate. “The New Governors: The People, Rules, and Processes Governing Online Speech.” *Harvard Law Review* 131, no. 5 (2018): 1598–670.
- Lenhart, Amanda, Michelle Ybarra, and Myeshia Price-Feeney. “Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of ‘Revenge Porn.’” 2016. https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf.
- Levendowski, Amanda. “Using Copyright to Combat Revenge Porn.” *New York University Journal of Intellectual Property and Entertainment Law* 3, no. 2 (2014): 422–46.

- MacKinnon, Catherine. *Feminism Unmodified: Discourses on Life and the Law*. Cambridge MA: Harvard University Press, 1988.
- Matthews, Steve. "Anonymity and the Social Self." *American Philosophical Quarterly* 47, no. 4 (2010): 351–63.
- McGeveran, William. "The Law of Friction." *University of Chicago Legal Forum* 2013, no. 1 (2013): 15–67.
- McGlotten, Shaka. *Virtual Intimacies: Media, Affect, and Queer Sexuality*. Albany, NY: SUNY Press, 2013.
- Miller, Brandon. "'Dude, Where's Your Face?' Self-Presentation, Self-Description, and Partner Preferences on a Social Networking Application for Men Who Have Sex with Men: A Content Analysis." *Sexuality and Culture* 19, no. 4 (2015a): 637–58.
- . "'They're the Modern Day Gay Bar': Exploring the Uses and Gratifications of Social Networks for Men Who Have Sex with Men." *Computers in Human Behavior* 51, part A (2015b): 476–82.
- Mondada, Lorenza. "Challenges of Multimodality: Language and the Body in Social Interaction." *Journal of Sociolinguistics* 20, no. 3 (2016): 336–66.
- Murray, Sarah, and Megan Sappner Ankerson. "Lez Takes Time: Designing Lesbian Contact in Geosocial Networking Apps." *Critical Studies in Media Communications* 33, no. 1 (2016): 53–69.
- Nissenbaum, Helen. *Privacy In Context*. Cambridge, MA: MIT Press, 2010.
- Norman, Donald. *The Design of Everyday Things*. New York: Basic Books, 1988.
- O'Brien, Sara Ashley. "1, 100 Strangers Showed Up at His Home for Sex. He Blames Grindr." *CNN Tech*. Apr. 2017. <http://money.cnn.com/2017/04/14/technology/grindr-lawsuit/index.html>.
- Palen, Leysia, and Paul Dourish. "Unpacking 'Privacy' for a Networked World." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 129 (2003): 129–36.
- Parsons, Talcott. *Action Theory and the Human Condition*. New York: Free Press, 1978.
- Phillips, Christian. "Self-Pornographic Representations with Grindr." *Journal of Visual Media and Anthropology* 1, no. 1 (2015): 65–79.
- Post, Robert C. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77, no. 5 (1989): 957–1010.
- Prosser, William. "Privacy." *California Law Review* 48, no. 3 (1960): 383–423.
- Richards, Neil, and Woodrow Hartzog. "Taking Trust Seriously in Privacy Law." *Stanford Technology Law Review* 19 (2016): 431–72.
- Robinson, Brandon Andrew. "'Personal Preference' as the New Racism: Gay Desire and Racial Cleansing in Cyberspace." *Sociology of Race and Ethnicity* 1, no. 2 (2015): 317–30.
- Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Vintage Books, 2001.
- Rubin, Gayle. *Deviations: A Gayle Rubin Reader*. Durham, NC: Duke University Press, 2011.
- Shils, Edward. "Privacy: Its Constitution and Vicissitudes." *Law and Contemporary Problems* 31 (Spring 1966): 281–306.
- Siegmán, Aron W., and Stanley Feldstein, eds. *Nonverbal Behavior and Communication*. New York: Psychology Press, 1987.
- Skinner-Thompson, Scott. "Outing Privacy." *Northwestern Law Review* 110, no. 1 (2015): 159–222.
- . "Privacy's Double Standards." *Washington Law Review* 93, no. 4 (2018): 2051–106.
- Smith, Aaron. "15% of American Adults Have Used Online Dating Sites or Mobile Dating Apps." 2016. <http://www.pewinternet.org/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/>.
- Smith, Aaron, and Monica Anderson. "5 Facts about Online Dating." 2016. <http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/>.
- Solove, Daniel J. *The Digital Person: Technology and Privacy in the Digital Age*. New York: NYU Press, 2004.
- . *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2010.
- Stein, Edward. "Queers Anonymous: Lesbians, Gay Men, Free Speech, and Cyberspace." *Harvard Civil Rights-Civil Liberties Law Review* 38, no. 1 (2003): 159–213.

- Stern, Mark Joseph. "This Daily Beast Grindr Stunt Is Sleazy, Dangerous, and Wildly Unethical." *Slate*. August 11, 2016. <https://slate.com/technology/2016/08/the-daily-beasts-olympics-grindr-stunt-is-dangerous-and-unethical.html>.
- Strahilevitz, Lior Jacob. "A Social Networks Theory of Privacy." *University of Chicago Law Review* 72, no. 4 (2005): 919–88.
- Sullivan, Kathleen M. "First Amendment Intermediaries in the Age of Cyberspace." *University of California Los Angeles Law Review* 45 (1998): 1653–81.
- Towle, Andy. "Two NC High School Students Catfished Gay Teacher for Nude Photos on Grindr, and Passed Them Around." *Towleroad*. 2017. <http://www.towleroad.com/2017/05/catfish-teacher/>.
- Turkle, Sherry. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books, 2011.
- Tziallas, Evangelos. "Gamified Eroticism: Gay Male 'Social Networking' Applications and Self-Pornography." *Sexuality & Culture* 19, no. 4 (2015): 759–75.
- Volokh, Eugene. "Cheap Speech and What It Will Do." *Yale Law Journal* 104, no. 5 (1995): 1805–50.
- Wajcman, Judy. *Feminism Confronts Technology*. University Park, PA: Pennsylvania State University Press, 1991.
- Waldman, Ari Ezra. "A Breach of Trust: Fighting 'Revenge Porn.'" *Iowa Law Review* 102, no. 2 (2017): 709–33.
- . *Privacy as Trust: Information Privacy for an Information Age*. Cambridge, UK: Cambridge University Press, 2018a.
- . "Designing without Privacy." *Houston Law Review* 55, no. 2 (2018b): 659–727.
- Weber, Max. *Essays in Sociology*. Oxford: Oxford University Press, 1946.
- Westin, Alan F. *Privacy and Freedom*. New York: Ig Publishing, 1967.
- White, Howard B. "The Right to Privacy." *Social Research* 18, no. 2 (1951): 171–202.
- Whitfield, Darren L. "Grindr, Scruff, and on the Hunt: Predictors of Condomless Anal Sex, Internet Use, and Mobile Application Use among Men Who Have Sex with Men." *American Journal of Men's Health* 11, no. 3 (2017): 775–84.
- Wohlfeiler, Dan, et al. "How Can We Improve Online HIV and STD Prevention for Men Who Have Sex With Men? Perspectives of Hook-Up Website Owners, Website Users, and HIV/STD Directors." *AIDS Behavior* 17, no. 9 (2013). doi: [10.1007/s10461-012-0375-y](https://doi.org/10.1007/s10461-012-0375-y).
- Woolgar, Steve. "Configuring the User: The Case of Usability Trials." *Sociological Review* 38, no. S1 (1990): 58–99.

CASES CITED

- Alberts v. Devine*, 479 N.E.2d 113, 120 (Mass. 1985).
- Bowers v. Hardwick*, 478 U.S. 186 (1986).
- Florida Star v. B.J.F.*, 491 U.S. 524, 527 (1989).
- Gill v. Hearst Pub. Co.*, 253 P.2d 441, 444 (Cal. 1953).
- Herrick v. Grindr*, Opinion and Order, 17-CV-932 (VEC) (S.D.N.Y. January 25, 2018).
- Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961).
- Smith v. Maryland*, 442 U.S. 735, 744 (1979).
- State v. Rhodes*, 61 N.C. 453 (1868).
- United States v. Miller*, 425 U.S. 435, 443 (1976).
- Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997).

STATUTES CITED

- Ala. Code § 13A-6-240 (West 2015).
- Alaska Stat. Ann. § 11.61.120 (West 2015).
- Ariz. Rev. Stat. § 13-1425 (Supp. 2015).

- Ark. Code Ann. §§ 5-26-302, 5-26-314 (Supp. 2015).
 Cal. Penal Code § 647 (West Supp. 2016).
 Colo. Rev. Stat. Ann. § 18-7-107 (West Supp. 2015).
 Communications Decency Act, 47 U.S.C. § 230.
 Conn. Gen. Stat. Ann. § 53a-189a (West 2012 & Supp. 2016).
 D.C. Code Ann. §§ 22-3051–57 (West 2016).
 Del. Code Ann. tit. 11, § 1335 (2015).
 Fla. Stat. Ann. § 784.049 (2015).
 Ga. Code Ann. § 16-11-90 (West Supp. 2015).
 Haw. Rev. Stat. § 711-1110.9 (2014).
 Idaho Code Ann. § 18-6609 (West 2016).
 Ill. Comp. Stat. Ann. § 5/11-23.5 (2015).
 Iowa Code Ann. § 708.7 (West 2015).
 Kan. Stat. Ann. § 21-6101(a)(8) (West 2016).
 Ky. Rev. Stat. § 531.120 (West 2018).
 La. Rev. Stat. Ann. § 14:283.2 (2004 & Supp. 2016).
 Me. Rev. Stat. Ann. tit. 17-A, § 511-A (West Supp. 2015).
 Md. Code Ann., Crim. Law § 3-809 (West Supp. 2015).
 Mich. Comp. Laws Ann. §§ 145e, 145f (West 2016).
 Minn. Stat. Ann. § 617.261 (2017).
 Mo. Rev. Stat. §§ 573.110, 573.112 (West 2018).
 Nev. Rev. Stat. Ann. § 200.780 (West 2015).
 N.H. Rev. Stat. Ann. § 644:9-a (West 2016).
 N.J. Stat. Ann. § 2C:14-9 (West 2015).
 N.M. Stat. Ann. § 30-37A-1 (West 2015).
 N.Y.C. Int. No. 1267 (enacted December 12, 2017).
 N.C. Gen. Stat. Ann. § 14-190.5A (2015).
 N.D. Cent. Code Ann. § 12.1-17-07.2 (Supp. 2015).
 Okla. Stat. Ann. tit. 1040.13b (2016).
 Or. Rev. Stat. Ann. § 163.472(1)(a) (2015).
 Pa. Cons. Stat. Ann. § 3131 (2015).
 Restatement (Second) of Torts § 46 (Am. Law Inst. 1965).
 Restatement (Second) of Torts § 652D-E (Am. Law Inst. 1977).
 R.I. Gen. Laws ch. 11-64-3 (2018).
 S.D. Codified Laws § 22-21-4 (West 2015).
 Tenn. Code Ann. § 39-17 (West 2016).
 Tex. Penal Code Ann. § 21.16 (West Supp. 2016).
 Utah Code Ann. § 76-5b-203 (West 2016).
 Vt. Stat. Ann. tit. 13, § 2606 (West Supp. 2015).
 Va. Code Ann. § 18.2-386.2 (2014).
 Wash. Rev. Code Ann. § 9A.86.010 (West 2016).
 W. Va. Code Ann. § 61-8-28a (West 2016).
 Wis. Stat. Ann. § 942.09 (2013-2014).

APPENDIX A Nonconsensual Image Sharing in the LGBTQ Community

This is a survey about the LGBTQ community's experience with nonconsensual image sharing. In particular, I am interested in the experiences of those who use and have shared explicit photographs on geosocial apps like Grindr, Tinder, and others. By "nonconsensual image sharing," I mean any time someone else sends one of your pictures to another person (or persons) without your consent. That dissemination could have happened via text message or by posting them online or in any number of other ways.

Please answer honestly.

The survey is anonymous. However, if you are willing, I may wish to follow up with some of you to get more details on your story. So, if you enter your email address at the end of the survey, I may contact you with follow up questions. Your identity will be kept confidential.

I identify as *

Female

Male

Prefer not to say

Non-Binary (including genderqueer, gender fluid)

Other:

I also identify as *

Prefer not to say

Transgender

Cisgender

My sexual orientation is *

Bisexual

Lesbian

Gay (male)

Prefer not to say

Other:

My age is *

18-24

25-34

35-44

45-54

55 and older

My relationship status is *

Single

Dating

In a committed relationship (including long term relationship, married, domestic partnerships, etc.)

Prefer not to say

Other:

The highest level of education I have achieved is *

Graduated high school

Attended some college

Graduated college

Attended some graduate or professional school

Graduated with an advanced degree (including Masters, JDs, PhDs, etc.)

I am located in what country?

If located within the United States, what state?

I use or have used which of the following geosocial dating apps geared toward the LGBTQ community . . . (Please select all that apply). *

OkCupid

Zoosk

Match.com

Jack'd

FindHRR

HER

Surge

BeNaughty

Scruff

Grindr

SCISSR

Tinder

Growlr

Hornet

Other:

The PRIMARY purpose for which I use these apps is *

Please choose no more than 2.

to have sex.

to chat online.

to find a relationship.

to make new friends.

to meet people to date.

Other:

I have shared graphic, explicit, or nude photos or videos of myself on any of these platforms? *

Yes

No

I have shared shirtless or otherwise revealing pictures of myself on any of these platforms? *

Yes

No

I share explicit or revealing photos of myself on these platforms with the expectation that the person I send them to will not share them with anyone else. *

Strongly Disagree

1

2

3

4

5

Strongly Agree

When I share explicit or revealing photos of myself on these platforms, I don't care if the person I send them to shares them with others. *

Strongly Disagree

1

2

3

4

5

Strongly Agree

Sharing photos is pretty much a necessary part of the process of meeting people on these apps. *

Strongly Disagree

- 1
- 2
- 3
- 4
- 5

Strongly Agree

Please provide more detail about your thought process when you have shared graphic, explicit, nude, partially nude, or revealing photos of yourself on these platforms. I am interested in learning about your motivations for sharing these photos and how, if at all, you process concerns about your privacy when sharing. If sharing photos is not a concern, please explain why.

I've met people on these apps without sharing explicit or revealing photos. *

Strongly Disagree

- 1
- 2
- 3
- 4
- 5

Strongly Agree

I trust other people on these apps. *

Strongly Disagree

- 1
- 2
- 3
- 4
- 5

Strongly Agree

Please expand on your answer to the last question. Why do you trust or distrust people on these apps?

Someone I spoke to on a geosocial dating app has threatened to distribute to others or make public revealing or explicit photos of me without my consent. *

- Yes
- No

On which app or apps did this occur (Please select all that apply)?

- Match.com
- Growlr
- Jack'd
- FindHRR
- Tinder
- Hornet
- HER
- Scruff

Grindr
Surge
Zoosk
SCISSR
OkCupid
BeNaughty
Other:

Someone I spoke to on a geosocial dating app has distributed or made public revealing or explicit photos of me without my consent. *

Yes
No

On which app or apps did this occur (Please select all that apply)?

Growlr
Scruff
Surge
OkCupid
BeNaughty
Grindr
Jack'd
Hornet
HER
SCISSR
Zoosk
Match.com
FindHRR
Tinder
Other:

Please describe what happened in your own words. Please also include how you reacted (emotionally and practically) to the situation.

Thank you for completing this story survey. If you are willing to potentially receive an email from the researcher to discuss, over email or telephone, more about any of your answers to the above questions, please enter an email below. Your identity will be kept confidential.

My email address is

APPENDIX B Sample Questions from Semistructured Interviews

Do you use geosocial dating apps like Grindr, Scruff, or Tinder?

Do you share graphic or explicit pictures of yourself on these platforms?

Do you worry that images you share can be distributed, shown to others, posted online?

How do you determine when you feel comfortable sharing explicit images of yourself?

Do you feel pressure to share explicit images of yourself?

Have you ever reported a profile to the app? What was the reason? Did the reporting or flagging work?

Has someone ever threatened to share your explicit images?

Has anyone actually done it?

If so, how did you respond?