

Chapter 22

Navigating Privacy on Gay-Oriented Mobile Dating Applications*

Ari Ezra Waldman

Abstract

Mobile dating apps are widely used in the queer community. Whether for sexual exploration or dating, mobile and geosocial dating apps facilitate connection. But they also bring attendant privacy risks. This chapter is based on original research about the ways gay and bisexual men navigate their privacy on geosocial dating apps geared toward the LGBTQI community. It argues that, contrary to the conventional wisdom that people who share semi-nude or nude photos do not care about their privacy, gay and bisexual users of geosocial dating apps care very much about their privacy and engage in complex, overlapping privacy navigation techniques when sharing photos. They share semi-nude and nude photos for a variety of reasons, but generally do so only after building organic trust with another person. Because trust can easily break down without supportive institutions, this chapter argues that law and design must help individuals protect their privacy on geosocial dating apps.

Keywords: LGBTQI; cyberharassment; privacy; trust; platform design; social networks; online dating


Introduction

Sharing personal information has always been an integral part of social life, binding us together in productive and healthy ways (Derlega, Metts, Petronio,

*Portions of this chapter are based on previously published work: Waldman, A. (2019). Law, privacy, and online dating: 'Revenge porn' in gay online communities. *Law & Social Inquiry*, 44(4), 987–1018.

The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 369–381

Copyright © 2021 Ari Ezra Waldman

 Published by Emerald Publishing Limited. This chapter is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of these chapters (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>.

doi:[10.1108/978-1-83982-848-520211027](https://doi.org/10.1108/978-1-83982-848-520211027)

& Margulis, 1993). At the same time, sharing creates privacy and safety risks, especially for marginalized populations. The moment we share something, we lose control over it. We run the risk of its wider dissemination. We are vulnerable to those who have information about us, especially when that information is stigmatizing, out of context, and potentially harmful (Richards & Hartzog, 2016). And yet, we still share. This is not because we do not care about our privacy; we care a great deal. We share personal information using complex privacy navigation techniques that develop organic trust within communities (boyd, 2014; Waldman, 2018a).

This chapter is about the privacy and safety risks faced by members of the LGBTQI community who use online social networks, particularly dating applications and platforms, and the ways in which LGBTQI persons navigate their privacy in a digital environment with strong and persistent norms of disclosure. I will make two arguments, one descriptive and one normative. The descriptive argument is that individuals engage in complex privacy self-navigation on queer-oriented geosocial dating applications to build and maintain organic trust norms that protect themselves from some privacy risks. In particular, gay and bisexual men anonymize photos, develop a rapport through conversation, engage reciprocal sharing and mutual surveillance, and rely on identity-based familiarity in an attempt to organically build trust and enhance safety. My normative argument is that self-navigation will always be insufficient, and that norms of trust in online social spaces require support from endogenous design and exogenous law to make those spaces safe for sharing.

This chapter proceeds in four parts. Part I explores the powerful disclosure norms in geosocial dating applications, particularly those that cater to gay and bisexual men. These norms are both designed-in and socially constructed, and they create strong pressures to share intimate information. Part II discusses the privacy risks that come with disclosure. Given that the focus of this chapter is on gay and bisexual experiences, this Part shows how sharing in the online dating context poses unique challenges to marginalized populations. Part III describes how users navigate their privacy in a disclosure-heavy environment. Finally, Part IV argues that the organic trust users are trying to create is insufficient to protect privacy online. Law and design must help.

The Disclosure Norms of Geosocial Dating Applications

Online social networks and mobile applications are multifactor information-sharing environments (Goffman, 1959). We disclose voluminous personal information on social networks like Facebook not just our “likes,” but everything Facebook can learn from that engagement. Geosocial dating platforms are a widely used subset of online social networks (Anderson, Vogels, & Turner, 2020) and they require or strongly encourage the disclosure and exchange of highly intimate information, including sexual interests, HIV status, and, at times, graphic or revealing images. Put another way, geosocial dating applications operate with powerful norms of disclosure generated in three ways: design requirements, design nudges, and social practice.

Design Requirements

Platform designers require that users share certain information. Grindr, the popular gay-oriented geosocial application, requires an email address and other information on the backend. As a geosocial application, it also requires location information; it incorporates 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. Some applications require at least one photograph; most require that all users are above a certain age. Disclosure requirements serve several purposes, some technical, some social, and some both. For example, platforms may require a valid email address or phone number for both verification and two-factor authorization. Those disclosure mandates stem from how the technology works. Dating platforms may also require users to select a gender identity and/or sexual orientation, allowing them to match users. The same is true for zip codes, the disclosure of which allows geosocial applications to function and meet users’ expectations.

Design Nudges

“Nudges” refer to any aspect of “choice architecture,” or the context in which people make decisions, can “alter people’s behavior in a predictable way without forbidding any options,” like how grouping expensive cereals at eye-level and relegating the cheaper ones below encourages a more expensive purchase (Thaler & Sunstein, 2008, p. 6). Nudges are subtle yet powerful, triggering any number of cognitive biases that make disclosure more likely (Mathur et al., 2019; Waldman, 2019c). Dating applications, especially those that purport to match compatible people, nudge users to disclose personal information to receive extra benefits from the platform. *OkCupid* (n.d.), for example, “ask[s] interesting questions to get to know [users] on a deeper level” and encourages users to answer as many questions as possible to improve their matches. Users answer questions about detailed and deeply personal questions: “If a partner asked you to have sex in a sex shop booth with others watching, would you?” or “How does the idea of being slapped hard in the face during sex make you feel?” or “Have you ever gone on a rampant sex spree while depressed?” (Donovan, 2012). Answering these questions is optional, but the platform pushes what it calls a “super-smart algorithm” that matches compatible users based on the answers. This implies that the more answers users provide, the better their match should be. Although there is reason to question the need for all these data points (Dressel & Farid, 2018; Salganik, 2019), the pressure to disclose remains.

The design of geosocial applications nudges users to share personal and intimate images, which are the currencies of these platforms. 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 about other users, thus creating pressure to upload at least one image. Although all platforms allow users to add information to their profiles including name, age, and physical characteristics,

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.

Social Practice

According to the Pew Research Center, 71% of online daters said it was important or very important to them that others' profiles included at least one photo of themselves (Anderson et al., 2020). Wide majorities also want to see complete profiles, filled with information that is at once intimate, but also necessary to set expectations. Gay and bisexual men want to know others' HIV status, sexual interests, and professional and educational backgrounds. They also want to see more than one photo, with at least one study arguing that representation through imagery was an important part of identity-formation on Grindr (Blackwell, Birnholtz, & Abbott 2014). This demand creates strong disclosure norms that put pressure on users to share intimate information and ultimately put their privacy at risk.

In previous research, I showed how the social practice of LGBTQI-oriented dating applications includes the expectation of sharing intimate photos (Waldman, 2019a). That study, which includes surveys and ethnography, suggested that for many gay and bisexual men, "if you don't share photos, you can't really participate" (p. 997). One respondent noted that "there's an expectation; gays want to see what you're offering" (p. 997). Another stated that "[s]haring photos seems to be essential to maintaining interest. I wish it weren't the case, but whatever" (p. 997). Although many gay and bisexual men share intimate photos for other reasons, such as body positivity and sexual exploration, other factors remain powerful, including the verification of identity and security, and the expectation to share and prevailing norms of disclosure. Put another way, any one individual may experience pressure to share personal information or intimate photos. The pervasiveness of that pressure makes disclosure a social fact of queer-oriented dating applications; the norm exists independent of any particular request for a photo.

With Disclosure Comes Privacy Risk

It is axiomatic that disclosing personal information to others online puts us at risk of privacy invasions, exploitation, extortion, and harassment. This is particularly true for women, sexual minorities, and other marginalized populations (Burkell & Bailey, 2018; Citron, 2014). Interactive digital technologies amplify those risks. Information is easy and cheap to store, disseminate, and leverage. Online interactions erode traditional in-person social norms by dehumanizing and flattening the identities of other individuals. Digital technologies, therefore, lower social barriers that hold hateful and harassing conduct at bay, and in so doing, amplify and entrench the power dynamics that already exist in society (Citron, 2009).

With respect to LGBTQI-oriented geosocial dating applications, concerns about privacy invasions, harassment, and stalking are neither theoretical nor idle. These

platforms have already exposed their users to major privacy breaches. Grindr shared its users' HIV status with third parties for years (Ghorayshi & 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 timestamp could allow someone to track users in real space. This information has been used in violent homophobic attacks. For example, people have used Grindr to murder and torture gay men in the United States, Canada, and across the world, especially in countries that criminalize homosexuality and sodomy (Carroll, 2019; Fitzsimmons, 2020; Tracy, 2020). On Badoo, which is identical to the Blendr application, Farnden et al. (2015) were able to collect profile names, chat histories, nearby users, profile information, and device information. On Tinder, the most popular dating application 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 in the closet (Stern, 2016).

Despite these risks, individuals who identify as gay and bisexual frequently use these applications and share information to meet others who share their identities. According to one study, dating application users who identified as heterosexual opened their applications eight times per week and used them for 71 seconds at a time (Grov et al., 2014). Gay and bisexual men, on the other hand, averaged 22 times per week for 96 seconds at a time. Grindr reported that in 2013, more than one million users logged in to the application every day and sent more than seven million messages and two million photos (Grov 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. Social engagements on these applications are also expressions of sexual and romantic freedom after decades of marginalization. Some even argue that they facilitate a form of self-pornography and eroticism (Tziallas, 2015). Whatever the reason, it is clear that gay and bisexual individuals use these applications frequently (Anderson et al., 2020) and share a significant amount of personal information as a result. Because everything that we share may be recorded, retained, screenshotted, and saved, this puts us at risk for cyberharassment, exploitation, so-called "revenge porn" (more appropriately termed "nonconsensual pornography" because it involves the nonconsensual sharing of someone else's identifiable intimate or graphic images or videos and is not necessarily done out of a desire for revenge), and technology-facilitated intimate partner violence, among myriad other abuses.

Privacy Self-Help

Gay and bisexual users of geosocial dating applications face strong pressures to disclose intimate information and images. Because doing so involves some risk, users go to great lengths to protect their privacy. This is not just true of members of the LGBTQI community. As Sarah Heath (2015) has shown, women and girls

leverage “controls initiated by users to protect and maintain their security online” (p. 362). The goal of these measures is to create and maintain norms of trust that can help ameliorate the risks of disclosure.

Previously, I surveyed 834 gay and bisexual men who used geosocial dating applications and engaged a subset of respondents in semi-structured interviews pursuant to their consent. Some findings from that study, particularly about the frequency with which nonconsensual pornography affects gay and bisexual men on these applications, have been published elsewhere (Waldman, 2019a). I demonstrated that 87.4% of gay and bisexual men have shared “graphic, explicit, or nude photos or videos” of themselves on geosocial dating applications, while 93.4% have shared “shirtless or otherwise revealing” photos (Waldman, 2019a, p. 996). But that disclosure is not random. It happens in the context of specific norms and expectations. Exactly 82.6% of survey respondents either agreed or strongly agreed with the statement: “Sharing photos is pretty much a necessary part of the process of meeting people on these applications.” That means the users in this survey felt the pressures of disclosure norms. At the same time, 89.7% share images with the expectation that they will not be shared further, which means their sharing takes place in a context of expectations of trust, discretion, and confidentiality (Richards & Hartzog, 2016; Waldman, 2019a).

Users create those expectations by engaging in, primarily, four privacy self-help techniques: anonymizing photos; developing a rapport through conversation; reciprocal sharing and mutual surveillance; and identity-based familiarity. Together, these strategies are aimed at building organic trust norms to mitigate the risks posed by the powerful norms of disclosure that have become social facts of these dating applications.

Anonymization

Many users upload or send intimate images without their faces or without identifying characteristics, at least initially. Or, they will send identifiable non-intimate pictures, but only cropped explicit photos. Or, they will only send photos that they “wouldn’t be embarrassed by if [they] were made public” (Waldman, 2019a, p. 998). This strategy reduces the risk of harm if the pictures are shared or posted online because identifiable nude photos are prime weapons in the perpetuation of nonconsensual pornography, extortion, and other forms of cyberexploitation (see Citron & Franks, 2014; Henry et al., 2020; Powell, Henry, & Flynn, 2018). This particular strategy navigates the design nudge to share photos, which are the first parts of profiles other users see. And it is a popular one. Over a period of two weeks in 2017, I logged onto Grindr and Scruff, two geosocial dating applications geared toward gay and bisexual men, once per day and categorized the first 40 photos visible on my feed for each application. Excluding repeat accounts or duplicate photos (105), the total number of photos in the sample was 455. Of those, 68.8% were anonymized or de-identified.

People share anonymized photos for several reasons. The most common explanation for this provided by the 24 individuals that consented to be

interviewed for this project was privacy through compartmentalization. Even if particular users had nothing to hide, they wanted a “strict separation between my Grindr life and my work life,” per one respondent’s formulation. The second most popular rationale was that users wanted to share sexualized photos of themselves and, as one reported, “didn’t want that to get around.” Both explanations are based on conceptualizations of privacy well-recognized in the scholarly literatures, including privacy as intimacy and separation from others (Waldman, 2018a).

Rapport Development

Online dating sites foster initial communication between potential romantic partners. Studies have shown that some online daters engage in long pre-meeting communications, but Whitty and Carr (2006) found that most online daters arranged to meet in person within one week of their initial online encounter. However, Ramirez and Zhang (2007) and Ramirez and Wang (2008) found that the amount of time and online communication between those who met online helped determine outcomes when they met offline. That is, although many but certainly not all people may not want to engage in an endless online back and forth, especially where sex rather than long term dating is involved, more opportunities to develop a rapport with someone online gave online daters a better sense of whether any offline meeting would be successful. Gay and bisexual men experience this on geosocial dating applications as well, choosing to use chat features to develop a rapport with others before sharing intimate information. Many gay and bisexual men only share photos, graphic or otherwise, after “chatting with the other person” (Waldman, 2019a, p. 998) for some time ranging from a few hours to a few weeks sufficient to “develop a rapport” (Waldman, 2019a, p. 998) or, as Jared S. responded in my previous study, “feel somewhat comfortable with the other person” (Waldman, 2019a, p. 998). As another anonymous respondent noted, “you begin to trust the person and let your guard down” (Waldman, 2019a, p. 998).

A rapport with another person, even one we have only recently met, is a signal of sharing values, worldviews, and ultimately trust. Although sociologists have long suggested that trust usually comes from long interactions with others, trust in the form of expectations of continued adherence to norms can develop between relative strangers (Waldman, 2018a). That is at least one goal of online engagements before meeting in person.

Reciprocity

Some gay and bisexual men 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, & McCabe, 1995; Brin, 1999; Kahan, 2003). As Ben Z. noted in my previous study, “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?” (Waldman, 2019a, p. 999). Then, after reciprocation, users rely on a form of mutually assured

surveillance. As one study participant noted, “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” (Waldman, 2019a, p. 999).

Familiar Identity

Some rely on the comfort and familiarity in an application’s exclusive queerness. Stephen P. noted in my previous study: “[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” (Waldman, 2019a). 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” (Waldman, 2019a, p. 999). 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 (Waldman, 2019a).

Self-Help isn’t Sufficient

These strategies make users *feel* safer. They create and try to maintain a sense of trust among social actors, and trust is an essential piece of the privacy puzzle (Richards & Hartzog, 2016; Waldman, 2018a). But these strategies cannot create safe social spaces on their own. Indeed, nonconsensual pornography is rampant on LGBTQI-oriented geosocial dating applications. According to the Data & Society Research Institute, 7% of lesbian, gay, and bisexual internet users say someone has shared their intimate images without their consent (Lenhart, Ybarra, & Price-Feeney, 2016; see also; Powell, Henry, Flynn, & Scott, 2019; Powell, Scott, Henry, & Flynn, 2020). Among gay and bisexual men who use geosocial dating applications, that number jumps to nearly 15% (Waldman, 2019a). There is also powerful anecdotal evidence. In May 2017, two North Carolina high school students created a fake profile on Grindr, the popular gay-oriented geosocial application. 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 lawsuit that an ex-boyfriend stole his intimate images, impersonated him on an application, 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*, 2018).

Norms of trust require the assistance of privacy- and safety-enhancing design and privacy-protective law to counter the powerful norms of disclosure and ameliorate the vulnerabilities those norms create (Waldman, 2019b). These elements endogenous design of the social environment and exogenous law providing protections to individuals, constraints on platforms, and opportunities for justice

are what make other social spaces safe for sharing. Scholars have long recognized that law and endogenous design work together to guide and constrain activities in digital spaces (Bailey & Steeves, 2015; Reidenberg, 1997). And we see this everywhere, both offline and online. The privacy of Alcoholics Anonymous meetings is protected by norms buttressed by organization rules and the courts, which protect expectations of confidentiality. Attorney-client relationships are based on trust, but that trust is protected and supported by ethical rules as well as legal regimes that punish lawyers who betray their clients' confidences. Even co-workers are more likely to share when they trust their teammates, but the trust that others will not work against the team or share their secrets is buttressed by both internal corporate rules and the law of trade secrets (Waldman, 2019b). These social institutions make social spaces safe in the offline context. There is no reason why they cannot be leveraged to protect online spaces as well.

Rather than operate to enhance and support trust norms on digital platforms like geosocial dating applications, technology design and the law do the opposite: they collect data from users, make it difficult to protect privacy and safety, and provide no legal incentive for companies to take necessary pro-privacy action. As Woodrow Hartzog (2018) has deftly described, digital platforms are designed as information extraction machines, passively gathering data on our behavior and nudging us to disclose more than we otherwise might. They leverage so-called "dark patterns" or design tricks that manipulate us into granting consent or giving up information (Mathur et al., 2019). And the law does not stop them. Regulators have never taken a close look at the ways in which technology design influences our behavior (Hartzog, 2018). And, in the United States, a federal law known as the Communications Decency Act Section 230 has been interpreted by the federal courts to grant broad immunity to technology companies for the tortious conduct of third parties on their platforms. That broad immunity takes away any legal incentive companies have to make their platforms safer, more privacy protective, and less welcoming to opportunists, mischief makers, and criminals (Citron & Wittes, 2017; Sylvain, 2018).

There are, therefore, specific steps platforms and policymakers can take to change this status quo. On the technical side, geosocial platforms can change their defaults to minimize information sharing with third parties, requiring users to take the affirmative step of opting in. Safety by design could involve ephemeral messaging for intimate images, access restrictions, streamlined takedown procedures, and frictionless tagging of profiles that spew hate, engage in harassment, and violate other terms of use (Hartzog, 2018). Privacy advocates can even be collocated with technical designers to provide them real-time insight on privacy issues as they come up (Waldman, 2018b).

Law can reorient the relationship between users and platforms by statutorily creating duties of care, loyalty, and confidentiality by which platforms must abide. Technology companies running techno-social platforms should be considered information fiduciaries for the same reasons that doctors, lawyers, and investment advisers are considered traditional fiduciaries. We are vulnerable to them because they know everything about us. We are dependent on them because of the services they provide and the expertise they bring to those services. And

they hold themselves out as sufficiently trustworthy to gain our business (Balkin, 2016). The notion of an information fiduciary would, as a practical matter, mean that platforms cannot abuse their users by extracting intimate information and nonconsensual pornography, for example, would be a violation of a duty of loyalty. Alongside a duty of loyalty, duties of care and confidentiality would impose specific requirements of reasonable security and limited disclosure to third parties in accordance with user expectations. Some of these ideas have been included in proposals for new privacy and data protection laws in the United States, but the prospects for approval are, as of this writing, slim.

Section 230 of the Communications Decency Act must be amended. It is difficult to see why a digital platform would, outside of market pressures, take steps to protect their users from harm without a legal incentive. Those market pressures, if they exist, do not seem to be working now. As such, legal changes are necessary. Olivier Sylvain (2018) suggests Congress maintain Section 230's immunity but create an explicit exception from immunity for civil rights violations. Policymakers have called for additional exceptions, in addition to those enacted recently by the Stop Enabling Sex Traffickers Act (SESTA), which exempted from Section 230 any platform knowingly hosting sex trafficking content (Brody & Nix, 2000; Cole, 2018). But these kinds of piecemeal approaches are flawed. Sylvain's well-intentioned proposal creates a hierarchy of harms, which is not only worrisome per se but also subject to misuse and misinterpretation by the federal courts. SESTA, again though well-intentioned, predicates liability on knowledge, which has the perverse incentive of encouraging ignorance or overinclusive content moderation to eliminate all sex-related content. Instead of these approaches, Andrea Slane and Ganaele Langlois (2018) have proposed a tiered system of liability. Those platforms that invite and welcome illegal conduct like nonconsensual pornography should be held directly liable as publishers of illegal conduct. Other platforms that do not directly traffic in harassment and exploitation, but are at high risk of doing so, like the amateur pornography industry, should be required to verify that all participants are of age. And those platforms, like Facebook, that operate digital spaces of user generated content at scale, should be required to respond to user complaints of nonconsensual pornography. Citron and Wittes (2017) suggest making Section 230 immunity contingent on good faith and reasonable content moderation: only those who make a good faith effort to remove harassing, unlawful, and tortious content would be able to take advantage of the immunity, leaving the otherwise "bad Samaritans" with a strong legal incentive to do something about the safety and privacy problems on their platforms.

Conclusion

In the end, no social spaces, online or offline, can always be safe. Life involves risk, and so do disclosures, social networking, online dating, and the conveniences of modern life. But privacy and safety remain relevant. Privacy, expectations of confidentiality and discretion, as well as relief from hate and harassment, are all necessary for identity formation, intellectual freedom, and equality. Marginalized

populations also bear a disproportionate burden of the hate and harassment and thus experience the greatest harms while being unable to exercise their rights as free citizens. Techno-social spaces do not have to be like this. Many of us want to engage on these platforms, and take significant steps to protect ourselves as best we can. But we cannot do this alone. Design and law can play guiding and expressive roles in support of enhancing trust, safety, and privacy.

References

- Anderson, M., Vogels, E., & Turner, E. (2020). *The virtues and downsides of online dating*. Pew Research Center. Retrieved from <https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/>
- Bailey, J., & Steeves, V. (2015). Introduction. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens: Putting technology, theory and policy into dialogue with girls' and young women's voices* (pp. 1–20). Ottawa, CA: University of Ottawa Press.
- Balkin, J. (2016). Information fiduciaries and the first amendment. *University of California, Davis Law Review*, 49(4), 1183–1234.
- Berg, J., Dickhaut, J., & McCabe, K. (1995). Trust, reciprocity, and social history. *Games and Economic Behavior*, 10(1), 122–142.
- Blackwell, C., Binrholtz, J., & Abbott, C. (2014). Seeing and being seen: Co-situation and impression formation using Grindr, a location-aware gay dating app. *New Media & Society*, 17(7), 1117–1136.
- Boyd, D. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.
- Brin, D. (1999). *The transparent society*. New York, NY: Basic Books.
- Brody, B., & Nix, N. (2000). *Lindsey Graham proposal could expose apple, Facebook to lawsuits*. Bloomberg. Retrieved from <https://www.bloomberg.com/news/articles/2020-01-30/lindsey-graham-proposal-could-expose-apple-facebook-to-lawsuits>
- Burkell, J., & Bailey, J. (2018). Equality at stake: Connecting the privacy/vulnerability cycle to the debate about publicly accessible online court records. *Canadian Journal of Comparative and Contemporary Law*, 4, 1–46.
- Carroll, O. (2019). Gay hunters: How criminal gangs lure men on dating apps before extorting cash and beating them. *Independent UK*. Retrieved from <https://www.independent.co.uk/news/world/europe/gay-hunters-russia-moscow-apps-gangs-homophobia-a8865376.html>
- Citron, D. K. (2009). Cyber civil rights. *Boston University Law Review*, 89, 61–125.
- Citron, D. K. (2014). *Hate crimes in cyberspace*. Cambridge, MA: Harvard University Press.
- Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, 49, 345–391.
- Citron, D. K., & Wittes, B. (2017). The internet will not break: Denying bad Samaritans section 230 immunity. *Fordham Law Review*, 86(2), 401–423.
- Cole, S. (2018). Senator suggests the Internet needs a FOSTA/SESTA for drug trafficking. *Vice*. Retrieved from https://www.vice.com/en_us/article/8xbwvp/joe-manchin-fosta-sesta-law-for-drug-trafficking-senate-intelligence-committee-hearing
- Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-disclosure*. Newbury Park, CA: Sage.

- Donovan, B. (2012). A tour of the sex questions on OkCupid. *Thought Catalog*. Retrieved from <https://thoughtcatalog.com/brian-donovan/2012/09/a-tour-of-the-sex-questions-on-okcupid/>
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4, 1–5. Retrieved from <https://advances.sciencemag.org/content/4/1/eaao5580/tab-pdf>
- Farnden, J., Martini, B., & Choo, K. R. (2015). Privacy risks in mobile dating apps. In *Proceedings of the 21st Americas conference on information systems (AMCIS 2015)*, Fajardo (pp. 1–16).
- Fitzsimmons, T. (2020). Michigan man charged in Grindr slaying. *NBC News*. Retrieved from <https://www.nbcnews.com/feature/nbc-out/michigan-man-charged-grindr-slaying-n1109596>. Accessed on April 30, 2020.
- Ghorayshi, A., & Ray, D. (2018). Grindr is letting other companies see user HIV status and location data. *BuzzFeed*. Retrieved from <https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy>. Accessed on March 20, 2020.
- Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Doubleday.
- Grov, C., Breslow, A. S., & Newcomb, M. E., (2014). Gay and bisexual men's use of the internet: Research from the 1990s through 2013. *The Journal of Sex Research*, 51(4), 390–409.
- Herrick V. Grindr. (2018, January 25). Opinion and order, 17-CV-932 (VEC) (S.D.N.Y.).
- Hartzog, W. (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Cambridge, MA: Harvard University Press.
- Heath, S. (2015). Security and insecurity online: Perspectives from girls and young women. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens: Putting technology, theory and policy into dialogue with girls' and young women's voices* (pp. 361–384). Ottawa, CA: University of Ottawa Press.
- Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., & Scott, A. J. (2020). *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*. London and New York, NY: Routledge.
- Kahan, D. M. (2003). The logic of reciprocity: Trust, collective action, and the law. *Michigan Law Review*, 102(1), 71–103.
- Lenhart, A., Ybarra, M., & Price-Feeney, M. (2016). Nonconsensual image sharing: One in 25 Americans has been a victim of “revenge porn.” Retrieved from https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf
- Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Retrieved from <https://arxiv.org/pdf/1907.07032.pdf>. Accessed on March 20, 2020.
- OkCupid. (n.d.). Retrieved from www.okcupid.com. Accessed on March 20, 2020.
- O'Brien, S. A. (2017). 1,100 strangers showed up at his home for sex. He blames Grindr. Retrieved from <http://money.cnn.com/2017/04/14/technology/grindr-lawsuit/index.html>. Accessed on March 20, 2020.
- Parsons, T. (1978). *Action theory and the human condition*. New York, NY: Free Press.
- Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In W. S. DeKeseredy & M. Dragiewicz (Eds.), *Routledge handbook of critical criminology* (2nd ed., pp. 305–315). Abingdon and New York, NY: Routledge.

- Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian adults. *Computers in Human Behavior*, 92, 393–402.
- Powell, A., Scott, A. J., Henry, N., & Flynn, A. (2020). *Image-based sexual abuse: An international study of victims and perpetrators. Summary report*. Melbourne, VIC: RMIT University.
- Ramirez, A., Jr., & Wang, Z. (2008). When online meets offline: An expectancy violations theory perspective on modality switching. *Journal of Communication*, 58(1), 20–39.
- Ramirez, A., Jr., & Zhang, S. (2007). When online meets offline: The effect of modality switching on relational communication. *Communication Monographs*, 74, 287–310.
- Reidenberg, J. (1997). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review*, 76, 553–593.
- Richards, N., & Hartzog, W. (2016). Taking trust seriously in privacy law. *Stanford Technology Law Review*, 19, 431–472.
- Salganik, M. (2019). Measuring the predictability of life outcomes with a scientific mass collaboration. Presentation at Princeton University, Center for Information Technology Policy, September 17, 2019. Retrieved from <https://cloud.swivl.com/v/8da7d538a3d9aa1972e3e5d5e38509df>
- Slane, A., & Langlois, G. (2018). Debunking the myth of “not my bad”: Sexual images, consent, and online host responsibilities in Canada. *Canadian Journal of Women and the Law*, 30, 42–81.
- Stern, M. J. (2016). This Daily Beast Grindr stunt is sleazy, dangerous, and wildly unethical. *Slate*. Retrieved from <https://slate.com/technology/2016/08/the-daily-beasts-olympics-grindr-stunt-is-dangerous-and-unethical.html>. Accessed on March 20, 2020.
- Sylvain, O. (2018). Intermediary design duties. *Connecticut Law Review*, 50, 203–277.
- Thaler, R. H., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yale University Press.
- Towle, A. (2017). Two NC high school students catfished gay teacher for nude photos on Grindr, and passed them around. *Towleroad*. Retrieved from <http://www.towleroad.com/2017/05/catfish-teacher/>. Accessed on March 20, 2020.
- Tracy, M. (2020). Moroccans use Grindr location data to out, target gay men. *Gay City News*. Retrieved from <https://www.gaycitynews.com/moroccans-use-grindr-location-data-to-out-target-gay-men/>
- Tziallas, E. (2015). Gamified eroticism: Gay male ‘social networking’ applications and self-pornography. *Sexuality & Culture*, 19(4), 759–775.
- Waldman, A. (2018a). *Privacy as trust: Information privacy in an information age*. New York, NY: Cambridge University Press.
- Waldman, A. (2018b). Designing without privacy. *Houston Law Review*, 55, 659–727.
- Waldman, A. (2019a). Law, privacy, and online dating: ‘Revenge porn’ in gay online communities. *Law & Social Inquiry*, 44(4), 987–1010.
- Waldman, A. (2019b). Safe social spaces. *Washington University Law Review*, 96, 1537–1579.
- Waldman, A. (2019c). Cognitive biases, dark patterns, and the ‘privacy paradox.’ *Current Opinion in Psychology*, 31, 105–109.
- Weber, M. (1946). *Essays in sociology*. Oxford: Oxford University Press.
- Whitty, M. T., & Carr, A. N. (2006). *Cyberspace romance: The psychology of online relationships*. Basingstoke: Palgrave Macmillan.