“No Overly Suggestive Photos of Any Kind”: Content Management and the Policing of Self in Gay Digital Communities

Yoel Roth

Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA 19104, USA

This article examines the policies and practices that manage user-submitted content on 3 gay-targeted social networking services. While managing user-generated content is a common practice across social networking services, the policies implemented on gay-targeted services tend to be distinctively restrictive in scope and highly specific in formulation. This analysis identifies the technical, legal, and social affordances that authorized the creation of these policies. Framing content management policies as derived from the technical rules of platforms such as Apple’s App Store obscures normative judgments about proper self-presentation and community formation. Identifying the normative character of these policies requires an analysis rooted simultaneously in technology studies, media policy, and subcultural identity politics.

Keywords: Platforms, Content Management, Social Media, LGBT, Identity Politics, Media Policy.

doi:10.1111/cccr.12096

Manhunt is a social networking service targeted at gay men, boasting over 6 million active members. As part of the registration process, new users are encouraged to upload a photo of themselves for inclusion on their profile. But not any photo will do. Photos uploaded to Manhunt are not immediately made publicly visible; instead, they are first reviewed by a team of screeners (many of whom are heterosexual men and women) against a published set of guidelines for acceptable content in user photos. Photos can be classified as “green” (unambiguously in compliance with photo rules and acceptable for public display), “yellow” (in compliance with the rules for photos that are not publicly visible), or “red” (unacceptable for display). The whole process typically takes half an hour, after which acceptable photos appear on the user’s profile. The procedure is, from the user’s perspective, effortless.

Corresponding author: Yoel Roth; e-mail: yoel@asc.upenn.edu
But what processes underlie the user experience of uploading a new photo? This article examines the content management policies and practices of the three largest gay-targeted social networking services—Manhunt, Grindr, and Scruff—in order to identify the technological, legal, institutional, and social affordances that enable the exclusion of certain types of images and behaviors from these services. What are the rules that govern the types of content that are permitted to be displayed on gay social networking services? How does the fact that these services are accessible primarily through mobile applications on smartphones impact their content policies? Are these policies the product of institutional restrictions on the kind of content that can appear in smartphone “app stores,” or do they represent a particular vision of what gay social networking should look like? How are those rules deployed in practice to manage user behavior? What is the responsibility of these services—to the law, to their users, and, perhaps, to gay communities at large? More generally, what are the sociotechnical norms that structure how these online services function?

Managing user-generated content—and, particularly, photos—is by no means a concern unique to gay-targeted social networking services. Social networking services, including ones focused on romantic or intimate relationships, cut across gay and straight communities; but the policies in place to manage gay services are distinctive in their specificity. While other scholarship has examined the social practices that emerge around these services (Crooks, 2013; Gudelunas, 2012; Mowlabocus, 2010), few have engaged directly with the distinctive normative and technical designs of these platforms. This article examines how the restrictive policies in place on services such as Grindr, Scruff, and Manhunt came to be authorized, both by application developers and the users of gay-targeted social networking services. In evaluating the relationship between policy and practice on these services, this study outlines both a model of content policies at their most specific, as well as a model for how the relationship between technical systems and subcultural practice should be conceptualized. Framing these content management policies as solely technical in origin obscreens the value judgments that are embedded in them. The subtleties of how these values are contested online—and, crucially, how patterns of user resistance to control figure into that process—only reveal themselves through an analysis of these policies in the hybrid terms of subcultural sociotechnics.

Method

Online content management practices are notoriously opaque. Joseph Turow, writing about Facebook, has referred to online service providers as a “black hole” (Turow, 2012, p. 138), absorbing and acting upon user information without providing any real indication of the logic behind or implementation of their procedures. Service providers are often reluctant to divulge proprietary or potentially competitively sensitive information. This introduces a number of methodological complications.
In lieu of looking inside the black hole, this article describes the documents, policies, and practices at its periphery; it interrogates the limited information that service providers make available in order to draw inferences about the internal logic of their content management practices. This focuses on three distinct questions, each of which requires a particular methodological approach. First, what are the principles of governance encoded in the text of terms of service documents and content guidelines? Using a legally informed close reading of the text of these policies, this article aims to outline the principles of governance they encode. While imperfect and often obtuse, these texts offer a concrete articulation (though not necessarily the only articulation) of how service providers understand their relationships with their users. Second, what are the on-the-ground practices of users and service providers that operationalize the codified rules encoded in terms of service documents? This analysis draws on two primary resources: (a) Participant observation on each of the three services, conducted over a period of 1 year in five major metropolitan areas, with a particular focus on observed user behavior and practical engagement with the policies and (b) interviews with members of the staff of the services included in this study. These resources contextualize the formal policies, focusing on how real-world engagements with or applications of these policies correspond with or differ from their textual articulations. Finally, what are the popular discourses and practices that emerge around these policies? Drawing on mainstream print and online publications, as well as publicly available user reviews of the three applications examined in this study, this analysis aims to elucidate the most prevalent discourses around these policies, focusing on how the relationship between policy and user behavior is described in media discourses about these services.

The problem of reading terms of service
The basic units of governance in the relationship between service providers and individual users are legal documents referred to as terms of service (TOS), end-user license agreements (EULAs), and privacy policies. Despite their ubiquity, the actual function of these documents remains open to contestation. Are these documents legalistic formalities, designed to protect service providers? Or are they a statement of the actual underlying principles of how a service understands itself, its information management practices, and its relationship with its users? This section outlines the traditional interpretive domains within which these policies have been examined with the aim of highlighting a gap in the hermeneutics of terms of service: By prioritizing the legal status of these documents, we neglect the pragmatics of their implementation.

On a basic level, electronic terms of service constitute a contract between a user and a service provider designed to ensure indemnity for the service provider. Despite the fact that EULAs and TOS documents have been in use regarding software for more than 3 decades, no new laws have been written to clarify their status in the United States. Instead, in a series cases before federal courts, existing contract law has been expanded to account for the questions raised by software contracts.
Central among these questions is the issue of informed decision-making: Do users meaningfully understand the terms they are agreeing to? This issue has had significant resonance with regulatory bodies such as the Federal Trade Commission (FTC). Recent research into regulatory behavior suggests a general level of skepticism toward the notion of a well-informed user, able to conscientiously enter into online contracts (Gindin, 2009). Users, this work argues, are not only uninformed, but also tend to eschew the practical steps they could take to become more informed. The FTC (2009) has acknowledged this tendency toward consumer inattention, independent of the length, clarity, or perceived importance of an agreement. It has, however, been unwilling to offer a firm normative injunction to users to actually invest the time and effort in understanding these agreements. The implication is that the agreements themselves, not users, are the problem.

Even if users took the 200 hours per year required to read every privacy policy, EULA, and TOS they encountered (Gomez, Pinnick, & Soltani, 2009), many would be unable to understand what they were reading. Despite attempts to educate consumers about online agreements, fewer than half of the respondents in a national survey indicated that the policies they encountered online are easy to understand (Turow, 2003, 2012)—mostly because the policies are opaque, overly broad, and confusing (Anton et al., 2004; Gomez et al., 2009; Nissenbaum, 2010). These misunderstandings are not helped by the fact that online terms of service are living documents, subject to frequent change with only minimal requirements for informing users about modifications. Even among individuals who are confident in their understanding of these policies, 66% have significant misconceptions about what service providers will or will not do on the basis of those agreements (Turow, 2003).

These arguments are important, and will continue to structure academic and policy-oriented discussions of how best to protect individuals online. But the broader problem—and one engaged with in this article—is one of practice. Would even a well-informed reading of an ideally written policy correspond with the actual experience of using an application or service? The basic assumption is that there exists a necessary and direct correspondence between what a company says it does in its user agreements and what a company actually does—and, crucially, why it does it. Knowing the rules may not be enough. This article reframes an analysis of terms of service in more practical terms: How do these policies translate into actual, user-facing practices of content management? More importantly, what do these policies indicate about the internal logic of service providers?

Objectionable, indecent, and pornographic

In February 2012, a former employee of oDesk, a company contracted to screen user-generated content on Facebook, leaked a copy of the service’s operating guidelines (Chen, 2012). Content screeners are instructed to review any material that Facebook users have flagged as offensive or inappropriate and determine whether
an actual violation of Facebook’s Community Standards (Facebook, n.d.) has taken place. The list of forbidden content is extensive, with 50 separate items for review in nine different categories, including “Sex and Nudity,” “Illegal Drug Use,” and “Graphic Content.” Among the myriad types of banned content are depictions of “any obvious sexual activity” (including in instances where no nudity is actually displayed), “female nipple bulges,” urine, feces, vomit, semen, pus, and earwax. The guidelines also ban photos of mothers breastfeeding, a policy that prompted a widespread backlash against the service in 2008 (Calhoun, 2008; Ibrahim, 2010). The real absurdity of the guidelines, comments Tarleton Gillespie (2012), is the need “to draw this many lines in this much sand.”

The leaked guidelines are compelling because they offer a rare look into the otherwise closed system of content review on Facebook. The process by which content is evaluated is completely opaque to users: The Community Standards—the only guidelines offered to users about what they may or may not post—are notoriously vague, and content disappears from view without explanation when moderated. The reasoning behind these content restrictions is likewise seldom made clear to users, though compliance with state and national laws is high on the site’s list of priorities.

Whatever the reasons for the restrictions, the fact that Facebook at all limits the content users are permitted to post has the effect of constituting a normative intervention on the part of the service into broad cultural controversies.

When Facebook steps into these controversial issues, decides to authorize itself as custodian of content that some of its users find egregious, establishes both general guidelines and precise instructions for removing that content, and then does so, it is not merely responding to cultural pressures, it is intervening in them, reifying the very distinctions it applies. (Gillespie, 2012)

This is not to advocate an “anything goes” policy; limiting certain types of patently reprehensible content (child pornography, rape, bestiality, and self-mutilation are classic examples) is not only legally required but also generally ethically unproblematic. But reasonable or not — ethically, legally, and technologically justifiable or not — the fact that Facebook declares certain types of content off-limits at all is normatively motivated, whether or not Facebook’s developers and users recognize it as such. The problem, suggests Gillespie, is that those norms are never made transparent to Facebook’s users.

The content policies of the gay-targeted social networking services examined in this article are a good deal narrower in focus. Yet, as is the case with Facebook, embedded in each of their policies is a core set of frequently recurring normative positions governing what content is considered “acceptable” within the context of gay-targeted social media. Excavating those positions requires a closer examination of the guidelines each service makes available to its users.

Each service begins with an extremely broad set of proscriptions on user behavior. Manhunt’s published “Terms of Access and Use” offer a representative example: Under
the miscellaneous heading of “Additional Use Restrictions,” the Manhunt terms of service indicate that users are expressly prohibited to:

Upload, post, e-mail or otherwise transmit any information, data, text, software, music, sound, photographs, graphics, video, messages or other materials (collectively, “Content”) that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another’s privacy, hateful, sexually intolerant or racially, ethnically or otherwise objectionable. (Manhunt, 2009c)

Similar language appears in both the Grindr and Scruff “Terms of Service,” which further broaden the category of prohibited content to include that which is “objectionable,” “indecent,” “pornographic,” “embarrassing,” or “otherwise inappropriate, regardless of whether this material or its dissemination is unlawful” (Grindr, 2012; Scruff, 2012). While indecency has been adjudicated in a general sense over several decades of American jurisprudence (Shafer & Adams, 2005), its specific meaning in the context of these services is left unstated.

Interpreting these policies requires an understanding of their various roles in governing the relationship between services and users. Content management policies rest at the nexus of two sets of standards: first, that which is lawful; and second, that which is proper, as determined outside of and beyond the law. Many of the published guidelines focus on ensuring the legal status of these services, such as prohibitions on mentions of recreational drugs or escorting and “massage” (typically code for solicitations for sex for money). But in each case, the TOS documents for Manhunt, Grindr, and Scruff establish a broader class of content that is forbidden within the context of these services, regardless of legality. This is not just a question of legal rhetoric; it is a normative declaration that what the law considers objectionable is, in some instances, not sufficient to govern online services.

What do “vulgar,” “obscene,” “objectionable,” and “indecent” look like in practice on these services? Manhunt, Grindr, and Scruff each translate their legal TOS and EULA documents into a set of operational guidelines for end users, often in significant and graphic detail (Grindr, n.d.; Manhunt, 2009a, 2009b; Scruff, n.d.). Manhunt, for example, delimits four categories of photos that are prohibited on the site: photos depicting scatology, urination on a person, blood, or weapons. Photos depicting “mid-stream urine or urination on inanimate objects,” as well as anal insertion and semen “in or around [an] orifice” are allowable, but only if designated as “private” photos, hidden from the general public of Manhunt.

The photo guidelines for Grindr and Scruff are considerably more restrictive. Scruff prohibits all instances of below-the-waist nudity (or partial nudity), including any exposed pubic hair or the display of genitals that are “obscured with hands, towels, hats, or by other means.” Visible erections or “tenting” in one’s clothing that suggests the presence of an erection are likewise forbidden. Grindr adopts a more general approach, writing simply, “No sexually explicit, revealing, or overly suggestive photos of any kind.” The guidelines then elaborate that skin below the hip
bones, exposed underwear, and sexually suggestive objects (Grindr’s now-notorious “fruits and veggies” rule) are not allowed to be displayed in photos. Grindr also prohibits disclosing the size of one’s genitals in the text of a profile, as well as any other references to sexual acts.

The mechanics of content management likewise differ from service to service. All three services encourage their users to police each other and report photos or profiles that violate community guidelines—a common practice across social media services (Albrechtslund, 2008; Andrejevic, 2005). Manhunt and Grindr, however, go further. Manhunt requires that every uploaded photo be screened before it becomes available on the site. The service’s published guidelines make careful note of the fact that the list of restrictions available to users is not exhaustive. The final determination of whether photos are “green,” “yellow,” or “red” is made at the discretion of the Manhunt staff during the photo review process. Grindr, like Manhunt, screens every uploaded photo manually, using a team of photo reviewers (“censors,” as Grindr’s CEO described them in an interview; Easton, 2009) to determine whether a photo violates the service’s profile guidelines. Users are not given access to the internal logic of the review process (including in the event that a decision is made to reject their content), nor do any of the services publicly provide information about who the reviewers responsible for these determinations are. A former Manhunt employee noted, anecdotally, that many of the service’s contracted photo screeners are heterosexual males; but, beyond anecdote, none of the three services were willing to disclose further demographic information about the people in the screening role. Users are encouraged to focus on the outcome of the screening procedure, rather than the process itself.

Some of this variability can be accounted for by considering the technical context of these services. Unlike multidevice social networking services such as Facebook, Grindr and Scruff can be accessed exclusively through mobile applications, distributed through application clearinghouses such as Apple’s App Store or Google Play. Accordingly, mobile-only or mobile-first social networks such as Grindr and Scruff are bound by rules set forth by these distributors. The developers of both Grindr and Scruff emphasize the fact that their content guidelines are designed primarily to ensure compliance with the rules set forth by Apple and Google for developers on their respective mobile platforms. In discussing his app’s restrictions, Grindr’s founder and chief executive Joel Simkhai begins by noting that, “Apple does not allow any nudity or profanity” (quoted in Easton, 2009), positioning Grindr’s specific policies as derived exclusively from externally imposed restrictions—even as Apple’s restrictions (discussed below) do not proscribe nudity or profanity in all instances.

The rhetorical logic herein is clear: Developers remind their users that apps distributed through mainstream smartphone application clearinghouses require more restrictive content standards. The narrative presented to users is that, faced with the choice between not offering an application at all or abiding by Apple and Google’s rules, developers have opted to limit the types of content available on their services for the users’ benefit. This focus on externally imposed developer guidelines reframes
the discourse around content management practices. In particular, it shifts the responsibility for these policies off of application developers and onto Apple and Google. As Grindr’s founder and chief executive Joel Simkhai explains, “From day one, we basically used the App Store guidelines as a framework for development.” The ambiguity of these guidelines, Simkhai continues explains the Grindr staff’s cautious development approach:

Apple and Google don’t have very specific guidelines—sometimes they can be quite vague. Trying to make sense of them is often a Talmudic exercise, so when we drew up the Grindr profile guidelines, we were very conservative in our interpretation of Apple and Google’s guidelines.

By focusing on the rules set forth by Apple and Google, Simkhai downplays the internal design process behind Grindr as a factor in developing content restrictions. The choices were made for Grindr by Apple and Google, rather than by Grindr’s staff. This explanation has caught on in popular discussions about the restrictions. Writing about an updated version of Grindr, the blog Queerty notes:

Software makers revise their guidelines all the time, but nobody tightens the rules faster than developers subject to Apple’s increasingly stringent rules about what can be sold in its iPhone app store. … [Grindr] has, because of the App Store’s existing rules, never allowed members to display naked photos in their main profile pictures. But updated rules go much farther. (Queerty, 2010)

In 2010, when Grindr’s amended profile guidelines went public, Apple had not substantially modified any section of its published developer guidelines, including sections that would affect services such as Grindr. Most observers of Grindr’s policy change presumed that Apple was responsible for the tightened restrictions, and Grindr’s developers did little to dispel that assumption.

But what do Apple and Google’s developer guidelines actually say? Are they sufficient in themselves to account for the policies in question? Apple’s developer guidelines are a combination of practical injunctions and broad ideological statements:

We view Apps different [sic] than books or songs, which we do not curate. If you want to criticize a religion, write a book. If you want to describe sex, write a book or a song, or create a medical App. It can get complicated, but we have decided not to allow certain kinds of content in the App Store. …

We will reject Apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, “I’ll know it when I see it.” And we think you will also know it when you cross it. (Apple, 2013)

The guidelines are more specific on the issue of pornography, noting that apps containing objectionable, crude, or patently pornographic material (user-generated or not) will not be distributed through the App Store. Google likewise notes that pornography, nudity, graphic sex acts, and sexually explicit material are all prohibited in
applications distributed on Google Play (Google, n.d.). While potentially ambiguous, these policies do not, in themselves, prohibit the full spectrum of content addressed in the Grindr, Scruff, and Manhunt guidelines.

We can account for the gap between platform policies and specific app practices in two ways. First, as Luis Hestres (2013) argues, these policies constitute an important and non-content-neutral restriction on developer behavior. This is the most direct explanation of control: App developers constrain user behavior because Apple and Google specifically proscribe certain types of content. But, in practice, these restrictions tend to be considerably more restrictive than direct control alone could account for. These platform-wide policies can create a chilling effect on developer behavior: Rather than running the risk of violating platform rules, developers might elect to be more conservative in their specific policies from the outset. This is the explanation offered by Grindr, Scruff, and Manhunt. Few services, however, acknowledge their own normative interventions into this process: An important act of translation occurs between the Apple and Google developer policies and the rules users actually engage with. Herein, both platform curators such as Apple and Google and application developers behave in a non-content-neutral manner. In practice, this results in content policies that are more specific and comprehensive than a hypothetical least-restrictive-alternative that would comply with the strictures of platform rules.

Normative platforms

In the early days of Web 2.0, interactive electronic content was seen as a boon for the agency of individual users. Free expression—of identities, of diverse viewpoints, of artistic creations—could be facilitated through open access to online services. As Andrew Barry optimistically put it, the logic of online interactivity is “You may!” not “You must!” (Barry, 2001, p. 149). But in practice, “may” and “must” have turned out to be two sides of the same coin. User behavior online has not only tended to be constrained, but in fact is engineered from the ground up in a manner that cannot help but be constrained. These constraints emerge in the content restrictions examined in this article. The key to understanding content restrictions is to position them in the broader sociotechnical context that authorized their creation in the first place.

Tensions over the normative characteristics of electronic services have tended to cluster around the management of user-generated content. The politics of content management play out in the discursive construction of platforms as a way to describe online service providers. The general characteristic of an ideal platform is that it is an “open, neutral, egalitarian and progressive support for activity” (Gillespie, 2010, p. 352)—that it exhibits the quality of content neutrality while giving users a medium for self-expression. An ideal platform, to return to Barry’s phrase, tells users, “You may!” and gives them the tools with which to do so.

In practice, the term “platform” has been applied to services that only rarely exhibit content neutrality and openness. In José van Dijck’s words, oftentimes a platform “shapes the performance of social acts instead of merely facilitating them” (van Dijck, 2009, 2013, p. 29). The idea of a platform has its own particular set of affordances. In
No Overly Suggestive Photos of Any Kind

Y. Roth

particular, calling a service a “platform” downplays the responsibility of the service’s owners and developers for the content they distribute:

Online content providers who do not produce their own information have long sought to enjoy limited liability for that information. … In the effort to limit their liability not only to these legal charges but also more broadly to the cultural charges of being puerile, frivolous, debased, etc., intermediaries like YouTube need to position themselves as just hosting—empowering all by choosing none. (Gillespie, 2010, p. 357)

By referring to a service as a “platform,” the burden for choices about content restrictions is shifted from the developer onto larger structures of constraint, such as legal requirements and nebulous social standards such as “common decency.” More generally, the rhetoric of platforms makes content management practices susceptible to what Zygmunt Bauman (1995) has termed “adiaphorization”: that certain activities, particularly by organizations, are rendered as outside of the sphere of moral or ethical evaluation. The rightness or wrongness of the rules in question becomes irrelevant; instead, “It’s not my department” becomes a characteristic means for deferring, potentially indefinitely, responsibility for the normative outcomes of enforced policies (Bauman & Lyon, 2013, p. 13; Clegg & Rhodes, 2006, p. 7).

I argue that these practices of normative deferral become yet more problematic when they take place in a digitally mediated institutional context. In the classic words of Lawrence Lessig (1999), code is law—and content management is represented to its users as a set of encoded, technical rules. But, As Wendy Chun puts it, code is better than law:

[Code is] an inhumanly perfect “performative” uttered by no one. Unlike any other law or performative utterance, code almost always does what it says because it needs no human acknowledgement. … Moreover, whereas a law’s effectiveness depends on enforcement (self- or otherwise), code’s enforcement stems from itself. (Chun, 2006, p. 66).

By eliminating the speaker (the developer or designer of an application) from the equation, code reifies rules of conduct in a way that forecloses most opportunities for disagreement. We forget that those rules of conduct—the principles encoded in software through programming—had their origin in the mind of a developer, and accordingly represent a particular ideologically motivated vision of how an application or service should operate.

The image approval processes of services such as Manhunt and Grindr are presented as constraints resulting from technical systems even as they manage user-generated content by encoding human norms about controversial or sensitive material in only quasi-technical terms. But this humanness is seldom revealed to users. The reviewers responsible for screening submitted photos operate in a black box. Photos, as if by magic, are approved, rejected, classified, and edited, with no revelation of the underlying mechanism. Hints of the human underbelly of technical
platforms are revealed only by accident, as in the case of the leak of the Facebook content guidelines.

At stake in these conversations is the place of values in the design of online services. As Helen Nissenbaum valuably recognizes, accounting for the operation of values in and through technology requires a broad analysis of the interplay “between the system or device, those who built it, what they had in mind, its conditions of use, and the natural, cultural, social, and political context in which it is embedded” (Nissenbaum, 2001, p. 120). Many of these factors are challenging to account for—Can we ever accurately discern what the developers of a technology truly had in mind?—but acknowledging their presence in the design process denaturalizes the choices that contribute to the emergence of certain types of technological systems. The developers of technologies have a corresponding ethical obligation to explicitly integrate some consideration of social values into their design processes (Flanagan, Howe, & Nissenbaum, 2008; Friedman, 1996; Friedman & Nissenbaum, 1996).

Conceiving of social services as value-neutral platforms has the effect of creating a “comforting sense of technical neutrality” (Gillespie, 2010, p. 360). But this obscures the broader political questions at stake: Do these services have responsibilities—and if so, to whom? The desires of a majority of their users? The law? Their shareholders? Where, if anywhere, can the particularities of political conflict, history, and subcultural construction be integrated into this understanding of how online service providers operate? Striking this balance is an inherently nonneutral process. Reconceptualizing these choices as the active negotiation of social responsibility would enable service providers to integrate value-sensitivity into their design process in a more robust way than the doctrine of platform neutrality allows.

Content management policies are an important instantiation of nonneutral design choices. Where the normative character of these policies is made properly visible to users and developers alike, it affords them the opportunity to engage with those struggles in a robust, value-centric way. The neutral rhetoric of platforms, by contrast, privileges the technological status of these services over their cultural valences. Value-sensitive design is of particular importance as an analytic framework when traditionally marginalized values are more contextually prominent than others, as is the case on these services.

**Negotiating gay visibility online**

In the cases of Manhunt, Grindr, and Scruff, a particular set of histories and struggles over the visibility of queer sexualities are implicated by virtue of their status as gay-targeted services. Gay-targeted online networks have existed for more than two decades, beginning with social spaces such as Usenet groups (O’Riordan, 2005) and Internet Relay Chat rooms (Campbell, 2004). The services examined in this study constitute the second and third generations of gay social media—services that are built around allowing users to express themselves with higher-bandwidth media like...
photos (as opposed to only text), and that take advantage of emergent technologies like geolocation and always-on mobile data connections. Yet, as gay-targeted social media have matured technologically, they have also become more restrictive of the types of content their users are permitted to share. This normative question has significant historical roots in and ramifications for Western gay politics.

The practices of content management taking place on gay-targeted social networking services parallel long-standing offline debates over the visibility of gay sexuality. Tearooms, bathhouses, and cruising areas—sites where certain types of gay sexuality can become visible to the public—played a significant role in structuring gay politics throughout the 20th century. The disavowal of highly visible forms of gay sexuality by mainstream gay organizations represented a significant and controversial turning point in the history of American gay politics. A wide range of scholarship has chronicled various facets of this shift—from public health to urban zoning laws to the emergence of a new “homonormativity” that privileges private, moderate, and often implicitly seronegative homosexuality (Berlant & Warner, 1998; Delany, 2001; Elovitz & Edwards, 1996; Seidman, 1992; Warner, 1999).

By consistently restricting the display of certain types of sexual content, social networking services such as Grindr and Manhunt are entering into these debates—whether or not they acknowledge their actions as doing so. Content management is an essentially political process. Prioritizing the technical nature of this process over its normative dimensions obscures political tensions that can and should be a part of the design and operation of social networking services.

This is not to say that every social networking service is obligated to subscribe to a version of gay politics that prioritizes highly visible sexuality. Gay social networking services are not a one-size-fits-all proposition. This logic is not new, or specific to gay social networking services (boyd, 2007). Different social networking services may appeal differently to particular segments of a population. Users who feel that they do not fit on omnibus services such as Manhunt, Grindr, or Jack'd can jump ship to their competitors, such as Scruff or Mister. Larger-bodied or more hirsute men may be drawn to Scruff instead of Grindr. Older men might prefer Mister. Ultimately, users of gay social networking services pragmatically seek out the applications that “work” for them—ones that offer the greatest number of social gratifications with the fewest burdens or barriers to participation.

Manhunt, Grindr, and Scruff are not developing software with the intention of marginalizing certain types of people. Inclusivity of a wide range of users, ease of access, and ubiquity unsurprisingly emerge as the dominant discourses in the marketing materials of each of these services. As Manhunt’s slogan puts it, “If he’s out there, he’s on here”—implying that users will have a better experience if the network they are a part of includes as large a segment of the gay population as possible. This logic directly informs these services’ approach to content management. At the core of their practices is the belief that the pursuit of a broad base of potential users and the overt display of sexual (or even highly suggestive) content are mutually exclusive.
The negotiation of overtness is at the heart of the content management practices of gay-targeted social networking sites. In the words of Grindr’s Simkhai,

We didn’t want our users to experience logging into Grindr and instantly seeing unexpected or unwanted nudity. … We want Grindr to be inclusive. A lot of the services that came before Grindr were more overt, and we think that narrowed the appeal and the experience of using those services.

The key to understanding these choices is a qualitative recognition of what kind of space a given application is supposed to be. Simkhai suggests that part of Grindr’s viability as a social network is based on keeping erotic images hidden from view. Content that falls outside of the boundaries of the Grindr profile guidelines is taken at face value by Grindr’s developers to be disruptive to the safe and enjoyable operation of the Grindr service.

But what are services like Grindr actually for? What types of interactions are disrupted by the overt presence of erotic images? The motivations of the users of gay-targeted social networking services are often diverse and not restricted to the solicitation of sexual partners, although “hooking up” is an important and frequently cited use (Crooks, 2013; Gudelunas, 2012; Landovitz et al., 2012; O’Bryan, 2012; Vernon, 2010; Worthingham, 2013). Grindr’s popularity is at least in part a product of enabling that diversity by embracing the polysemy of the service: Grindr’s developers refer to the service as a “gay friend finder,” cautious and possibly euphemistic rhetoric that leaves the actual negotiation of the service’s use open to users. Users are left to determine for themselves the character of their in-app interactions.

Whatever the actual use-cases of these apps, users have rejected the premise that effective gay social networking requires hiding sexual or suggestive content from public view. Many cite these policies as disruptive to their experiences using these apps. In the case of Grindr, for example, the service’s content policies are a frequently recurring theme in the more than 30,000 reviews of the application in the Apple App Store. Many users refer to content policies as a form of censorship on the part of the app’s developers. These policies, users contend, are at odds with the idea of a social service targeted at adults. “I can understand no nudity,” writes one user, “But these guys go overboard.” The seeming arbitrariness of the guidelines — and the fact that other social services do not similarly restrict user content in such a granular manner — appeared often in users’ complaints. As one user notes, “If Facebook approves a photo … shouldn’t a site like this?” These accounts have been repeated in mainstream and online press coverage. An article published in Vanity Fair referred to Grindr’s content policies as akin to “the student handbook at a parochial school” (Kapp, 2011), and a number of the most trafficked gay blogs have called the practices “puritanical” or “prudish” (Easton, 2009; Queerty, 2010; Towle, 2010).

Despite public outcry about the policies, users have been ineffective in prompting widespread changes in policy. Developers are able to resist public pressure by framing the rules of their services as technically derived, rather than normative (and therefore
open to contestation). Users themselves occasionally repeat these explanations. As one reviewer of Grindr notes, “Most of the negative reviews here ... seem to be primarily by folks expecting some sort of x-rated free for all on an app store product.” In this account, the App Store, not Grindr, is responsible.

Additionally, the all-or-nothing approach of these policies precludes many forms of resistance by definitionally excluding users who disagree. Users can either accept the terms of service, or opt-out altogether. In the words of a Grindr user, “The worst part of the app is that it might be the best app like it in the app store.” Despite frequently expressed and often quite vehement criticism, users decline to opt out. Opting out as a strategy of resistance has its own corresponding set of constraints. Peer pressure and collective inertia create significant disincentives to “vote with one’s feet” and leave a particular service. The dominance of a small number of services means that electing to use their less popular competitors necessarily reduces the number of available connections. The fact that millions of users continue to do business with Grindr, Manhunt, and Scruff should not be taken as a strong indicator of their approval of the services’ practices; at best, it demonstrates that the disincentives of leaving are not outweighed by the potential benefits of networking elsewhere.

In lieu of opting out altogether, users often elect to use particular gay-targeted social networking services for contextually specific purposes. David Gudelunas (2012) reports that, among his respondents, some indicated having 7 to 10 active profiles across different services. These profiles are not redundant. Instead, users present themselves in different ways on different services, both in accordance with the rules of the service and based on their own expectations of what types of interactions a particular network has to offer. These profiles, Gudelunas notes, “were not seen as discrete entities, but rather as part of an elaborate network”—a fragmented, yet coherent, version of individual identity online that accounts for the differential permissions and gratifications afforded by social services. Opting-out altogether is a last resort.

Even within the context of a particular service, users are not completely disempowered by sociotechnical constraints. Rather, behavior is dialogically negotiated on an ongoing basis, often in ways that neither the user nor the developer would initially anticipate (Best & Tozer, 2013). Some users creatively engage with the rules of technologies they encounter in order to make externally imposed boundaries more personally comfortable or agreeable. They can, borrowing from Michel de Certeau (1988), work tactically within systemic constraints to achieve a desired outcome. While Grindr and Manhunt’s manual photo review processes leave little room for circumventing guidelines about images, users nevertheless display prohibited content on their profiles in only slightly disguised ways. On Grindr and Scruff, for example, users employ pictograms known as “emoji” to identify as either the penetrating (“active” or “top”) or penetrated (“passive” or “bottom”) partner in anal sex—explicit references to sexual activity that are prohibited under the content guidelines. Through the use of the emoji “;top,” “;bottom,” and “;penetrated,” users maintain compliance with the text of the content policies, even as their profiles convey information that would otherwise not be permitted. Likewise, some seropositive users of Grindr and Scruff
work around the lack of a formal interface element for disclosing seropositivity by including a bracketed “[+]” in their profile headline. The limitations of a particular service—whether created by explicit proscription in content guidelines or through the omission of a particular feature—nevertheless leave room for a limited amount of user negotiation.

In some instances, developers have responded to these encoded practices by integrating specific mentions of user vernacular into content guidelines. For example, across the services examined in this study, users deploy terms such as “partying” (a general reference to the use of recreational drugs), “skiing” (a specific reference to cocaine), and “420” (a specific reference to marijuana) to make their interests legible to other users while not running afoul of laws or the rules of a service. Manhunt, in response, has specified the grammatical circumstances within which the term “party” may be used, in an effort to combat drug references in user profiles: “The term ‘party’ isn’t allowed when used as a verb or adjective, but as a noun such as in ‘sex party, dinner party’ or ‘group party’ it is allowed” (Manhunt, 2009b). These guidelines recognize the possibility that, in online spaces, users may attempt to subvert services’ limitations on their conduct by encoding discussions of their practices in ways that are legible only to other members of the community—to circumvent the rules, albeit covertly.

Proscribing and algorithmically detecting the use of emoji to express overtly sexual content on profiles would be trivial, from a programming perspective. Grindr and Scruff could, as does Manhunt, identify and prohibit coded linguistic tactics of user misbehavior in their terms of service. In practice, they do not. The specificity of many of the content policies indicates that developers have invested a great deal of time and effort in understanding what users do on their services, and how best to govern their conduct. Developers are not ignorant of what their users are doing; instead, in select instances, they appear to behave as though they are. The fact that Grindr, Scruff, and Manhunt are vigilant about enforcing some content restrictions while allowing for what Foucault calls a “margin of tolerated illegality” (Foucault, 1978, p. 82) in others, suggests that the normative prioritization of certain values is inseparable from the presumptively “neutral” practices of platform stewardship. Certain practices are selected as worthy of specific proscription in content guidelines, whereas others go unacknowledged—and therefore are permitted by default (until or unless a service’s developers specify otherwise). On the whole, user-generated content is still tightly controlled, and certain practices remain categorically marginalized; but the highly specific policies these services adopt are effective in creating a zone of plausible deniability within which user behavior may be relatively less constrained. The specificity of technical management gives rise to the possibilities of individual resistance.

Conclusions: The managed face of gay community

Services such as Grindr, Manhunt, and Scruff are increasingly regarded as the new popular front of gay sociality. But what values are embedded in the networks created
by these applications—and what are their consequences for gay communities, both on- and offline? Even as these services bring together millions of users from across the globe, certain elements of gay culture have been systematically pushed to the margins. The homosocial is made visible by calling these services “friend finders,” while the homosexual is marginalized. Nonnormative practices—fetishistic, “unsafe,” or highly visible sexualities, for instance—are consistently hidden from view. Where nonnormative or overtly sexual discourses persist, they only manage do so tactically, as a form of resistance. And as the user base for these services continues to grow, the stakes for this elision will only become greater.

The technical systems that frame these services obscure the relations of power encoded in them. Presenting a content policy as the product of technological requirements rather than normative ones reduces opportunities for user resistance and self-expression. Hiding certain types of sexuality from view on social networking services is not to say that they do not exist; but diminishing their visibility is in itself a value judgment and an affordance for a particular and limited type of representation. These are normative considerations, not technological ones—considerations that have important consequences for the agency of individual users as well as the visibility of diverse practices and patterns of self-expression in gay communities. As social applications continue to become more prominent, particularly in subcultural communities, frameworks of values and norms will be indispensable in the design and management of technical systems. Technological and legal considerations alone are insufficient.

Acknowledgments

The author would like to thank Sharrona Pearl, Carolyn Marvin, Lance Wahlert, and the anonymous reviewers for their feedback.

References


No Overly Suggestive Photos of Any Kind

Y. Roth


