Article

Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder

Christoph Lutz[1] and Giulia Ranzini[2]

Abstract

The widespread diffusion of location-based real-time dating or mobile dating apps, such as Tinder and Grindr, is changing dating practices. The affordances of these dating apps differ from those of "old school" dating sites, for example, by privileging picture-based selection, minimizing room for textual self-description, and drawing upon existing Facebook profile data. They might also affect users' privacy perceptions as these services are location based and often include personal conversations and data. Based on a survey collected via Mechanical Turk, we assess how Tinder users perceive privacy concerns. We find that the users are more concerned about institutional privacy than social privacy. Moreover, different motivations for using Tinder—hooking up, relationship, friendship, travel, self-validation, and entertainment—affect social privacy concerns more strongly than institutional concerns. Finally, loneliness significantly increases users' social and institutional privacy concerns, while narcissism decreases them.

Keywords

privacy, social networks, online relationships, mobile dating, Tinder

Introduction

Global positioning system (GPS)-based dating apps such as Tinder and Grindr brought about a small revolution in the way individuals meet, interact, and sometimes fall in love with each other. In fact, thanks to their mobile status making them portable as well as easily accessible, they have contributed to both improving the diffusion of online dating and significantly reducing the stigma associated with it (Smith & Anderson, 2015). A 2015 study from Pew Research determined that in the course of 10 years, the percentage of Americans who believe that online dating is "a good way to meet people" has increased from 44% to two thirds of the population (Smith & Anderson, 2015). Despite early media coverage depicting location-based real-time dating (LBRTD) apps as being the highest expressions of hookup culture[1] (Sales, 2015), and depicting their users as "*looking for love, or sex, or something*" (Feuer, 2015), research has highlighted how Tinder users might be aiming at more than instant gratification (Duguay, 2016) and responding to a number of different needs (Ranzini & Lutz, 2017). Both such characteristics could help explain the enormous success of apps such as Tinder, currently in use by more than 25 million individuals.

However, the mobility of Tinder and similar apps, as well as their use of GPS to minimize the time between an online and offline encounter, is what made them emerge over the competition of dating platforms and what has attracted the attention of research so far. Previous studies have concentrated on how "matching" on an LBRTD app might be an attempt for users to "co-situate" themselves, that is, exist in a parallel within a place that is both physical and virtual (Van de Wiele & Tong, 2014). In this sense, for lesbian, gay, bisexual, transgender, and queer (LGBTQ) communities, apps such as Grindr or Brenda have represented an important cultural shift into creating and performing a community without a shared physical place (Blackwell, Birnholtz, & Abbott, 2014; Fitzpatrick, Birnholtz, & Brubaker, 2015).

[1]BI Norwegian Business School, Norway
[2]VU University Amsterdam, The Netherlands

Corresponding Author:
Christoph Lutz, Department of Communication and Culture and Nordic Centre for Internet and Society, BI Norwegian Business School, Nydalsveien 37, NO-0484 Oslo, Norway.
Email: christoph.lutz@bi.no

The exploration of motivations behind users' self-presentation on LBRTD apps has been an important topic within the emerging field of online dating research so far (Duguay, 2016; Ranzini & Lutz, 2017). To this day, however, the topic of users' privacy concerns, especially in connection with their motivations, remains relatively understudied. We wish to cover this gap, approaching Tinder as a platform where privacy and privacy concerns are important aspects to consider.

The goal of this article is thus to explore Tinder users' privacy concerns, connecting them to their motivations and demographic characteristics. In more detail, we distinguish social and institutional privacy concerns. Since Tinder is a mobile and location-based app, we will consider specific mobile affordances that are unique to this type of dating service. We will first discuss literature on the affordances of mobile media and LBRTD as well as previous research on privacy online and location-based services in particular. The theoretical foundation for the empirical parts of this article is built upon this literature. After presenting the sample, measures, and method, we will discuss the results. We will then conclude with a short summary of the results, implications, and limitations of our approach.

Theoretical Background

Affordances of Mobile Dating and Tinder

LBRTD apps such as Tinder belong to the genre of mobile media. They include communicative affordances which differentiate them from traditional web-based online dating services such as Match.com (Marcus, 2016). Schrock (2015) summarizes the previous literature on the affordances of mobile media and proposes four key affordances: portability, availability, locatability, and multimediality. Tinder relies on all four of these communicative affordances. Thanks to the portability of tablets and smartphones, Tinder can be used in different locations, from public, to semipublic, and private spaces. Traditional desktop-based dating sites, on the contrary, are mostly restricted to private spaces. In addition, the availability affordance of mobile media enhances the spontaneity and use-frequency of the app. The locatability affordance facilitates meeting, texting, and matching with users in physical proximity—a key characteristic of Tinder. Finally, while the multimediality affordance seems limited on Tinder, the app relies on at least two modes of communication (texting and photo sharing). Users can also link their Instagram profiles with Tinder, enabling greater multimediality. As soon as they are matched, the users can then continue the conversation through other media such as video messaging, snapchatting or phone calls (Marcus, 2016).

Tinder adds specific affordances to those affordances coming from its mobile status (David & Cambre, 2016; Duguay, 2016; Marcus, 2016). For example, its forced connection with a Facebook profile represents what early social media studies described as "an anchor" (Zhao, Grasmuck, & Martin, 2008), that is, a further source of identification that better situates an online identity in an offline environment. Furthermore, Marcus (2016) defines Tinder's dependence on Facebook as affordance of "convergenceability": The information on users' profiles is automatically filled-in, allowing them to spend less time and efforts in self-presentation. An additional affordance of Tinder is its reliance on visual self-presentation through photos (David & Cambre, 2016). According to Marcus (2016), users rely on limited information to make swiping decisions specifically because of this heavy reliance on photos.

Two additional affordances of Tinder are its mobility affordance and its synchronicity affordance (Marcus, 2016). The mobility affordance extends Schrock's (2015) portability affordance of mobile media. Because of its suitability for use in public places, Tinder incentivizes more social uses than traditional dating, accentuating the entertainment component of browsing other people's profiles (Sales, 2015). The synchronicity affordance is instead described as "the short amount of time in which messages are sent" (Marcus, 2016, p. 7). This affordance requires spontaneity and availability from users, as a response to the need to decide quickly on their own self-presentation as well as on whether they like someone else's. The combination of the synchronicity affordance with Tinder's limited information availability represents important constraints on the users, leading to issues such as information overload, distraction from "real life," and a feeling of competition due to the large number of users (Marcus, 2016).

Privacy Online and on Location-Based Services

Many Internet services collect personal information. Such information often includes sensitive data such as personal preferences, health and location information, and financial information in the form of bank account or credit card numbers. Given the huge amount of data collected by private and public actors alike, privacy has become an important topic in the study of digital, social, and mobile media.[2]

Against this background, scholars from various fields have increasingly investigated phenomena related to online privacy and provided different understandings of the concept. The perspectives range from economic (privacy as a commodity; Hui & Png, 2006; Kuner, Cate, Millard, & Svantesson, 2012; Shivendu & Chellappa, 2007) and psychological (privacy as a feeling) to legal (privacy as a right; Bender, 1974; Warren & Brandeis, 1890) and philosophical approaches (privacy as a state of control; Altman, 1975; see Pavlou, 2011, for more on this). Recently, Marwick and boyd (2014) have pointed to some key weaknesses in traditional models of privacy. In particular, such models focus too strongly on the individual and neglect users', especially young users', embeddedness in social contexts and networks. "Privacy law follows a model of liberal selfhood in which

privacy is an individual right, and privacy harms are measured by their impact on the individual" (Marwick & boyd, 2014, p. 1053). By contrast, privacy in today's digital environment is networked, contextual, dynamic, and complex, with the possibility of "context collapse" being pronounced (Marwick & boyd, 2011).

Not surprisingly, some scholars have pointed out that current Internet and mobile applications are associated with a puzzling variety of privacy threats such as social, psychological, or informational threats (Dienlin & Trepte, 2015). In an important distinction, Raynes-Goldie (2010) differentiates between social and institutional privacy. Social privacy refers to situations where other, often familiar, individuals are involved. Receiving an inappropriate friend request or being stalked by a colleague are examples of social privacy violations. Institutional privacy, on the contrary, describes how institutions (such as Facebook, as in Raynes-Goldie, 2010) deal with personal data. Security agencies analyzing vast amounts of data against users' will are an example of an institutional privacy violation. Several studies in the context of social network sites have found that (young) users are more concerned about their social privacy than their institutional privacy (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). As social privacy concerns revolve around user behavior, they may be more accessible and easy to understand for users, highlighting the importance of awareness and understanding. Accordingly, users adapt their privacy behavior to protect their social privacy but not their institutional privacy. In other words, users do tend to adapt to privacy threats emanating from their immediate social environment, such as stalking and cyberbullying, but react less consistently to perceived threats from institutional data retention (boyd & Hargittai, 2010).

Despite a large number of studies on online privacy in general (and specific aspects such as the privacy paradox, see Kokolakis, 2017), less research has been done on privacy for mobile applications and location-based services (Farnden, Martini, & Choo, 2015).[3] As discussed above, mobile applications—and LBRTD in particular—have partly different affordances from traditional online services. GPS functionality and the low weight and size of mobile devices enable key communicative affordances such as portability, availability, locatability, and multimediality (Schrock, 2015). This enhances the user experience and enables new services such as Tinder, Pokémon Go, and Snapchat. However, mobile apps, and those relying on location tracking in particular, collect sensitive data, which leads to privacy risks. Recent media reports about Pokémon Go have highlighted such vulnerabilities of mobile apps (Silber, 2016, as a good example).

In one of the few studies on privacy and mobile media, Madden, Lenhart, Cortesi, and Gasser (2013) conducted a survey among US teens aged 12–17 years. They found that the majority of "teen app users have avoided certain apps due to privacy concerns" (Madden et al., 2013, p. 2). Location tracking seems to be an especially privacy invasive function for the teenagers: "46% of teen users have turned off location tracking features on their cell phone or in an app because they were worried about the privacy of the information," with girls being substantially more likely to do this than the boys (Madden et al., 2013, p. 2). At the same time, recent systems security literature suggests that trained attackers can relatively easily bypass mobile dating services' location obfuscation and thus precisely reveal the location of a potential victim (Qin, Patsakis, & Bouroche, 2014). Therefore, we would expect substantial privacy concerns around an app such as Tinder. In particular, we would expect social privacy concerns to be more pronounced than institutional concerns—given that Tinder is a social application and reports about "creepy" Tinder users and aspects of context collapse are frequent. In order to explore privacy concerns on Tinder and its antecedents, we will find empirical answers to the following research question:

> How pronounced are users' social and institutional privacy concerns on Tinder? How are their social and institutional concerns influenced by demographic, motivational and psychological characteristics?

Methodology

Data and Sample

We conducted an online survey of 497 US-based respondents recruited through Amazon Mechanical Turk in March 2016.[4] The survey was programmed in Qualtrics and took an average of 13 min to fill out. It was geared toward Tinder users—as opposed to non-users. The introduction and welcome message specified the topic,[5] explained how we intend to use the survey data, and expressed specifically that the research team has no commercial interests and connections to Tinder. We posted the link to the survey on Mechanical Turk—with a small monetary reward for the participants—and had the desired number of respondents within 24 hr. We consider the recruiting of participants on Mechanical Turk appropriate as these users are known to "exhibit the classic heuristics and biases and pay attention to directions at least as much as subjects from traditional sources" (Paolacci, Chandler, & Ipeirotis, 2010, p. 417). In addition, Tinder's user base is primarily young, urban, and tech-savvy. In this sense, we deemed Mechanical Turk a good environment to quickly get access to a relatively large number of Tinder users.

Table 1 shows the demographic profile of the sample. The average age was 30.9 years, with a *SD* of 8.2 years, which indicates a relatively young sample composition. The median highest degree of education was 4 on a 1- to 6-point scale, with relatively few participants in the extreme categories 1 (*no formal educational degree*) and 6 (*postgraduate degrees*). Despite not being a representative sample of individuals, the findings allow limited generalizability and go beyond mere convenience and student samples.

Table 1. Demographic Composition of the Sample.

	Absolute numbers	Percentage
Gender		
Male	278	55.9
Female	218	43.9
Other	1	0.2
Total	497	100
Age (years)		
19–20	13	2.6
21–30	272	54.7
31–40	158	31.9
41–50	39	7.8
51 or older	15	3.0
Total	497	100
Education (current or highest school completed)		
High school graduate	57	11.5
Some college	173	34.9
Bachelor's degree or equivalent	203	40.9
Master's degree or equivalent	46	9.3
Doctoral degree or equivalent	12	2.4
Other	5	1.0
Total	496	100
(Missing)	(1)	
Sexual orientation (self-identified)		
Heterosexual	419	84.5
Homosexual	15	3.0
Bisexual	49	9.8
Other	13	2.6
Total	496	100
(Missing)	(1)	

Measures

The measures for the survey were mostly taken from previous studies and adapted to the context of Tinder. We used four items from the Narcissism Personality Inventory 16 (NPI-16) scale (Ames, Rose, & Anderson, 2006) to measure narcissism and five items from the Rosenberg Self-Esteem Scale (Rosenberg, 1979) to measure self-esteem. Loneliness was measured with 5 items out of the 11-item De Jong Gierveld scale (De Jong Gierveld & Kamphuls, 1985), one of the most established measures for loneliness (see Table 6 in the Appendix for the wording of these constructs). We used a slider with fine-grained values from 0 to 100 for this scale. The narcissism, self-esteem, and loneliness scales reveal sufficient reliability (Cronbach's α is .78 for narcissism, .89 for self-esteem, and .91 for loneliness; convergent and discriminant validity given). Tables 5 and 6 in the Appendix report these scales.

For the dependent variable of privacy concerns, we distinguished between social and institutional privacy concerns (Young & Quan-Haase, 2013). We used a scale by Stutzman, Capra, and Thompson (2011) to measure social privacy concerns. This scale was originally developed in the context of self-disclosure on social network sites, but we adapted it to Tinder.[6] Drawing on the previous privacy literature, Stutzman et al. (2011) consider concerns about five social privacy risks: identity theft, information leakage, hacking, blackmail, and cyberstalking. For our survey, we excluded blackmail but kept identity theft, information leakage, hacking, and cyberstalking. The social privacy concerns scale had a Cronbach's α of .906 indicating high reliability and sufficient internal consistence. For institutional privacy concerns, we used the same question format and prompt as for social privacy concerns but instead of other users, Tinder—as the data collecting entity—was the origin of the privacy threat. We included four items covering data protection (or the lack of it) by the collecting institution, in this case Tinder: overall data security, data tracking and analysis, data sharing to third parties, and data sharing to government agencies. These four items were based on the extensive informational privacy literature in general online settings, as found in information systems research in particular (Malhotra, Kim, & Agarwal, 2004, in particular). The institutional privacy concerns scale had a Cronbach's α of .905 indicating high reliability and sufficient internal consistence. The exact wording of all privacy concerns items can be found in Tables 3 and 4 in the Appendix.

We included a wide range of variables on the motives for using Tinder. The use motives scales were adapted to the Tinder context from Van de Wiele and Tong's (2014) uses and gratifications study of Grindr. Using exploratory factor analysis, Van de Wiele and Tong (2014) identify six motives for using Grindr: social inclusion/approval (five items), sex (four items), friendship/network (five items), entertainment (four items), romantic relationships (two items), and location-based searching (three items). Some of these motives cater to the affordances of mobile media, especially the location-based searching motive. However, to cover more of the Tinder affordances described in the previous chapter, we adapted some of the items in Van de Wiele and Tong's (2014) study. Tables 5 and 6 in the Appendix show the use motive scales in our study. These motives were assessed on a 5-point Likert-type scale (*completely disagree* to *completely agree*). They reveal good reliability, with Cronbach's α between .83 and .94, except for entertainment, which falls slightly short of .7. We decided to retain entertainment as a motive because of its relevance in the Tinder context. Finally, we used age (in years), gender, education (highest educational degree on an ordinal scale with six values, ranging from "*no schooling completed*" to "*doctoral degree*"), and sexual orientation (heterosexual, homosexual, bisexual, and other) as control variables.

Method of Analysis

We used principal component analysis (PCA) to build factors for social privacy concerns, institutional privacy concerns, the three psychological predictors, and the six motives

considered. We then applied linear regression to answer the research question and explain the influence of the independent variables on social and institutional privacy concerns. Both the PCA and the linear regression were carried out with the SPSS statistical software package (Version 23). We checked for multicollinearity by displaying the variance inflation factors (VIFs) and tolerance values in SPSS. The largest VIF was 1.81 for "motives: hook up," and the other VIFs were between 1.08 (employment status) on the lower end and 1.57 ("motives: travel") on the higher end. We could, therefore, exclude serious multicollinearity issues.

Results and Discussion

Tables 3 and 4 in the Appendix present the frequency counts for the eight privacy concerns items. The respondents in our sample score higher on institutional than on social privacy concerns. The label that evokes most privacy concerns is "*Tinder selling personal data to third parties*" with an arithmetic *M* of 3.00 (on a 1- to 5-Likert-type scale). Overall, the Tinder users in our sample report moderate concern for their institutional privacy and low to moderate concern for their social privacy. In terms of social privacy, other users stalking and forwarding personal information are the most pronounced concerns, with arithmetic *M*s of 2.62 and 2.70, respectively. The relatively low values of concern might be partly due to the sampling of Tinder (ex-)users rather than non-users (see section "Data and sample" for more information). Despite not having and finding data on this, we suspect that privacy concerns are higher among Tinder non-users than among users. Thus, privacy concerns, possibly fueled by media coverage about Tinder's privacy risks (e.g. Hern, 2016), might be a reason why some individuals shy away from using the app. In that sense, it is important to keep in mind that our results only apply to those already using the app or having used it recently. In the next step, we attempt to explain social and institutional privacy concerns on Tinder.

Table 2 shows the results of the linear regression analysis. We first discuss social privacy concerns. Four out of the six motives significantly influence social privacy concerns on Tinder: hook up, friends, travel, and self-validation. Of these, only hook up has a negative effect. Individuals on Tinder who use the app for hooking up have significantly lower privacy concerns than those who do not use it for hooking up. By contrast, the more that respondents use Tinder for friendship, self-validation, and travel experiences, the higher they score on social privacy concerns. None of the demographic predictors has a significant influence on social privacy concerns. However, two out of the three considered psychological constructs affect social privacy concerns. Tinder users scoring higher on narcissism have significantly fewer privacy concerns than less narcissistic individuals. Finally, the more loneliness the respondents report, the more social privacy concerns they have. It seems that the social nature and purpose of Tinder—as expressed in the variety of motives for using

Table 2. Results of the Linear Regression Analysis.

	Social privacy concerns	Institutional privacy concerns
Motive: hook up	−.114* (.06)	−.072 (.06)
Motive: friends	.130** (.05)	.058 (.05)
Motive: partner	−.025 (.05)	−.043 (.05)
Motive: travel	.134* (.05)	.079 (.06)
Motive: self-validation	.101* (.05)	.039 (.05)
Motive: entertainment	−.061 (.05)	.031 (.05)
Sexual orientation	−.081 (.06)	−.038 (.06)
Gender	.074 (.10)	−.032 (.10)
Education	−.013 (.05)	.001 (.05)
Income	.088 (.07)	.051 (.07)
Employment status	.028 (.03)	.032 (.03)
Age	.045 (.01)	.147** (.01)
Narcissism	−.154** (.05)	−.144** (.05)
Self-esteem	−.025 (.05)	−.053 (.05)
Loneliness	.126* (.05)	.162** (.05)
R^2	.127	.104

N = 491; standardized regression coefficients; standard errors in parentheses.
*p < .05, **p < .01, ***p < .001.

it—has an effect on users' privacy perceptions. It might be that respondents who use Tinder for hooking up perceive privacy risks in general and social privacy risks in particular as unimportant or secondary to their use. Such a functional and more open approach to using the app contrasts with other uses (especially friendship seeking), where users seem to be more concerned about their social privacy. Possibly, individuals who use Tinder for non-mainstream purposes such as friendship, self-validation, and travel might perceive themselves as more vulnerable and at risk for social privacy violations.

Turning to institutional privacy concerns, we find that the motives do not matter at all. None of the six motives assessed has a significant effect on institutional privacy concerns. However, there is a significant age effect with older users being more concerned about their institutional privacy than younger ones. The effects of the psychological predictors are similar to those in the social privacy case. Again, Tinder users scoring higher on narcissism have significantly fewer privacy concerns than less narcissistic individuals do. The higher loneliness scores the respondents report, the more institutional privacy concerns they have. The age effect is partly in line with some previous studies on online privacy concerns in general (e.g. Jones, Johnson-Yale, Millermaier, & Perez, 2009; Palfrey & Gasser, 2008), despite inconclusive evidence overall (see discussion in Blank, Bolsover, & Dubois, 2014, and in Miltgen & Peyrat-Guillard, 2014). A recent study on Facebook among Dutch-speaking adults suggests a differentiated effect of age on online privacy, with older users being more concerned but less protective than younger users (Van den Broeck, Poels, & Walrave, 2015).

Comparing social and institutional privacy concerns on Tinder, we are better able to explain the former. The independent variables explain 13% of the variance in social privacy concerns but only 10% of the variance in institutional privacy concerns. The motives account for the difference in variance explained. It seems that the social nature of most motivations considered (except for maybe self-validation and entertainment) connects more to social than to institutional privacy concerns. In other words, the topic of institutional privacy might be too far removed from the everyday experiences and gratifications of Tinder users to be a matter of concern. The only two independent variables that have a significant impact on both social and institutional privacy concerns are narcissism and loneliness. Users with high loneliness and low narcissism scores express more privacy concerns than the average user. This might indicate a vicious circle, where such users limit or even censor themselves more and might not be able to fully profit from Tinder and its affordances.

Conclusion

This article has investigated privacy concerns on Tinder with a sample of 497 individuals recruited through Amazon Mechanical Turk. In accordance with previous research (Young & Quan-Haase, 2013; Vitak, 2015), we distinguished social privacy (i.e., directed at peers) from institutional privacy concerns (i.e., targeting the app, as well as other organizations or governments). Given the affordances of mobile dating and Tinder in particular, we expected social privacy concerns to be more pronounced than institutional privacy concerns. However, the respondents in our sample revealed more concerns about Tinder as the data collecting entity than about other users. Thus, they worried more about the unintended use of personal data by Tinder than about privacy invasions through other users in the form of stalking, hacking, or identity theft. The respondents expressed most concern about Tinder tracking them, selling their personal data to third parties, and about information leaks.

We then tried to explain social and institutional privacy concerns by testing the influence of motivational, psychological, and demographic predictors. Using linear regression, we could show that narcissism and the motives of Tinder use are the strongest predictors of social privacy concerns. Those with high narcissism scores had the fewest privacy concerns on Tinder. Moreover, individuals who reported using the app for friendship and while traveling expressed more social privacy concerns than those who did not. Interestingly, none of the demographic characteristics exerted a significant influence on social privacy concerns.

The picture was different for institutional privacy concerns. Here, none of the use motives affected the respondents' concerns significantly. Instead, age as a demographic predictor had a comparatively large and positive effect. The older Tinder (ex-)users were significantly more concerned about their institutional privacy than the younger ones. We did not test for skills, awareness of data collection, and privacy literacy. Therefore, we cannot say whether the effect would still hold after controlling for these important factors (Bartsch & Dienlin, 2016; Büchi, Just, & Latzer, 2016; Park, 2013; Park & Jang, 2014).

Overall, our lack of findings concerning the influence of motivation of use on institutional privacy concerns confirms Young and Quan-Haase's (2013) findings about social privacy being a predominant concern for users on social networking sites (SNS). At the same time, the negative effect of narcissism on both institutional and social privacy is coherent with Smith, Mendez, and White (2014). This might highlight how narcissistic Tinder users prioritize self-expression over privacy threats. However, more research is needed to further explore this relationship, possibly even employing a more multifaceted measure for narcissism (Ahn, Kwolek, & Bowman, 2015). The positive relationship between loneliness and both types of privacy concerns represents an interesting insight that should be further explored with future studies.

Our study is one of the first to empirically investigate privacy on Tinder from a social science perspective and to shed light on the relatively new phenomenon of LBRTD. While research has covered the effect of motivations of, for example, Facebook use on users' privacy concerns (Spiliotopoulos & Oakley, 2013), dating apps have not yet been the subject of similar analyses. We think that the lens of privacy is a useful one and hope that future efforts proceed in that direction. While being quite exploratory, our results have several *implications* for research on privacy management in a mobile context, especially mobile dating. In fact, more than standard dating sites, apps such as Tinder emphasize instantaneous decisions, rely on users' location, and are connected with existing services for a more convenient registration and user experience. Viewing the profile of a user who belongs to a user's network can represent an incentive for a match; however, it can lead to the collapse of separate contexts in an individual's virtual life (Marwick & boyd, 2011). As seen in the literature review, networked understandings of privacy (Marwick & boyd, 2014) might be more appropriate to understand users' experiences in this context than individualistic and legal notions. Moreover, we believe that the location-based aspect brings physical privacy back into play. Most research about online privacy, especially in a social media context, revolves around informational privacy (Smith, Dinev, & Xu, 2011). However, with mobile dating apps, their co-situation (Blackwell et al., 2014) and their specific affordances (Ranzini & Lutz, 2017), additional privacy risks emerge when users move their online communication offline by going on dates. This adds a layer of physical privacy to the concept of social privacy concerns, and it introduces a point of connection between online and offline interaction that should be investigated through future research. Our

findings on institutional privacy concerns, instead, should offer some guidance to the providers of LBRTD apps on how they can help user feel safer. In particular, they should do as much as they can to guarantee the safety of user data, especially if they want to extend the user base to older users. Transparency over whether and how other social media, such as Facebook in the case of Tinder, access user data would probably also help decrease concerns related to institutional privacy.

Finally, our study is subject to a number of *limitations*, providing food for thought and many opportunities for future LBRTD research. First, our sample was small, cross-sectional, and composed of a relatively specific, young audience. This limits the generalizability of the results and might explain some of the findings, for example, the low levels of privacy concern and social privacy concerns in particular. Future research is encouraged to use larger samples, if possible with a user base that is representative of the current Tinder user population. It should also compare users and non-user regarding their privacy concerns. Second, we relied on self-reported data, which is subject to a number of problems, such as social desirability, memory bias, and response fatigue (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Unfortunately, we could not collect observational or trace data from the respondents. Future research might use mixed-methods approaches and combine different data sources to investigate the phenomenon more holistically. This could be done by conducting qualitative interviews and including users' data in this process (Dubois & Ford, 2015), for example, by securing informed consent to use the profile picture and/or descriptions. Other promising approaches are big data analyses of actual user profiles; ethnographic inquiries of specific user groups, for example, obsessive Tinder users; and experimental studies that manipulate the constraints and opportunities of self-presentation. Third, with narcissism, loneliness, and self-esteem, we only considered three psychological antecedents. Future research should rely on a more holistic set, such as the big-five personality characteristics. Fourth, our study does not include fine-grained behavioral measures such as engagement levels with different functionalities of Tinder. Users who use the app more actively and reveal much personal information about themselves, for example, through a lot of texting before meeting up with a match, might have more institutional privacy concerns. Future investigations should, therefore, control for the degree of behavioral engagement. Fifth and finally, we could not do justice to contextual factors, such as the cultural background and location of users. A recommendable next step would be to systematically compare different countries and/or regions within a country (e.g., rural vs. urban areas) in terms of Tinder use and privacy. Such comparative analyses might shed light on the cultural contingencies of LBRTD and provide useful guidance and much needed empirical material to better understand the phenomenon.

Notes

1. Bogle (2007, p. 776), distinguishing it from dating, defines hooking up as "a term widely used on campuses to describe heterosexual intimate interaction. [. . .] A hallmark of hooking up is that there are no obligations or 'strings attached' to the encounter." A hookup culture is defined as "a nationwide phenomenon that has largely replaced traditional dating on college campuses" (Bogle, 2008, p. 5).

2. A Google Scholar search for privacy reveals almost 5 million results as of October 2016. In 2016 alone, 220,000 documents with the search term "privacy" and 1,860 documents with the search term "online privacy" have been indexed in Google Scholar so far. This illustrates the huge interest in the topic (see also the systematic review and Zhang & Leung, 2015, which showed that privacy was one of four major key themes in top-tier communication and Internet journals).

3. In fact, despite a few technical publications, we encountered little social science literature on the topic. This is in line with Farnden et al.'s (2015, p. 1) summary, who write,
   Before commencement of our research, we conducted a survey of publications on the general topic of Android mobile device and mobile app user security and privacy published between 1 Jan 20091 and 1 May 2014. When conducting this survey, we found that there was little published work on the privacy implications of GeoSocial Networking (GSN) apps and services.

4. We are aware of the practical problems of Amazon Mechanical Turk as a data source, for example, when it comes to sampling (Paolacci & Chandler, 2014). In addition, serious ethical concerns have been raised toward the platform. Problematic points include low pay, power imbalances between workers and requesters (Kingsley, Gray, & Suri, 2015), and worker invisibility, as a lack of representation and voice (Irani & Silberman, 2013). We attempted to make the survey short and tried to compensate the respondents appropriately. Accordingly, the

reviews posted on Turkopticon for this task were positive, with only 5/5 for pay, fair, and fast.

5. We specified the topic in relatively abstract terms in order not to prime the respondents. The first paragraph of the introduction and welcome message was: "In the following survey, we are interested in your use of Tinder. The questionnaire is for those who are familiar with Tinder and are using it currently or have used it recently."

6. The original question prompt was "Indicate [their] level of concern about the following potential privacy risks that arise when [they] share [their] personal information on Facebook" (Stutzman et al., 2011, p. 592), We adapted it to "Please indicate your level of concern about the following potential privacy risks that arise when you share your personal information on Tinder?"

References

Ahn, H., Kwolek, E. A., & Bowman, N. D. (2015). Two faces of narcissism on SNS: The distinct effects of vulnerable and grandiose narcissism on SNS privacy control. *Computers in Human Behavior*, *45*, 375–381.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole Publishing.

Ames, D. R., Rose, P., & Anderson, C. P. (2006). The NPI-16 as a short measure of narcissism. *Journal of Research in Personality*, *40*, 440–450.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154.

Bender, P. (1974, April). Privacies of life. *Harper's Magazine*, pp. 36–45.

Blackwell, C., Birnholtz, 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*, 1117–1136.

Blank, G., Bolsover, G., & Dubois, E. (2014, August 17). A new privacy paradox: Young people and privacy on social network sites (Vol. 17). *Prepared for the Annual Meeting of the American Sociological Association*, San Francisco, CA. Retrieved from https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2479938

Bogle, K. A. (2007). The shift from dating to hooking up in college: What scholars have missed. *Sociology Compass*, *1*, 775–788.

Bogle, K. A. (2008). *Hooking up: Sex, dating, and relationships on campus*. New York: New York University Press.

boyd, d., & Hargittai, E. (2010, August 2). Facebook privacy settings: Who cares? *First Monday*, *15*(8).

Büchi, M., Just, N., & Latzer, M. (2016). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*. Advance online publication. doi:10.1080/1369118X.2016.1229001

David, G., & Cambre, C. (2016). Screened intimacies: Tinder and the swipe logic. *Social Media + Society*, *2*, 1–11.

De Jong Gierveld, J., & Kamphuls, F. (1985). The development of a Rasch-type loneliness scale. *Applied Psychological Measurement*, *9*, 289–299.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*, 285–297.

Dubois, E., & Ford, H. (2015). Trace interviews: An actor-centered approach. *International Journal of Communication Systems*, *9*, 2067–2091.

Duguay, S. (2016). Dressing up Tinderella: Interrogating authenticity claims on the mobile dating app Tinder. *Information, Communication & Society*, *20*, 351–367.

Farnden, J., Martini, B., & Choo, K. K. R. (2015). *Privacy risks in mobile dating apps*. Retrieved from https://arxiv.org/ftp/arxiv/papers/1505/1505.02906.pdf

Feuer, A. (2015, February 13). On Tinder, taking a swipe at love, or sex, or something, in New York. *The New York Times*. Retrieved from http://www.nytimes.com/2015/02/15/nyregion/on-tinder-taking-a-swipe-at-love-or-sex-or-something-in-new-york.html

Fitzpatrick, C., Birnholtz, J., & Brubaker, J. R. (2015). Social and personal disclosure in a location-based real time dating app. In: *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)* (pp. 1983–1992). New York, NY: IEEE.

Hern, A. (2016, April 5). New website lets anyone spy on Tinder users. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/apr/05/tinder-swipebuster-spy-on-users-privacy-dating-app

Hui, K. L., & Png, I. P. L. (2006). The economics of privacy. In T. Hendershott (Ed.), *Handbooks in information systems: Economics and information systems* (pp. 471–498). Bingley, UK: Emerald Publishing.

Irani, L. C., & Silberman, M. (2013). Turkopticon: Interrupting worker invisibility in Amazon mechanical Turk. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 611–620). New York, NY: ACM.

Jones, S., Johnson-Yale, C., Millermaier, S., & Perez, F. S. (2009, October 5). Everyday life, online: US college students' use of the Internet. *First Monday*, *14*(10).

Kingsley, S. C., Gray, M. L., & Suri, S. (2015). Accounting for market frictions and power asymmetries in online labor markets. *Policy & Internet*, *7*, 383–400.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2012). The challenge of big data for data protection. *International Data Privacy Law*, *2*, 47–49.

Madden, M., Lenhart, A., Cortesi, S., & Gasser, U. (2013, August 22). Teens and mobile apps privacy. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2013/08/22/teens-and-mobile-apps-privacy/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*, 336–355.

Marcus, S.-R. (2016, June 9–13). *"Swipe to the right": Assessing self-presentation in the context of mobile dating applications*. Paper presented at the Annual Conference of the International Communication Association (ICA), Fukuoka, Japan.

Marwick, A. E., & boyd, d (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*, 114–133.

Marwick, A. E., & boyd, d (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*, 1051–1067.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*, 103–125.

Palfrey, J., & Gasser, U. (2008). *Born digital: Understanding the first generation of digital natives*. New York, NY: Basic Books.

Paolacci, G., & Chandler, J. (2014). Inside the Turk: Understanding mechanical Turk as a participant pool. *Current Directions in Psychological Science*, *23*, 184–188.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon mechanical Turk. *Judgment and Decision Making*, *5*, 411–419.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*, 215–236.

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, *35*, 977–988.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*, 879–903.

Qin, G., Patsakis, C., & Bouroche, M. (2014, June 2–4). Playing hide and seek with mobile dating applications. In: N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. A. El Kalam, & T. Sans (Eds.), *Proceeding of the IFIP International Information Security Conference* (pp. 185–196). Berlin, Germany: Springer.

Ranzini, G., & Lutz, C. (2017). Love at first swipe? Explaining Tinder self-presentation and motives. *Mobile Media & Communication*, *5*, 80–101.

Raynes-Goldie, K. (2010, January 4). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1).

Rosenberg, M. (1979). *Conceiving the self*. New York, NY: Basic Books.

Sales, N. (2015). Tinder and the dawn of the "dating apocalypse." *Vanity Fair*. Retrieved from http://www.vanityfair.com/culture/2015/08/tinder-hook-up-culture-end-of-dating

Schrock, A. R. (2015). Communicative affordances of mobile media: Portability, availability, locatability, and multimediality. *International Journal of Communication Systems*, *9*, 18.

Shivendu, S., & Chellappa, R. K. (2007). An economic model of privacy: A property rights approach to regulatory choices for online personalization. *Journal of Management Information Systems*, *24*, 193–225.

Silber, R. (2016, August 1). Apps are disrupting traditional industries — and your privacy. *CNBC*. Retrieved from http://www.cnbc.com/2016/08/01/pokemon-go-and-other-apps-are-putting-your-privacy-at-risk.html

Smith, A., & Anderson, M. (2015). 5 Facts about online dating. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2015/04/20/5-facts-about-online-dating/

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*, 989–1016.

Smith, K., Mendez, F., & White, G. L. (2014). Narcissism as a predictor of Facebook users' privacy concern, vigilance, and exposure to risk. *International Journal of Technology and Human Interaction*, *10*, 78–95.

Spiliotopoulos, T., & Oakley, I. (2013). Understanding motivations for Facebook use: Usage metrics, network structure, and privacy. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3287–3296). New York, NY: ACM.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*, 590–598.

Van De Wiele, C., & Tong, S. T. (2014). Breaking boundaries: The uses & gratifications of grindr. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (pp. 619–630). New York, NY: ACM.

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, *1*(2).

Vitak, J. (2015, July 22–24). *Balancing privacy concerns and impression management strategies on Facebook*. Symposium on Usable Privacy and Security (SOUPS), Ottawa, Ontario, Canada. Retrieved from https://cups.cs.cmu.edu/soups/2015/papers/ppsVitak.pdf

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*, 193–220.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*, 479–500.

Zhang, Y., & Leung, L. (2015). A review of social networking service (SNS) research in communication journals from 2006 to 2011. *New Media & Society*, *17*, 1007–1024.

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, *24*, 1816–1836.

Author Biographies

Christoph Lutz (PhD, University of St. Gallen) is an Assistant Professor at the Nordic Centre for Internet and Society, BI Norwegian Business School (Oslo). His research interests include digital inequality, privacy, participation, the sharing economy, and social robots.

Giulia Ranzini (PhD, University of St. Gallen) is a Professor of Communication at the Vrije Universiteit Amsterdam. Her research interests include self-presentation on social media and users' perception of privacy.

Appendix

Table 3. Distribution of the Social Privacy Concerns Items.

Question prompt	Answer option	Absolute numbers	Percentage
Please indicate your level of concern about the following potential privacy risks that arise when you share your personal information on Tinder?			
Other users engaging in identity theft:	No concern at all (1)	109	21.9
arithmetic $M = 2.44$; $SD = 1.14$	Low concern	182	36.6
	Moderate concern	108	21.7
	High concern	72	14.5
	Very high concern (5)	26	5.2
	Total	497	100.0
Other users hacking into my account:	No concern at all (1)	123	24.7
arithmetic $M = 2.42$; $SD = 1.12$	Low concern	177	35.6
	Moderate concern	97	19.5
	High concern	65	13.1
	Very high concern (5)	35	7.0
	Total	497	100.0
Other users stalking me:	No concern at all (1)	100	20.1
arithmetic $M = 2.62$; $SD = 1.24$	Low concern	161	32.4
	Moderate concern	110	22.1
	High concern	79	15.9
	Very high concern (5)	47	9.5
	Total	497	100.0
Other users publishing my personal information without my consent:	No concern at all (1)	90	18.1
arithmetic $M = 2.70$; $SD = 1.24$	Low concern	153	30.8
	Moderate concern	122	24.5
	High concern	80	16.1
	Very high concern (5)	52	10.5
	Total	497	100.0

SD: standard deviation.

Table 4. Distribution of the Institutional Privacy Concerns Items.

Question prompt	Answer option	Absolute numbers	Percentage
Please indicate your level of concern about the following potential privacy risks that arise when you share your personal information on Tinder?			
Tinder insufficiently protecting personal data (information leakage):	No concern at all (1)	81	16.3
arithmetic $M = 2.89$; $SD = 1.22$	Low concern	125	25.2
	Moderate concern	143	28.8
	High concern	95	19.1
	Very high concern (5)	53	10.7
	Total	497	100.0
Tinder tracking and analyzing personal data:	No concern at all (1)	76	15.3
arithmetic $M = 2.90$; $SD = 1.24$	Low concern	125	25.2
	Moderate concern	129	26.0
	High concern	109	21.9
	Very high concern (5)	58	11.7
	Total	497	100.0
Tinder selling personal data to third parties:	No concern at all (1)	65	13.1
arithmetic $M = 3.00$; $SD = 1.26$	Low concern	124	24.9
	Moderate concern	129	26.0
	High concern	106	21.3
	Very high concern (5)	73	14.7
	Total	497	100.0
Tinder sharing personal data with government agencies:	No concern at all (1)	86	17.3
arithmetic $M = 2.80$; $SD = 1.28$	Low concern	143	28.8
	Moderate concern	115	23.1
	High concern	90	18.1
	Very high concern (5)	63	12.7
	Total	497	100.0

SD: standard deviation.

Table 5. Summary of Independent Factors.

Construct	Arithmetic M (1–5, except for loneliness)	Median	SD	Cronbach's α
Self-esteem	3.96	4.00	0.98	.89
Narcissism (reverse)	3.45	4.00	1.20	.78
Loneliness (0–100)	35.83	29.50	31.08	.91
Motives: hooking up	3.26	3.50	1.38	.94
Motives: friends	3.23	3.75	1.26	.83
Motives: relationship	3.46	3.67	1.24	.86
Motives: traveling	3.32	4.00	1.27	.86
Motives: self-validation	3.06	3.50	1.30	.85
Motives: entertainment	3.96	4.00	0.98	.68

SD: standard deviation.

Table 6. Wording of Self-esteem, Narcissism, Loneliness, and Motives Items.

Question wording	Item number	Average/SD (1–5)
Self-esteem (five items)		
On the whole, I am satisfied with myself.	se_1	3.74/1.11
I feel that I have a number of good qualities.	se_2	4.16/0.84
I am able to do things as well as most other people.	se_3	4.04/0.93
I feel that I'm a person of worth, or at least on an equal plane with others.	se_4	4.05/0.94
I take a positive attitude toward myself.	se_5	3.83/1.08
Narcissism (four items)		
When people compliment me I sometimes get embarrassed. (reverse)	narc_1	3.40/1.24
I prefer to blend in with the crowd. (reverse)	narc_2	3.38/1.18
I try not to be a show off. (reverse)	narc_3	3.72/1.08
It makes me uncomfortable to be the center of attention. (reverse)	narc_4	3.31/1.28
Loneliness (four items, range from 0 to 100)		
I miss having a really close friend.	lon_1	39.95/32.67
I miss the pleasure of the company of others.	lon_2	35.32/30.59
I find my circle of friends and acquaintances too limited.	lon_3	40.35/31.60
I miss having people around.	lon_4	27.71/29.44
Motives: hooking up/sex		
How much do you use Tinder to . . .		
Find new sexual partners?	sex_1	3.34/1.35
Hook up with men/women?	sex_2	3.36/1.37
Satisfy my sexual curiosity?	sex_3	3.22/1.36
Have casual sex?	sex_4	3.10/1.44
Motives: friends/social network		
How much do you use Tinder to . . .		
Find new friends?	friend_1	3.52/1.18
Talk to my friends?	friend_2	2.90/1.37
Build my social/friendship network?	friend_3	3.31/1.29
Plug in the existing network around me?	friend_4	3.19/1.18
Motives: relationship/partner		
How much do you use Tinder to . . .		
Find someone to date?	rel_1	3.52/1.23
Find a long-term relationship, partner or boyfriend/girlfriend?	rel_2	3.23/1.28
Meet a potential partner in the area?	rel_3	3.64/1.20
Motives: traveling		
How much do you use Tinder to . . .		
Meet new people when I'm traveling?	travel_1	3.28/1.29

(Continued)

Table 6. (Continued)

Question wording	Item number	Average/*SD* (1–5)
Go on a date in a different place?	travel_2	3.30/1.26
Explore the dating scene in a new city/town?	travel_3	3.37/1.27
Motives: self-validation		
How much do you use Tinder to . . .		
Get self-validation from others?	valid_1	2.98/1.29
Get an ego-boost?	valid_2	3.13/1.31
Motives: entertainment		
How much do you use Tinder to . . .		
Satisfy my social curiosity?	enter_1	3.92/0.96
Look at pictures of men/women?	enter_2	3.95/1.03
Alleviate my boredom?	enter_3	4.02/0.95

SD: standard deviation.