How Public Is My Private Life? Privacy in Online Dating

Camille Cobb
University of Washington
cobbc12@cs.washington.edu

Tadayoshi Kohno
University of Washington
yoshi@cs.washington.edu

ABSTRACT

Online dating services let users expand their dating pool beyond their social network and specify important characteristics of potential partners. To assess compatibility, users share personal information — e.g., identifying details or sensitive opinions about sexual preferences or worldviews — in profiles or in one-on-one communication. Thus, participating in online dating poses inherent privacy risks. How people reason about these privacy risks in modern online dating ecosystems has not been extensively studied. We present the results of a survey we designed to examine privacy-related risks, practices, and expectations of people who use or have used online dating, then delve deeper using semi-structured interviews. We additionally analyzed 400 Tinder profiles to explore how these issues manifest in practice. Our results reveal tensions between privacy and competing user values and goals, and we demonstrate how these results can inform future designs.

1. INTRODUCTION

Online dating services enable users to connect and develop romantic relationships with other users who they might not otherwise meet. Past research has examined varied aspects of the online dating ecosystem, such as how people cultivate the impressions that they give others and how to provide a better user experience, e.g., [28, 42, 43]. Much less attention has been paid to how users perceive, navigate, and manage privacy risks in online dating.

Online dating is a particularly unique domain because information in online dating profiles may be simultaneously *more public* (e.g., accessible to a wider audience since users often aim to connect with people *outside* their social networks) and contain *more sensitive information* than profiles on other social media. Users may be motivated to include information, such as their sexual kinks and religious beliefs, that they believe will help them find a compatible romantic partner yet might not share with people they know (e.g., Facebook friends). This situation is in direct conflict with the goals of most permissions models. Recent high-profile events demonstrate that privacy issues in online dating deserve additional attention. For example, during the Rio Olympics, a Tinder user took screenshots of Olympians' profiles and posted them publicly on social media [9]; subsequently, a journalist used Grindr to collect identifying information about closeted gay Olympians [29].

Our focus on privacy is multi-fold. First, we seek to understand users' perceptions about and actions governing their privacy. For example, we seek to assess users' level of concern about their own privacy, the reasons for their concern or lack thereof, and how these concerns manifest in online dating behaviors. Additionally, since privacy involves multiple actors (the party who has information to share or keep private, and the party who might intentionally or accidentally learn that information), we study the reciprocal side of privacy: how users consume (possibly) private information from and about others. We leverage a combination of methods to achieve our goals: a survey, follow-up semi-structured interviews, and an analysis of Tinder profiles. A key contribution of our work is a portrait of existing user practices and views surrounding privacy in online dating. From this, we identify explicit tensions and challenges (presented inline with our results) and give suggestions for how online dating system designers can better support user goals, including privacy (§ 11).

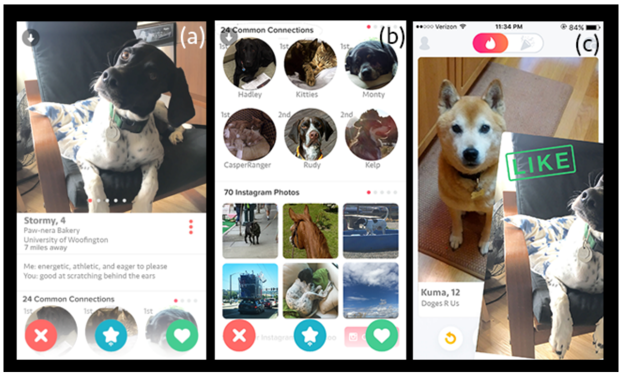
2. ONLINE DATING OVERVIEW

We now review online dating services, focusing on two that were most discussed in our surveys — OKCupid and Tinder; we then broadly discuss others. A 2016 report says that 15% of Americans have used online dating — three times the number who had used it in 2013 [1]. Tinder generates 26 million matches per day [5]; OKCupid claims over 1 million app installs per week [3]. We describe the services as they exist now but acknowledge that features change, and some survey participants used only previous versions (see § 5).

Tinder. By default, a user's first name, age, gender, job, and education (if present) are imported from Facebook and displayed in Tinder profiles. Profiles also include photos and text. When a user views a profile, they see mutual Facebook friends and the distance to the other user (based on the phones' GPS locations). Users may link their Instagram account to display recent photos and their Instagram username. Figure 1 gives an example (synthetic) Tinder profile.

Users view profiles in a queue called "Discovery." To view another profile, the user must "swipe right" to indicate a desire to connect or "swipe left" if they are not interested.

WWW 2017, April 3–7, 2017, Perth, Australia.
ACM 978-1-4503-4913-0/17/04.
http://dx.doi.org/10.1145/3038912.3052592



Stormy, 4
Paw-nera Bakery
University of Woofington
7 miles away

Me: energetic, athletic, and eager to please
You: good at scratching behind the ears

24 Common Connections

Hadley
Kitties
Monty
CasperRanger
Rudy
Kelp

70 Instagram Photos

●●○○○ Verizon 11:34 PM 84%

Kuma, 12
Doges R Us

Figure 1: Example Tinder profile (generated in Photoshop, not a real user) in (a), scrolled down in (b); right swiping reveals the next profile, (c).

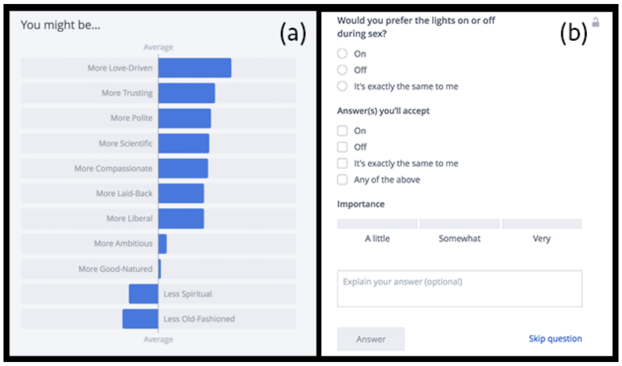
Users have a limited number of right swipes per day. If both users swipe right, they "match" and may exchange messages and view each others' profiles at any time. Users select which gender(s) they are looking for and specify an age range and search radius. Users appear in queues only if they fit each other's search criteria. A paid subscription to "Tinder Plus" lets users "rewind" the most recent swipe, hide their age or location, "passport" to any location in the world (swipe as though they were there), and make their profile visible only to those they right swipe.

OKCupid. OKCupid profiles consist of: (1) a unique username, (2) demographic information, (3) text in suggested paragraphs, such as "What I'm doing with my life", (4) photos, (5) answers to multiple choice questions, many of which concern sensitive topics such as sexual history or preferences, religion, and drug use, and (6) a personality assessment based on answers to (5). Examples of (5) and (6) are shown in Figure 2. Questions also determine a "match percentage" with other users. By default, users answer questions "publicly," and answers become visible to others who answer the same question; "privately" answered questions influence match percentage and personality.

Users can view the profile of and send messages to other users unless they have been blocked. By default, users can see who has viewed their profile since their last login; they can browse covertly but cannot monitor who views their profile while they are "invisible." Users receive a notification if they mutually "like" others. A paid subscription to "A-list" lets a user see everyone who likes them and browse invisibly while retaining the ability to see who visits their profile.

Other Dating Services. Many general-purpose online dating applications exist, some with features or designs that pose potential privacy implications. Coffee Meets Bagel gives users only a handful of profiles to evaluate each day and displays users' first names only if matched. The League leverages users' LinkedIn accounts to block coworkers. On Bumble, women must initiate conversations, and matches expire if no messages are exchanged within a specified time frame. Other online dating services — like Grindr, JSwipe, and ChristianMingle — cater to specific demographics.

Although they did not surface in our study, third-party applications may break users' expectations. For example, Firetind claims to let Tinder users browse profiles with no queue and see *everyone* who right swipes them.



You might be...

More Love-Driven
More Trusting
More Polite
More Scientific
More Compassionate
More Laid-Back
More Liberal
More Ambitious
More Good-Natured
Less Spiritual
Less Old-Fashioned

Would you prefer the lights on or off during sex?

○ On
○ Off
○ It's exactly the same to me

Answer(s) you'll accept

□ On
□ Off
□ It's exactly the same to me
□ Any of the above

Importance

A little Somewhat Very

Explain your answer (optional)

Answer Skip question

Figure 2: Screenshots showing OKCupid's personality assessment (a) which is based on answers to questions, like the one in (b).

3. CONTEXT AND RELATED WORK

Privacy, online dating, and recent high-profile incidents. The media has covered data breaches and vulnerabilities in online dating systems. For example, online dating sites Ashley-Madison [40], PositiveSingles [7], and HZone [34] were targets of breaches that divulged identifying data, and association with those sites revealed that users had considered an affair, had an STD, or had HIV (respectively). Researchers have found, for example, that dating apps exposed sensitive past in-app messages [18] and allowed precise geolocation of users [32]. We do not consider the effects of technical vulnerabilities in this work.

Recent events emphasize the importance of understanding how users' privacy expectations can be violated by other users: researchers released sensitive and identifying information about 70,000 users by creating an account to scrape OKCupid [4], screenshots of Olympians' Tinder profiles were shared publicly on social media [9], identifying information from closeted Olympians' Grindr profiles was published by a news site [29], and news has also covered stories about online dating users experiencing physical violence or stalking [8]. In these examples, in contrast to data breaches, authorized parties (with accounts) caused harm by violating users' expectations and trust.

Online dating research. Several past studies have also focused on privacy in online dating. One study [19] used data collected in 2006 — when Facebook was relatively new and the iPhone had not yet been released — and found a statistical correlation between online dating users' concerns about personal security, misrepresentation, and being recognized by someone they knew and "uncertainty reduction behaviors" (e.g., looking someone up, saving messages, and asking follow-up questions of the other user). The researchers additionally note that their results do not explain the high degree of variance in participants' responses. A more recent survey of Wellesley College students who use Tinder [36] asked participants what privacy meant to them and if they considered it to be important. They also looked at 30 Tinder profiles to determine if people can be re-identified from their profile. In our Tinder profile analysis, we begin with the same question, but for a larger population, and study not only whether users can be re-identified from their profiles but also what properties affect identifiability (§ 10). Additionally, compared to both works, our surveys and interviews take a qualitative approach to understand a wide range of issues and include participants who have used a variety of online dating systems at some point during a relatively long time-frame (2001 to present).

Within the online dating ecosystem, other research has explored a broad range of topics, such as: whether people portray themselves accurately [21, 38], impression management [43], how people leave online dating systems [14], and how users are successful at online dating [28, 42]. A line of related work focused on understanding Grindr users' preferences and desires in online dating, e.g., [13, 16, 20, 39]. Although privacy was not the focus, because of its importance, privacy considerations surfaced in some of these studies.

Additional privacy-focused research. Prior work related to privacy in other social media applications — including Facebook [10, 17, 23, 25, 26, 31, 35], Twitter [27, 30], and Snapchat [33] — have revealed evidence of misunderstandings about permissions, misuse of others' information, and social, physical, and financial risks resulting from privacy breaches. Other studies have explored factors that influence privacy preferences — what information is being shared, at what granularity, with whom, and the broader context [11, 12, 22, 24] (e.g., in the case of sharing location information, *where* the user is, the time, and who they are with). Additional works focus on location privacy in social applications, e.g., [15, 37], and the right to not be identified [41].

4. METHODS

Our research combines three methods, all approved by our institution's IRB: (1) an open-ended survey, (2) an analysis of Tinder profiles, and (3) semi-structured interviews with a subset of survey respondents. Survey responses informed the design of Tinder profile analysis, and both surveys and profile analysis informed the structure of follow-up interviews.

Because the surveys provided an initial glimpse into privacy preferences and practices and interviews let us delve more deeply into those same issues, we present our survey and interview results together, followed by the results of our Tinder profile analysis. Despite this presentation order, our Tinder analysis results contributed to the interview design. Further, we stress that our goal is not to provide comprehensive, quantitative, generalizable results over all online dating systems and populations, but rather to consider a diversity of populations and systems with the goal of uncovering unique challenges and lessons.

4.1 Survey

Our survey contained 24 multiple-choice, 15 open-ended, and 10 demographic questions[1]. We designed the survey using an iterative process, informed by our own experiences with online dating, feedback from colleagues, and small-scale pilots. The survey remained open throughout the duration of our research, though most responses were collected prior to Tinder profile analysis and interviews. We recruited participants by posting a link to the survey on public forums and by propagating it through our social and university networks (i.e., snowball sampling).

Survey questions addressed respondents' general use of online dating and their experiences, practices, expectations, and feelings about disclosing information, looking up other users or being looked up, taking screenshots, and the intersection of real-world and online encounters. We intentionally did not define privacy and instead let users surface the concerns that are most relevant to them.

Age	20-24 (18), 25-29 (44), 30-34 (16), 35-39 (9), 40-44 (3), 45-49 (4), 50-55 (3)
Education	High School or GED (2), Associate Degree (4), Some College (6), Still in College (3), College or More (82)
Ethnicity	White (68), Asian (10), Hispanic (3), Black (2), Other or Unspecified (14)
Gender	Male (35), Female (61), Unspecified (1)
Occupation	Student (26), Teacher (9), Computer Engineer (7), Other or Unspecified (55)
Relationship Status	Single (50), Seeing Someone or Married (37), Divorced, Separated, or Widowed (7), Open Relationship (2), Unspecified (1)
Religious Views	Christian (36), Atheist (17), Agnostic (12), Jewish (7), Other or Unspecified (25)
Sexual Orientation	Straight (83), Bisexual (6), Gay or Lesbian (4), Other or Unspecified (4)

Table 1: Summary of survey demographics

Demographics. The survey received 99 total responses, of which we used 97.[2] We excluded two responses: one person had not used online dating, and one submitted the form twice. Table 1 summarizes study demographics.

51 participants had used online dating for at least three months of the past year, while 28 had not used it at all in the past year. 60 started online dating in 2012 or later. 66 use or previously used OKCupid; 44 use or previously used Tinder (and an additional 17 tried it). Use of 27 additional dating services was reported by participants, and 65 participants tried at least 3 online dating services. 44 reported that it was common or very common to use dating services amongst their friends; 15 said it was uncommon or very uncommon, while 38 were neutral.

4.2 Tinder Profile Analysis

To gather ground-truth insights about profiles' content and findability (defined below) to supplement self-reported participant information, we analyzed content from 400 Tinder profiles: 100 26 year-old women (men) seeking men (women) in Seattle, and a corresponding number in Atlanta. 26 year-olds are well-represented in online dating [2] and old enough to have employment histories. We consider only women (men) looking for men (women), which is the most common demographic. Atlanta and Seattle represent cities with different demographics. We chose Tinder because it is popular and has the convenient property of its queue dictating an order in which to consider profiles.

We created two Tinder accounts associated with Facebook accounts for a 26 year-old man and a 26 year-old woman. To minimize possible effects on queue ordering, we used new (blank) accounts, swiped only left, and viewed profiles during the day on weekdays. Per our IRB's request that we not interact with other users or collect identifying information, we used settings that prevented others from seeing our profile unless we swiped right, which we did not; we were also careful never to record identifying information. All searches

[1] Survey instrument can be accessed at homes.cs.washington.edu/∼cobbc12/HowPublicIsMyPrivateLife_SurveyInstrument.pdf

[2] Percentages out of 97 are similar to the raw numbers of respondents, so we do not include the percentages.

were in a private browser, and we did not use reverse image search, which would involve saving profile photos.

Our team collaboratively conducted pilot data collection to refine and systematize data collection and search procedures. We delineated both steps that we would take and steps that we would explicitly not take to look someone up. This process allowed us to develop a consistent, uniform approach for data collection. One researcher collected the final data and both researchers participated in the data analysis.

Defining "found." We marked a profile as "found" if: (1) we found their last name, (2) we found additional account(s) of theirs or page(s) with information about them, *and* (3) we were sure it was the same person. This is likely an overly restrictive definition of finding someone, and searching would be easier without the constraint of never saving identifying information and using new accounts with no friends. Hence, our results offer a rough lower bound on users' searchability.

Data collected. For each profile, we recorded: (1) if we found the person, (2) if found, if their Tinder photos were found elsewhere, (3) if their job and/or school were listed, (4) if their Instagram was linked or if usernames for other accounts were listed, and (5) how unique their first name was according to howmanyofme.com.

4.3 Interviews

We conducted 14 semi-structured phone interviews, each lasting up to an hour, with survey participants who consented to follow-ups and responded to interview requests by our internal cutoff date (seven men and seven women). The interviewer, a woman with online dating experience, audio recorded the interviews with participant consent; all researchers participated in analysis, including an affinity diagram exercise to identify themes in surveys and interviews. Informed by survey results and Tinder profile analysis and leveraging the semi-structured nature of the interviews, we probed further into topics surfaced in surveys and additionally discussed why users chose particular dating services, use of paid features, and perspectives about recent privacy-violating events related to online dating (§ 3).

5. GENERAL RESULTS

We begin our analysis by focusing first on general observations, then turning to in-depth discussions of specific topics (§ 6–9). We combine survey and interview analyses in § 6–9 and discuss Tinder profile analyses in § 10. Note that survey and interview data were self-reported and may reveal the union of a participant's practices on multiple services.

Motivations for using online dating. 62 survey respondents' goal for online dating was dating or marriage; 20 hoped to date and make friends; 13 sought casual sex in addition to friendship and/or dating; one was exclusively seeking platonic relationships; one wanted to "see what's out there"; no one reported using the service only to find casual sex partners. Participants also reported using online dating for entertainment, to get over an ex, "to think about who I want to date," (P41, F, 21, interview)[3] or to "familiarise myself with a new area after moving" (P71, F, 26).

P73 (M, 27) compared it to a basic need: "eveybody [*sic*] needs the chance to get out their [*sic*]." P1 (F, 27) felt pressure to use online dating: "I feel like I need to meet people, then realize that I actually don't really like it and stop for a few months, then worry that it's hard to meet people otherwise anymore." On why she preferred online dating, P40 (F, 23) wrote, "We were introverts and we liked the ability to see people's interests and KNOW they were interesting [*sic*] in dating before speaking to them."

Though not addressed in the survey, interviewees gave the following reasons for choosing a dating service: their friends used it; it was popular; it was free; it had specific security or usability features; they had more success than with others; or they knew successful couples who met using it.

Reasons for stopping online dating. Mirroring reasons for choosing a dating service, survey respondents mentioned cost and lack of success as reasons they stopped using a service. 30 survey respondents stopped using online dating because they found a partner. Others got bored, preferred to meet someone offline, ran out of potential matches, did not like the messages they received, felt they required too much time, or became frustrated over scams or bots.

Related to privacy, P48 (F, 23) wrote, "It felt weird to know a lot about a person before meeting them." In contrast, two survey respondents stopped using services with limited profile space because "the apps generally had less information than I wanted" (P7, M, 33) and they "couldn't glean any actually useful info from any profiles" (P2, F, 22).

Paying for features. Although many participants preferred free online dating services, three (not asked directly) appreciated OKCupid's paid privacy features which allow users to specify (i.e., whitelist) who may view their profile. Some users were not familiar with these options. For example, P80 (F, 24, interview) thought paying offered only a way to *boost* her profile's visibility rather than increase privacy. Current implementations of features on Tinder and OKCupid that allow users to whitelist audiences prevent users with similarly restrictive privacy settings from encountering each others' profiles. Facilitating connections between users who may be romantically compatible but have incompatible (or equally restrictive) privacy settings is a design challenge.

Impacts of demographic characteristics. These characteristics may influence users' experiences and perspectives on privacy in online dating. For example, P1 noted that young people were likely to be on their parents' phone plan and have a number with an area code, which reveals their hometown and makes them more searchable (§ 8). Users' locations when using these services could affect their privacy-relevant experiences. For example, P80 pointed out that because of gender imbalance in Silicon Valley, she was unlikely to encounter her male friends' Tinder profiles. Likewise, because there are fewer women in the area, her male friends might be more likely to encounter her Tinder profile. Navigating privacy implications when different demographics are impacted differently is another challenge.

6. PERCEIVED OR EXPERIENCED RISKS

To understand why users might be motivated to remain private (or not) in their profiles and what their internal threat models are, we highlight risks that participants anticipated or encountered using online dating.

Uncomfortable feelings. Awkwardness or embarrassment was a risk acknowledged by most participants, albeit often dismissively; however, it influenced how they used online dating services and is therefore an important consider-

[3](P41, F, 21, interview) denotes Participant 41 (after randomizing participant order), female, 21 years of age, and that the quote was from an interview and not the survey.

ation. 81 reported seeing the profile of someone they knew well offline, and 33 had seen a coworker's profile. 37 reported recognizing someone in public from their dating profile, and 30 coincidentally met someone in person shortly before or after seeing their online dating profile. Some had mostly positive feelings, noting that it was "kind of nice to know we're all in the same boat" (P93, F, 28), but others had a negative reaction: "I felt like I did something wrong, especially when I remember the app shows who has looked at your profile" (P68, F, 27).

Details remembered from profiles shaded some people's future in-person impressions: "It was one of those, I've totally seen that girl and remember her being really skanky online" (P73). Uncomfortable feelings were exacerbated if either user expressed interest: "It was also someone who had expressed interest in me who I wasn't interested in, so that was extra awkward" (P93). Sometimes the privacy of revealing only mutual attraction was appreciated: "I swiped right. They didn't do the same. All was well with no lingering curiosity" (P75, M, 30). However, this could be complicated because not everyone put the same care into swiping: "[My friends swiped using my account] with my consent but they would pick matches that I typically didn't like" (P65, F, 27).

Unanticipated disclosure. Online dating users may be unable to anticipate who will see their profile. Unanticipated disclosure can occur through data breaches, users sharing information or screenshots (see § 9), or other unexpected uses of the service. For example, users may not expect people to view profiles of people they are not interested in, as P94 (F, 36) did: "One time I was browsing other women's profiles just to get a sense of what the norms are in the online dating world (I'm a hetero woman), and I came across a friend's profile ... her profile made her seem emotionally unstable and batshit crazy." The impact of unanticipated disclosure varies; although P94's opinion of her friend may not have changed, in another case: "We discovered a friend's boyfriend was cheating on her, which led to the breakup of their relationship" (P71). We discuss strategies used to avoid unanticipated disclosure in § 7.

Scams, bots, and catfishing. Concerns about scams, bots, and catfishing (e.g., people presenting themselves as someone else through pictures and profile information) may affect users' privacy-relevant decisions. P76 (M, 26) aims to "Have a meaningful conversation with the person, so that I'm sure they're not some kind of scammer." P87 (M, 26, interview) was led on by a catfisher for several weeks and then threatened; he now takes the opposite approach: "I would never go after a girl that long without meeting them first." Each approach has its own risks — a meaningful online conversation could reveal sensitive information prematurely and with a written record, but meeting a stranger in person after only a brief conversation raises safety concerns.

After being asked if she was a bot because she did not disclose much in her profile, P89 (F, 27, interview) changed her profile to include where she went to school. As we discuss in § 10, revealing one's school can affect privacy by making one more findable. A design challenge is how to enable P89 to convince others that she is not a bot while also not revealing more private information.

Although both men and women expressed concerns about these threats, two interviewees believed that men are at greater risk: "It does take presumably some work to create [fake accounts] and it's so much more likely to be successful as a woman. Dudes are so much more likely to swipe right" (P56, M, 27, interview).

Stalking, cyberstalking, inappropriate messages, violence. When asked why they omitted certain information from their profile (free-response), nine survey respondents stated concerns about "creepy" people finding them or safety. People also felt relief or regret (depending on how the situation evolved) after revealing personal information to someone met via online dating, "I met someone once who turned out to live across the street and half a block down from me. Figured that out on the first date — good thing she wasn't nuts since she knew where I lived at that point ..." (P7). "After I did not choose to go on a subsequent date with someone, they found information about me online that I did not think was easy to locate, and they used this information to make me feel guilty. I was concerned the behavior might escalate" (P68). This participant explained later in an interview that she believed the person learned her last name when an iMessage was sent "from" her email address instead of phone number, used this to find her on Twitter, and followed links in her distant Twitter past to personal blog posts. This situation highlights the challenge that even if a person has certain privacy settings within their online dating app, other apps may leak private information.

Safety concerns might influence users to take actions that violate their own or others' privacy, such as informing friends about a date, looking up other users (§ 8), taking screenshots (§ 9), and asking a match for personal information (§ 7).

On the other hand, participants identified how online dating could empower users through mechanisms not available with traditional dating. For example, users can block people, exchange messages through the service until they feel comfortable exchanging contact information, and have sufficient information to "check up on"' someone before going out with them. P41 saved messages to re-identify users who messaged her again after a long time and/or from a different account. To stay safe, some participants used strategies such as only meeting with someone who shares certain information (e.g., a phone number) or if they are able to confirm their identity online or via mutual friends (see § 8): "I usually wouldn't meet someone unless we have mutual acquaintances or I can find validating information about them online" (P11, F, 31). However, as discussed in § 7, some users may wish to avoid sharing contact information or having a large online presence.

Employment and businesses. 65 survey respondents disagreed or strongly disagreed that it would be okay for an employer to use information from someone's online dating profile to make an employment decision, but only 36 felt the same way about public Facebook profiles. 12 survey respondents had seen the online dating profile of someone who worked in a public position at a business they frequented, such as a bartender, doctor, or instructor. Of the people who had this experience, nine changed their opinion of the person or the person's ability to do their job, suggesting that someone's online dating presence can influence users' impressions of businesses. Six participants said they preferred not to see and/or be seen by people who work at businesses they frequent. Participants who worked in public positions similarly expressed concerns about clients viewing their profiles: "I am a teacher and I was always afraid that my profile would be found by my students. I feel like anyone taking a screenshot would increase that likelihood" (P55, F, 26).

7. DISCLOSURE OF INFORMATION

Although some participants think dating services should prevent leaks, others believe users can prevent undesirable consequences: "I think one just has to be careful how many personal details they put online . . . I think it could be possible to avoid security issues" (P31, F, 35). Indeed, some users did not worry about disclosure because they lacked "anything to be ashamed of" (P72, M, 27) in their profile: "if . . . security is breached, I take comfort in my own profile's relative banality" (P35, M, 27). However, there are valid reasons to include potentially sensitive information in a profile, and even very basic information could be harmful if used in unexpected or malicious ways.

What people revealed in their profiles. We asked survey participants directly about content in their online dating profiles. 62 revealed their first name (only 8 revealed their last name); 45 revealed their job; 42 revealed their school; 38 had information about their sexual history or preferences; 64 revealed their religion; and 44 expressed political opinions or leanings. Only P42, a 39 year-old male who aimed to be "as private as possible," did not have a photo that included his face in his profile. 17 had photos that might be considered sensitive (e.g., of them drinking, wearing a swimsuit, in a sexually explicit position, or naked). Specific information participants withheld included their religion, name, job, school, physique, salary, and sexual preferences. When meeting in person, some were careful not to reveal their license plate or exactly where they lived.

How people chose what information to disclose. A dating service's design and default settings can influence what information users disclose. For example, Tinder requires users to display the name from their Facebook account, and OKCupid users must upload a photo before they can see more than a thumbnail of other users' photos.

Participants disclosed information to find more compatible matches; increase chances for a match; reciprocate when others share information; communicate their values, hobbies, sense of humor, and personality; or as a response to direct or perceived pressure from other users. Reasons for withholding information included safety, remaining anonymous, avoiding embarrassment, discouraging harassing messages (e.g., not answering overtly sexual questions on OKCupid directly because of a perception that this leads to receiving more vulgar messages), controlling the way they present themselves to potential matches (e.g., "I leave out the fact that I am bisexual, because it . . . scares off both men and women" (P50, M, 28)), not being judged prematurely (e.g., for living with his parents (P32, M, 28)), or because they did not consider the information relevant.

Interviewees wanted to get a sense of the character, interests, or other characteristics of potential matches. Rather than attributing it to privacy concerns, some users dismissed users who disclosed very little information: "If they don't have anything, I kind of skip over them because clearly they didn't put any effort into it" (P80). Some participants expressed a desire to learn specific information that others preferred not to disclose or had been pressured to reveal information they did not want to disclose (e.g., job, socioeconomic level, apartment complex, full name, bra size, or phone number): "I dont [*sic*] like when people ask for my phone number, that's the limit" (P67, F, 29).

Some users noted internal tensions, realizing that, while uncomfortable to disclose, "things like names and locations are important to know when you're online dating . . . and it's important to know that someone is employed" (P23, F, 29). We return to the privacy implications of disclosing employment in § 8. P87 reconciled some of these tensions by modifying content rather than leaving it out completely, for example, by blurring logos or faces of friends in photos.

Selective disclosure. As discussed in § 6, some users wished to selectively keep the fact that they are using online dating or information in their dating profile from some people (e.g., friends, family, coworkers) while still making their profile available to potential matches. Beyond the paid features mentioned in § 5, participants noted strategies to achieve (or approximate) this goal. P93, upon creating her account, "spent a whole day . . . to find as many [people who work nearby] as I could and block them . . . I missed somebody, inevitably." To minimize risk when using location-based applications, P68 reported: "I feel very uncomfortable when I see my coworkers' profiles, so I make sure to not use proximity-driven apps at work."

We did not identify direct concerns about someone actively trying to find users' profiles, but six participants used fake accounts or friends' accounts to covertly view profiles or send messages. 18 respondents acknowledged that, though they were unlikely to try, someone who knew them could probably find their online dating profiles. Others believed this would be difficult: "I think it would be very hard to 'find' it on purpose if they went out looking for it" (P94).

8. SEARCHABILITY

Our study surfaced a wide spectrum of views and practices on searching for information about other users.

Reasons to look people up. In surveys and interviews, users said that they looked up other users out of general curiosity, to find more recent photos, to be sure they were "real" people, to see if they were telling the truth, or to see if they had a criminal record: "I also liked it when [Coffee Meets Bagel] profiles included information that allowed me to Google someone . . . I am extremely hesitant to go on a date without that information, because I want to prevent sexual assault" (P28, F, 28). 58 survey respondents looked someone up when deciding whether to send them a message, respond to a message, or go out with them. 44 sought additional information after going on a date or agreeing to a date. 10 said they might look someone up if they caught their attention regardless of romantic interest.

What information was found. Based on information in their profiles, 77 survey respondents thought someone might be able to find their Facebook profiles. Although not asked directly, five participants offered that they would not want their Facebook to be found: "Facebook to me is very personal, basically an invitation to my life" (P31, interview). Participants reported finding other users' Facebook and LinkedIn pages, YouTube videos, other social media accounts, blog posts, and poetry.

How people searched. In surveys, five people explicitly mentioned using LinkedIn to search for people; 20 mentioned Facebook; and 19 mentioned Google. Survey participants also searched through Spokeo, court records, and other social media. We specifically asked about reverse image search, and 12 participants reported using it to find someone who reuses photos. Five people looked up someone's username on other sites, and four looked up a phone number. As a non-technical approach, 53 might ask a mutual friend.

Survey participants pointed out that finding information was easier with details such as name, location, phone number, occupation, or mutual friends: "If you know their name you can use Spokeo - if you know where they live and their name you can access State records like property tax records to see if they own a home" (P15, F, 51). P85 (F, 23) noted that inherent traits might make searching for them especially easy: "I have a fairly unique name, so while I have specific privacy settings on my Facebook, I could probably be found just with my name." Furthermore, participants indicated awareness of factors that made searching more difficult: "Only use site-specific photos, din't [*sic*] use the same pictures anywhere else online" (P25, M, 33). "My last name is a common word, so that makes things hard. There's a c-list celebrity with my name" (P32, interview).

Acceptability and etiquette. Some people did not think it appropriate to look people up or thought only certain techniques were acceptable for looking someone up: "I try not to do anything like that unless I'm planning to meet someone, and even then I'm probably restricting myself to google" (P62, M, 22). 72 thought it was common or very common to look people up. 14 never looked someone up — four said it was an invasion of privacy, the others cited reasons, such as not caring enough to bother. For example, P50: "I honestly never thought about doing this . . . I haven't tried any of that - I take dating profiles at face value. Am I supposed to creep on folks?" On the other hand, P11 did not think it took much effort: "I'm really good at using Google to find information about people, so I assume others are too." And some people thought it was common to put in the effort: "Based off of what my friends do, I kind of expect people to really go in and try to figure things out. They're kind of like spies" (P70, F, 24).

Several participants expressed a desire to be covert if they did look someone up: "I won't friend them, but I will scroll through their photos" (P40). Mirroring this, some expressed a preference that others not make it obvious or mention it if they know more than they should. In some cases, users may unwittingly reveal that they have looked up a potential match. For example, P54 (M, 26) was suspicious that someone had looked him up because she appeared in his list of "suggested friends" on Facebook — another example of how the use of multiple apps can affect a user's overall online dating privacy. Other people are okay with or prefer for the person knowing when they find information about them. For example, P31 was unconcerned about the fact that LinkedIn shows who has viewed her profile: she wanted her match to know that she had viewed his profile and for him to look at hers. The timing of disclosing this may be an important factor: "At some point, not on the first date . . . but at some point, I prefer to acknowledge the fact that we both looked each other up. Often it happens when you tell them your last name [because they admit they already knew it]" (P56, interview).

9. SCREENSHOTS

Taking screenshots of online dating content may violate privacy by saving data that might otherwise be ephemeral and taking that information outside of the service, sometimes in insecure or public ways. 48 participants never took screenshots; two did it once per day or more; and the remaining respondents took screenshots periodically.

Reasons to take screenshots. Our study surfaced motivations to take screenshots, including: safety, "just because" (P35, M, 27, interview), to shame rude or inappropriate behavior, to tease users, to avoid registering a profile view (e.g., at odd hours, like the middle of the night (P87, interview)), or for sentimental reasons ("Who wouldn't save their love letters?" (P43, F, 38)). 26 survey respondents took screenshots of especially funny, weird, offensive, or strange content. Respondents also screenshot cute dogs, interesting world views, attractive people, or people they knew.

28 survey respondents shared screenshots with friends (e.g., to get opinions about a potential match or for safety so that someone else had information about the person they were meeting). In addition to sharing with friends, participants reported that they or someone they knew had posted screenshots on social media, e.g., in private Facebook groups or on public forums like a subreddit called "creepypms." Respondents mentioned seeing online dating screenshots that "went viral" on Buzzfeed or other popular news sites. In § 11 we consider how designers might accommodate these motivations alongside users' privacy goals.

Acceptability and etiquette. Some participants viewed screenshots as privacy violations: "I would see it as a huge breach of privacy. Online dating is about putting yourself out there, yes, but screenshotting a dating app conversation is like bringing a tape recorder on a first date. It's just creepy!" (P40). 31 participants said they were not concerned about screenshots because their profiles did not contain sensitive information. Two people said they were not worried because they did not expect to be targeted: "My profile and photos are not then [*sic*] kind of pics [*sic*] that you would fee [*sic*] the need to screenshot" (P40). 14 saw profile content as public information: "Everything is public, it wouldn't bother me" (P73).

A troublesome idea for some participants was the public sharing of screenshots. P81 (F, 27) wrote, "I guess I would be embarrassed if I knew about it (like if it went viral or ended up on Buzzfeed) but I don't care as long as I don't know." Although not asked directly, three survey respondents thought it inappropriate for screenshots to be used for making fun of people: "It bothers me that someone who is putting themself out there gets teased" (P26, F, 24). Some participants were supportive of or had themselves taken screenshots to publicly acknowledge and condemn inappropriate online dating behavior, although one survey respondent noted: "Sometimes I send rude responses to rude messages, and I wouldn't want those to be screenshotted and spread" (P17, F, 25). A question explored in some interviews was whether screenshots should be de-identified (e.g., faces blurred). P56 felt he was not in a position to judge but thought his friends who shared screenshots on social media *did* obscure faces.

Some people considered messages more private than profiles and, thus, a more serious violation to screenshot: "Honestly I never thought about the messages I sent when I was on a dating site being shared outside of it. If I had I would have been more careful about what I said!" (P18, F, 31). Another participant sent sensitive information in messages: "I hope people don't take screenshots of sexually explicit conversations" (P51, F, 48).

P36 (F, 26) noted users' lack of control over what is done with screenshots, e.g., using Photoshop to alter screenshots:

"I think I wouldn't care unless they misuse it by using photoshop to edit it or post it elsewhere which is inappropriate."

10. TINDER PROFILE ANALYSIS

Our analysis of Tinder profiles provides ground-truth evidence to support and contrast surveys and interviews. In addition to (1) whether we found the user, we recorded: (2) if photos were reused, (3) if job and/or school were listed, (4) if Instagram was linked or other usernames were listed, and (5) how unique their first name was. In this section, we report the two tailed p-values for N-1 Two Proportion tests.

In total, we found ("found" as defined in § 4) people from 188 of 400 profiles (47%). We saw no significant differences in findability between men and women ($p = 0.11$) or between users in Seattle vs. Atlanta ($p = 0.69$). Of the 188 profiles we found, 75 reused photos from their online dating profile in other places (40%).

Users with linked accounts. Having an explicit link to another account or explicitly listing a username for another service could indicate that a user prefers to be findable. Indeed, the 129 people whose profiles included a linked Instagram account or another username were statistically more likely to be findable ($p < 0.001$) — 103 were findable on other sites (80%). Of the remaining 26 that were not findable, several were "almost findable." That is, we: found them on other services but did not find their full name; found their full name but no other information; or were not confident enough that we found the same person.

However, there are indications that some of these 106 people might not realize they were findable or what other information could be found. Although some had private Instagram accounts, their names and profile photos on Instagram were public. Additionally, we saw at least 11 variations of external services that performed analytics or backups of Instagram — possibly without users' awareness. In some cases, these backups contained information no longer available on Instagram (e.g., full names), speaking again to the challenges of maintaining privacy in a multi-application ecosystem.

Users without linked accounts. Of the remaining profiles, only 85 of 271 were findable (31%). We use this subset of profiles to explore how other information — job, school, and first name — influence findability.

Employment and educational history are imported by default, so users without this information have explicitly removed it or chosen not to include it on Facebook either. Only one of 60 users who did not list a job or school was found. 28 of 106 (26%) who listed either a job or school (but not both) were found. 56 of 104 (54%) who included both job and school were found. Thus, there is a statistical difference in the percentage of people found between those who list neither and those who list one ($p < 0.001$), and between those who list one and those who list both ($p < 0.001$).

The final factor we considered in terms of its impact on findability was a user's name. For people with common names (i.e., >100,000 people in the U.S. share this name according to howmanyofme.com), only 37 out of 140 were findable (26%). For people with less common names, 48 out of 82 were findable (59%). People with less common names were statistically more findable ($p < 0.001$) — an observation made informally in surveys (§ 8).

Observations. Notable content observed in some profiles but not methodically recorded included plans to travel alone, that the person was a recovering alcoholic, references to drug or excessive alcohol use, and other sensitive information. In some cases, users shared content that could make them more findable, including photos of an ID or name tag and recognizable features in the background of photos (e.g., landmarks on college campuses). Distinguishing features, such as unique hair color, made users more recognizable on other sites; in contrast, major changes in appearance could be misleading. Other characteristics that may influence findability but that we chose not to record included content or number of photos, content or length of profile text, indications that someone was using Tinder Plus, and whether a specific job was listed or just the type of work. We also note that people who listed certain jobs (e.g., the specific coffee shop where they worked) may be findable in real life even if they were not findable online.

For some profiles, we found information about users across several sites even if we did not find their full names; for example, some people used the same pseudonyms on multiple sites. Given that some users change their names on Facebook (e.g., to be less identifiable to employers [6]), two tensions arise: choosing a unique pseudonym may make a user *more* findable, and some users may have chosen a pseudonym that does not make the desired impression on potential matches. We also encountered a profile that supported an assertion by P32 (§ 8) that having the same name as a celebrity decreased findability.

11. SUGGESTIONS FOR DESIGN

A core contribution from this data is to help educate dating site designers so that they can make informed decisions based on users' values and needs, beyond the specific suggestions we make here. We discuss some design implications in the preceding sections; below, we elaborate on two concrete examples of how our findings could inform design.

A key risk of screenshots is content being shared outside of a service, where that service has no control over when and where the content is re-shared. Online dating systems could introduce features that allow users to achieve their sharing goals while discouraging (or even preventing) screenshots. To provide users agency in protecting their safety, which some currently do by taking screenshots before a date and sharing them with friends, and also to support users' social goals of getting friends' opinions (e.g., of whether a potential match is attractive or how to respond to a message), online dating services could have a built-in feature to (temporarily) share message and profile content and converse with friends directly in the app. To discourage users from mass-screenshotting profiles (as in the Rio example or on Buzzfeed) without preventing practices such as shaming exceptionally offensive behavior, online dating services could restrict the number of screenshots a user may take per day or notify the other party when a screenshot occurs.

There may also be opportunities for new mechanisms to help users control information disclosure. Tinder users might prefer default settings that do not import their employment or educational history, since that information may make them searchable. Tinder could additionally allow users to review and curate their profile before it is visible to others. Tinder Plus users can search for users anywhere in the world, thereby creating a privacy imbalance between the remote and local users. To mitigate this imbalance, Tinder could allow free (or paid) users to disallow remote matches. In addition to addressing privacy concerns raised in our study, this capability might have minimized harms in Rio [9].

Different users have different privacy sensitivities and practices. Our results also speak to the benefits of privacy awareness campaigns, whether enacted by industry or a public service organization. Users who are aware of how others might violate their privacy preferences can make better-informed decisions to protect their own privacy. Users who are aware of others' preferences might be more thoughtful when taking actions that could violate privacy preferences.

12. CONCLUSION

Our work provides an in-depth study focused on understanding and surfacing users' privacy preferences and practices in online dating. This portrait of the privacy-related aspects of the online dating ecosystem is our first contribution. Our other contributions are the identification of privacy-related tensions and challenges in online dating — challenges that pit privacy directly in tension with other user goals — and specific recommendations for mitigating several key challenges. We hope our work helps inform and focus industry and research efforts on addressing these challenges, thereby helping empower online dating users to more effectively control their privacy while also achieving their other online dating goals.

Acknowledgements

We thank Alexis Hiniker, Karl Koscher, Kiron Lebeck, Adam Lerner, Shrirang Mare, Peter Ney, Lucy Simko, Anna Kornfeld Simpson, Paul Vines, and Doug Woos for feedback on earlier drafts. This work was supported in part by the UW Tech Policy Lab, an NSF Graduate Research Fellowship, and the Short-Dooley Professorship.

13. REFERENCES

[1] 15% of American adults have used online dating sites or mobile dating apps. http://pewrsr.ch/1SgNCZl. Accessed: 2016-10-22.

[2] The case for an older woman. http://blog.okcupid.com/index.php/the-case-for-an-older-woman/. Accessed: 2016-10-22.

[3] OKCupid about. http://www.okcupid.com/about. Accessed: 2016-10-22.

[4] Researchers caused an uproar by publishing data from 70,000 OKCupid users. http://fortune.com/2016/05/18/okcupid-data-research/. Accessed: 2016-15-9.

[5] Tinder. www.gotinder.com/press. Accessed: 2016-10-22.

[6] Young job-seekers hiding their Facebook pages. http://www.cnn.com/2010/TECH/03/29/facebook.job-seekers . Accessed: 2016-10-22.

[7] PositiveSingles STD dating site faces $16.5m penalty. BBC, 2014.

[8] Tourist sexually assaulted in Sydney by several men after meeting on Tinder. News.com.au, 2014.

[9] Olympics and chill, 'a sexually charged time': Inside Rio Olympic's Tinder game where athletes are getting their swipe on. The Sun, 2016.

[10] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *PETS*, 2006.

[11] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Comput.*, 15(7):679–694, Oct. 2011.

[12] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, and J.-P. Hubaux. Adaptive information-sharing for privacy-aware mobile social networks. In *UbiComp*, 2013.

[13] C. Blackwell, J. Birnholtz, and C. Abbott. Seeing and being seen: Co-situation and impression formation using grindr, a location-aware gay dating app. *New Media & Society*, 2014.

[14] J. R. Brubaker, M. Ananny, and K. Crawford. Departing glances: A sociotechnical account of 'leaving' Grindr. *New Media & Society*, 2014.

[15] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *CHI*, 2005.

[16] E. F. Corriero and S. T. Tong. Managing uncertainty in mobile dating applications: Goals, concerns of use, and information seeking in Grindr. *New Media & Society*, 2016.

[17] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 2009.

[18] J. Farnden, B. Martini, and K. R. Choo. Privacy risks in mobile dating apps. *CoRR*, 2015.

[19] J. L. Gibbs, N. B. Ellison, and C.-H. Lai. First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, 2010.

[20] D. Gudelunas. There's an app for that: The uses and gratifications of online social networks for gay men. *Sexuality & Culture*, 2012.

[21] J. T. Hancock, C. Toma, and N. Ellison. The truth about lying in online dating profiles. In *CHI*, 2007.

[22] L. K. John, A. Acquisti, and G. Loewenstein. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, 37(5):858–873, 2011.

[23] M. Johnson, S. Egelman, and S. M. Bellovin. Facebook and privacy: It's complicated. In *SOUPS*, 2012.

[24] S. Lederer, J. Mankoff, and A. K. Dey. Who wants to know what when? Privacy preference determinants in ubiquitous computing. In *CHI EA*, 2003.

[25] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing Facebook privacy settings: User expectations vs. reality. In *IMC*, 2011.

[26] S. Livingstone. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 2008.

[27] H. Mao, X. Shuai, and A. Kapadia. Loose tweets: An analysis of privacy leaks on Twitter. In *WPES*, 2011.

[28] C. M. Mascaro, R. M. Magee, and S. P. Goggins. Not just a wink and smile: an analysis of user-defined success in online dating. In *iConference*, 2012.

[29] B. McNamara. Olympics 2016: Closeted gay athletes outed by Daily Beast Grindr article. Teen Vogue, 2016.

[30] B. Meeder, J. Tam, P. G. Kelley, , and L. F. Cranor. RT @IWantPrivacy: Widespread violation of privacy settings in the Twitter social network. In *SNSP*, 2010.

[31] D. O'Brien and A. M. Torres. Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, 2012.

[32] I. Polakis, G. Argyros, T. Petsios, S. Sivakorn, and A. D. Keromytis. Where's Wally?: Precise user discovery attacks in location proximity services. In *CCS*, 2015.

[33] F. Roesner, B. T. Gill, and T. Kohno. Sex, lies, or kittens? Investigating the use of Snapchat's self-destructing messages. In *Financial Crypto*, 2014.

[34] S. Shah. Hzone HIV dating app suffers massive data breach exposing 5,000 user accounts. 2015.

[35] J. Staddon, D. Huffaker, L. Brown, and A. Sedley. Are privacy concerns a turn-off?: Engagement and privacy in social networks. In *SOUPS*, 2012.

[36] C. Stenson, A. Balcells, and M. Chen. Burning up privacy on Tinder. In *SOUPS (Posters)*, 2015.

[37] E. Toch and I. Levi. Locality and privacy in people-nearby applications. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 539–548, New York, NY, USA, 2013. ACM.

[38] C. L. Toma, J. T. Hancock, and N. B. Ellison. Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin*, 2008.

[39] C. Van De Wiele and S. T. Tong. Breaking boundaries: The uses &#38; gratifications of grindr. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14, pages 619–630, New York, NY, USA, 2014. ACM.

[40] D. Victor. The Ashley Madison data dump, explained. The New York Times, 2015.

[41] J. Woo. The right not to be identified: privacy and anonymity in the interactive media environment. *New Media & Society*, 2006.

[42] P. Xia, B. F. Ribeiro, C. X. Chen, B. Liu, and D. F. Towsley. A study of user behavior on an online dating site. In *ASONAM*, 2013.

[43] D. Zytko, S. A. Grandhi, and Q. Jones. Impression management struggles in online dating. In *GROUP*, 2014.