Exploring the Privacy Experiences of Closeted Users of Online Dating Services in the US

Elijah Bouma-Sims
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
eboumasi@andrew.cmu.edu

Sanjnah Ananda Kumar
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA

Lorrie Faith Cranor
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
lorrie@cmu.edu

ABSTRACT

Online dating services present significant privacy risks, especially for LGBTQ+ people who are "in the closet" and have not shared their LGBTQ+ identity with others. We conducted a survey (n = 114) and nine follow-up interviews with US-based, closeted users of online dating services focused on their privacy experience. We found that participants in the study were strongly concerned about the risk of being seen by social relations and institutional data sharing practices like targeted advertising. Participants experienced a range of privacy and safety harms, including inadvertent outing, unauthorized saving and sharing of photos, extortion, and harassment. To protect their privacy, participants typically limited the amount of information and the photos they included in their profile. In order to improve their privacy experience, participants requested better profile visibility controls, limits on the ability of others to download or screenshot their photos, better user verification, and making premium privacy features available for free.

KEYWORDS

online dating services, privacy, LGBTQ+, the closet

1 INTRODUCTION

While online dating services are an increasingly popular way for American adults to form intimate relationships, these services pose significant privacy risks, especially for those who have not shared their gender or sexual identity with all of their friends or family. In order to facilitate matches with other platform members, users are often asked to provide potentially sensitive information, such as their age, gender identity, sexual orientation, and HIV status. While users may not intend this information to be shared outside of the context of online dating services, the data is essentially public. In a study conducted by Cobb et al. [10], the authors found the full name and associated social media profiles of 47% of the analyzed users. Additionally, on services that display the precise geographic distance between users, users may be vulnerable to triangulation of their exact location [29].

LGBTQ+ individuals (an acronym including lesbian, gay, bisexual, transgender, queer, and other gender/sexual minority groups) who are *in the closet* are uniquely vulnerable to these risks. Being in the closet or *closeted* refers to when a person internally identifies with a particular sexual orientation and/or gender identity but does not disclose it to some or all of their social relations [54, 62]. Closeted users of online dating services may be targeted for violence [65] or extortion [35]. Even in the absence of a deliberate adversary, these users may also risk incidental outing. For example, in a study conducted by Geeng et al. [20], P4, a gay and trans man, described finding a coworker on Grindr—a popular online dating service predominantly for men who have sex with men—and fearing that they would reveal his identity to others in the workplace.

While some research has explored the privacy risks faced by LGBTQ+ users of dating services [29, 74], no prior study has examined the unique needs of closeted individuals. To fill this gap, we present an online, exploratory study of the privacy-related behavior and needs of LGBTQ+ individuals in the closet on dating services. In particular, we seek to answer the following research questions in the US context:

(1) What privacy concerns do individuals in the closet have in the context of online dating services?
(2) How do individuals in the closet protect their privacy in the context of online dating services?
(3) How might online dating services better protect the privacy of individuals in the closet?

To answer these research questions, we conducted an online survey with 114 participants recruited via snowball sampling, advertisements on Grindr, physical posters at Carnegie Mellon University, and digital fliers distributed to LGBTQ+-focused organizations at universities around the United States. We also conducted nine follow-up interviews with survey participants via Zoom and email exchange to provide additional context to their survey responses.

We found that closeted dating service users were most strongly concerned about institutional data-sharing practices (i.e., targeted advertising) and the risk of encountering social relations. Many participants discussed experiencing privacy harms and other threats to their safety, including unauthorized downloading and sharing of their photos, inadvertent outing, extortion, and harassment. Most participants discussed some form of privacy-protective behavior, most often involving omitting certain information from their dating profiles. Finally, users addressed a range of possible features to protect their privacy better, including restrictions on downloading/screenshotting photos, better profile visibility controls, and making some paid privacy features available for free.

Our primary contribution is exploring the experience of closeted dating service users and offering actionable recommendations to dating services about how they can better address users' privacy and safety needs.

Proceedings on Privacy Enhancing Technologies 2024(2), 160–181

https://doi.org/10.56553/popets-2024-0046

2 BACKGROUND AND RELATED WORK

This section reviews related work and essential background information underlying our research. We first discuss the concept of the closet and LGBTQ+ stigma in greater depth. We then review prior work on dating privacy as well as other studies in LGBTQ+ focused usable security and privacy.

2.1 The Closet and LGBTQ+ Stigma

In general, society assumes that individuals are cisgender and heterosexual [37, 42]. It is, therefore, necessary for LGBTQ+ individuals to disclose their identity to others for it to be recognized. The process of progressing from inward recognition of LGBTQ+ identity to increasing levels of disclosure is typically referred to as *coming out of the closet* or simply *coming out* [54]. Coming out is also used to refer to individual acts of disclosure [41]. While often used to describe the experience of those identifying with non-heterosexual sexual orientations, this terminology has been adopted by transgender, non-binary, and other gender non-conforming people [5, 27]

Being out of the closet is generally associated with better mental health for LGBTQ+ people [55]; however, being out also requires individuals to navigate stigma and discrimination [7, 66]. For people with little support, coming out may not improve their quality of life [36]. It is thus essential that LGBTQ+ people are allowed to choose if and when they disclose their identity to others. Openly identifying LGBTQ+ people may face barriers to accessing healthcare [28], housing [9], and employment [8]. LGBTQ+ youth often experience bullying at school [14] and are at higher risk of facing homelessness [45]. Like other forms of discrimination, these issues are not uniform and are experienced differently based on other social identities such as race [12, 30, 31].

The terms "in" and "out" of the closet do not represent a rigid binary but rather a spectrum of approaches to identity management. For example, rarely is an LGBTQ+ person totally out at all times. An out person may choose not to disclose their identity to particular people in order to protect themselves from stigma [51]. Individuals may be forced back into the closet to avoid discrimination [79]. There is thus debate around the operational delineation between being in or out of the closet [16]. While some prior work associates being closeted with a total lack of identity disclosure [53, 54], other studies categorize individuals who have disclosed their identity to only a small group of people as being closeted [21, 52]. Reified models of the closet also struggle to account for how identity may change over time [16]. Does a person who previously came out as gay become closeted again if they begin to identify as bisexual?

In the present study, we rely on self-identification rather than imposing a precise definition of the closet. We focus on people who consider themselves closeted, regardless of their specific identity management practices. To accommodate a spectrum of disclosure practices, we adopt a broad definition of being in the closet as referring to people who do not disclose their LGBTQ+ identity to some or all of their friends, family, and other social relations. In line with the colloquial use of the term, we expect that those identifying as closeted will rarely disclose or discuss their LGBTQ+ identity and experience the stress associated with concealment. By using self-identification, we risk excluding some people who meet operational definitions of being in the closet but do not identify with the label closeted. Likewise, some participants who identify with our broad definition of the closet may not be defined as closeted under other definitions.

The internet has provided new avenues for LGBTQ+ people to explore their identities, even while remaining in the closet. DeVito et al. [13] conducted 20 semi-structured interviews to analyze how LGBTQ+ people present their identity across multiple social media platforms. They found that LGBTQ+ individuals take advantage of the different audiences and affordances of different platforms to avoid stigmatization while still expressing their LGBTQ+ identity. Taylor et al. [69] conducted an online survey of 274 users of Grindr, finding that use of the app was associated with less loneliness. More generally, online resources can play an essential role in defining and exploring one's identity, especially for LGBTQ+ youth [18, 39].

2.2 Online Dating Services and Associated Privacy Risks

There are a wide variety of dating services with different properties and users. Tinder is the most popular dating service in the US, with 46% of US dating service users reporting that they use Tinder. Grindr is the most prominent LGBTQ+ focused dating service, with 34% of US-based lesbian, gay, and bisexual dating service users reporting that they use the app [46]. LGBTQ+ people are more likely than heterosexual, cisgender people to use dating services, with 51% of US-based lesbian, gay, or bisexual people reporting that they have ever used an online dating service as compared to 45% of US-based heterosexual people [46].

To use a dating service, users generally must create a profile with information about themselves (e.g., photos, age, interests, profession, education, etc.). On many dating platforms, users can only view a subset of other users at a time, determined by their GPS location, preferences, use of a paid membership, and/or responses to specific questions. While many platforms (e.g., Tinder, Bumble, Hinge, etc.) require users to "match" with one another (i.e., mutually agree to connect) before interacting, some (e.g., Grindr) allow users to message other users without prior authorization.

As has been previously observed by Cobb et al. [10], information on online dating services may both be more public (i.e., accessible to more people outside of a user's personal connections) and more sensitive than information on other social media services. Users may want to share information to aid in finding a potential partner that they would not feel comfortable sharing with other social relations, such as their sexual orientation or religious beliefs. The public nature of this data can leave users open to harm. For example, in 2021, a Catholic priest was forced to resign after a Catholic news site reported that he regularly used Grindr [49]. Users also may experience context collapse when social relations encounter their dating profile unintentionally [44]. While some services have adopted unique access control methods to limit unwanted exposure (e.g., Tinder allowing users to block people from their phone contacts preemptively [70]), preventing unwanted data flows remains an open problem in online dating.

Online dating services also present privacy risks associated with targeted advertising and data handling. Many online dating services monetize users via advertisements. For example, the Match Group—owners of Tinder, Match.com, OkCupid, Hinge, and other dating services across the world—sells ad space on their platforms via Match Media Group,[1] Facebook, and Google. While they do not sell profile data to third parties, profile data may be shared between the different companies within the corporation [26]. Grindr also directly sells ads on its platform and, from at least 2017 to 2020, sold precise location information to advertisers [68]. While the practice has stopped, Grindr has also unintentionally exposed user data via security vulnerabilities several times [32, 78].

Many dating services also offer paid memberships that provide additional features. For example, Tinder offers three levels of paid memberships. All membership levels hide ads, remove limits on the number of people a user can like in a day, and allow users to set their location freely. Tinder users can also purchase single-use items that boost the visibility of a user's profile or enable a person to notify another user that they have been liked [71, 72]. Some paid features may help users protect their privacy. For example, Grindr's "Unlimited" membership enables an incognito mode where users can hide their profile from users they have not messaged while still using the service normally [25].

Most prior user studies on privacy and online dating services have focused on the general population of dating app users. Cobb et al. [10] surveyed 97 users of online dating services and conducted follow-up interviews to investigate their privacy attitudes and behaviors. They found tensions between different user goals, such as individual privacy and personal safety. Their survey is the most directly comparable to the present study. Lutz et al. [40] surveyed 497 Amazon Mechanical Turk workers who used Tinder, focusing on privacy concerns. The study differentiated between "institutional" privacy concerns (i.e., issues relating to how institutions such as internet services collect and use information) and "social" privacy concerns (i.e., issues related to other individuals), finding that users were more concerned about institutional privacy than social privacy. The results of these studies influenced our survey design and helped us understand the privacy experience of the general population of dating app users.

Some researchers have investigated online dating services with a focus on LGBTQ+ people. Hoang et al. [29] investigated the privacy risks associated with three LGBTQ+-oriented mobile dating applications (Grindr, Jack'd, and Hornet), demonstrating that users were vulnerable to triangulation of their location. Fernandez et al. [17] interviewed 20 transgender dating service users about their self-disclosure of transgender identity, finding that many users engage in proactive disclosure to protect their physical safety. Waldman [73, 75] surveyed 834 gay and bisexual men on their sharing of intimate photos on LGBTQ+-oriented dating applications. Among other findings, he found that many users engage in privacy "self-help" strategies such as cropping their faces from nude pictures before sharing. While neither of these studies explicitly addresses closeted individuals, they inform our survey design and analysis.

2.3 LGBTQ+ Focused Privacy and Security

Privacy researchers have given special attention to the needs of marginalized communities due to the increased harm they face when their privacy is violated [60, 76]. A few previous user studies have explored general privacy issues with members of the LGBTQ+ community. For example, Geeng et al. [20] conducted a semi-structured interview study with 14 participants to understand the experience of members of the LGBTQ+ community with online security and privacy advice, including in the context of online dating. They found that members of the LGBTQ+ community often turn to trusted queer support groups who experience similar threats. They identified several barriers to finding or using advice, including advice interfering with livelihood or diminishing enjoyment of activities. Lerner et al. [38] conducted 18 semi-structured interviews with transgender people about their computer security and privacy experiences. Their participants focused on prosocial behavior (e.g., role-modeling transgender identity) and activism. They identified several risk models relating to visibility, luck, and identity that participants used to make decisions. They also described a variety of technological defenses used by their participants, including obfuscation of profile pictures, use of encrypted messaging, and opting out of political discourse. We build on these studies and provide additional evidence of LGBTQ+ users' privacy strategies online.

3 METHODS

We administered an online survey to 114 participants and conducted nine follow-up interviews. We also analyzed the privacy policy and privacy-related features of the five most popular online dating services used by our participants.

3.1 Recruitment

We recruited participants primarily through physical posters and digital advertisements in various LGBTQ+ spaces. All advertisements include a description of the study and a link to take our survey. The headline of each recruitment advertisement indicated that participants should identify as closeted. Appendix A includes copies of the recruitment material. We placed these posters on the campuses of Carnegie Mellon University in Pittsburgh, Pennsylvania and Mountain View, California. We also distributed digital copies of the posters to LGBTQ+-focused organizations at universities around the United States. Online, we posted advertisements on LGBTQ+-related sub-forums of the social media service Reddit. We purchased advertisements on the largest LGBTQ+-focused dating service, Grindr. To increase the diversity of the sample, we recruited a small number of participants through snowball sampling [56]: We sent the survey advertisement to several members of the LGBTQ+ community known to the authors. We asked them to share the advertisement with other eligible dating service users who might be willing to participate. As our primary goal was to gain qualitative insights into the experience of closeted LGBTQ+ in the US, we stopped recruiting once theoretical saturation was reached (i.e., we observed no new insights from further survey responses [11, pg. 134]). We recruited 114 participants from October 10, 2022, to January 20, 2023. The majority of participants (55.5%) were recruited via Grindr.

3.2 Survey

The survey began with an informed consent form that disclosed the risks and benefits of the study and required participants to affirm their agreement to participate. In compensation for their

[1] https://www.matchmediagroup.com/

participation, they were offered the opportunity to enter a raffle for $125 per 100 people who completed the survey.

As part of the informed consent form, participants were required to complete a series of screening questions that verified their eligibility to participate in the study. In particular, they had to be 18 years of age or older, located in the United States, fluent in English, a member of the LGBTQ+ community, to some degree "in the closet," and have used a dating app or online dating service within the last three months. We instructed participants that they are considered in the closet "if you do not reveal your LGBTQ+ identity to some or all of your friends or family."

The text of the survey can be found in Appendix B. The median completion time was 8 minutes and 56 seconds. The survey began with demographic questions (Q1 to Q6) to characterize our sample (i.e., gender, sexual orientation, age, race, etc.). In asking participants to disclose their gender identity, we used the terms "male" and "female." We recognize that "man" and "woman" are more accurate when referring to gender rather than sex [64]. We, therefore, refer to those who selected "male" and "female" as men and women, respectively. This terminology may have led to inconsistencies in recording gender, especially for trans individuals.

To quantify how approaches to identity disclosure varied between our participants, we next asked them to complete a shortened version of Mohr et al.'s Outness Inventory (OI) [48]. Our version of the OI consists of a series of Likert scale questions that request participants to indicate how open they are about their sexual orientation to eight different individuals and groups: their mother, father, siblings, extended family, work peers, work supervisors, new straight friends, and old straight friends. Options range from 1 ("Person definitely does not know about my sexual orientation status") to 7 ("Person definitely knows about my sexual orientation status, and it is openly talked about"), with an additional "N/A" option for questions that do not apply to an individual. For brevity, we removed items from the original OI that we felt were superfluous or irrelevant to many respondents, such as statements concerning their "religious community."[2] The OI is one of the most commonly adopted scales for measuring outness among sexual minorities (e.g., [2, 19, 36, 57, 58, 61]). It has shown high internal consistency [2, 48] and correlates well with other measures of outness, such as the Nebraska Outness Scale [47]. The OI has some limitations: it does not account for non-traditional family structures (i.e., those without a mother or father, those with multiple parents of the same gender, etc.), and it fails to assess how people present their gender identity. It also conflates a person's knowledge of one's sexual orientation with how often one's sexuality is discussed [16].

The next set of questions (Q8 to Q12) characterized participants' use of online dating services. We asked which dating services they use, when they first used dating services, the last time they used online dating services, how frequently they use online dating services, and what their primary purpose is for using dating services.

The next section of the survey focused on participants' privacy behavior. We first asked (Q13) participants to select what information they include in their dating profile from predefined options (e.g., name, photos, general location, etc.). About six weeks after the survey was launched, we added a question (Q14) asking whether the participant's dating service(s) required location permissions. We noticed that many participants were not indicating that they shared their location on their profile despite using services that depend on GPS information. We wanted to verify that participants understood that the dating services use location information. 80 participants saw this question.

The following two questions explicitly asked about privacy-protecting strategies. We first asked whether participants do anything to protect their privacy on dating services (Q15). If they answered yes to this question, we asked them to explain how they protect their privacy in a free response question (Q16).

The next four questions (Q17–Q20) consisted of a series of 21 five-point Likert scale questions, requesting that participants rate their agreement or disagreement to privacy-related statements where 1 corresponds to "Strongly disagree" and 5 corresponds to "Strongly agree." Broadly, these statements were meant to gauge participants' concern about different institutional privacy risks (e.g., "I am fine with my dating profile being used to personalize advertisements.") and social privacy risks (e.g., "I am concerned that people who I haven't been 'out' to in real life will see my sexual orientation on dating apps/online dating services.") associated with the use of online dating services. We also included statements to assess privacy-related behavior participants may engage in (e.g., "I lie about information on my dating profile(s) to protect my privacy."). These statements were developed based on the results of prior research [10, 40, 75].

After the Likert scale questions, we asked participants again if they did anything else to protect their privacy (Q21), as the agree/disagree statements may have prompted users to think of more behaviors they engage in to protect their privacy. We analyzed the responses to this question separately from the first time participants were asked about privacy-protecting behavior. We refer to the responses before the Likert scale questions as "unprimed" and those after the Likert scale questions as "primed."

In the following question (Q22), we asked participants if their privacy had ever been violated while using online dating services, and if it had, we asked them to describe what happened. About five weeks after the survey was launched we added a follow-up question asking whether participants had been threatened on an online dating service and, if they had been, requested that they describe what happened. This question was marked as optional. It was added because several participants alluded to being threatened by other users of dating services without describing the specifics of what happened. 84 participants saw this question.

The survey's final question (Q24) was an open-ended question requesting that participants share any feature they would like to be improved or added to dating services to protect their privacy better. We requested that participants make specific reference to the service they use so that responses were adequately contextualized.

3.3 Follow-up Interview

After the survey (Q25), participants had the opportunity to volunteer to be interviewed on their responses to the survey in exchange for a $15 Amazon gift card. To protect participants' privacy, we

[2] In prior studies that use the OI, statements about one's religious community are often not answered (e.g., [2, 36, 48]).

offered them the opportunity to either participate in an audio-recorded Zoom interview or answer questions via email. Our primary goal in conducting interviews was to gain additional insight into specific experiences and feature recommendations from survey participants. They also allowed us to partially explore questions not in our survey (e.g., gender disclosure, motivation for using particular services, etc.). During the interview, we asked participants unique questions based on their responses to the survey. When necessary, we also asked follow-up questions to clarify their responses.

Of the 73 participants who indicated a willingness to participate in a follow-up interview, we invited 21 to participate in interviews. We recruited participants who provided non-trivial survey responses. We focused on recruiting those who shared experiences of privacy harm. Potential interviewees were sent an email outlining the interview procedure and inviting them to reply if they were still interested in being interviewed. Nine participants ultimately participated in interviews, five via Zoom and four via email-exchange. The average Zoom interview length was 16 minutes 42 seconds.

3.4 Qualitative Data Analysis

We analyzed responses to open-ended questions using qualitative coding [34, pg. 299-320]. The lead coder determined codes inductively based on 20% of the responses to each question. The lead coder and another author then independently coded the entire set of responses for each question. New codes were added during this stage as needed. After all responses were analyzed, the coders reconciled differences and finalized the code books for each question. The complete list of codes can be found in Appendix C. When appropriate, we reference responses from interviews to provide deeper qualitative insights. We refer to participants with the letter S followed by a number between 1 and 114. We provide specific demographic information for survey respondents who participated in interviews in Appendix E, table 3.

3.5 Correlational Analysis

In order to measure the extent to which participants' responses to the Likert scale questions relate to their reported level of outness, we computed Spearman's rank correlation coefficient (ρ) between the responses to each Likert scale question and the average OI score. In order to compute the average OI score, we exclude items where users selected N/A. The computation of ρ is non-parametric and does not require the data to be normally distributed. Values can range from -1 to 1, where an absolute value above .7 indicates a strong correlation, an absolute value between .7 and .4 indicates a moderate correlation, and an absolute value between .4 and .2 indicates a weak correlation [1]. We also provide a p-value, where a significant result corresponds to $p \leq \alpha = .05$. We report the complete results of the analysis in table 2 in Appendix D.

3.6 Inspection of Dating Services

In order to better understand the existing privacy posture of dating services, we systematically analyzed the privacy policies and privacy features of the five most popular online dating services used by our participants: Grindr, Tinder, Bumble, Hinge, and OkCupid. For each service, we first analyzed the privacy policy, recording the types of data collected and how that data is used. We then installed the Android app for each service on a Samsung Galaxy Z Fold 3, running Android version 13 and OneUI 5.1. We completed the registration process for each service using fake personal details. We then reviewed all settings in each application, recording the privacy-related features available on each service. We did not interact with any users during this process. All steps were completed on April 4-5, 2023. We reference the results of this analysis when appropriate in order to contextualize participant responses. For example, this analysis allowed us to evaluate whether certain requested features existed. It also permitted us to determine the institutional data-sharing practices of the most popular dating services. Finally, we considered these results when developing recommendations for changes.

3.7 Ethics

Due to the sensitive nature of this study and the risk of harm to our participants, we took ethics very seriously. Carnegie Mellon University's Institutional Review Board approved our complete study protocol. To protect participants' privacy, all participants could complete the survey anonymously. For those who wished to enter the raffle, we collected email addresses in a separate survey so that their email would not be tied to a specific survey response. Email addresses collected for compensation and facilitating interviews were deleted after the study. Audio recordings of the interview were deleted once the interviews had been transcribed. Email-exchange threads were deleted once the contents were extracted. All potentially identifiable information disclosed during interviews (e.g., name, place of work, etc.) was redacted from interview transcripts and email-exchange threads. Analysis was performed on password-protected devices that were only accessible to the team of researchers. To protect participants' emotional well-being, all participants were informed during the consent process that they could discontinue participation at any time. Interview participants were told that they could choose not to answer any questions or stop participating at any time while still receiving compensation. No participants expressed concerns about their emotional well-being during or after the study.

3.8 Limitations

Due to our recruitment methods, college students, Grindr users, and men are overrepresented in our sample. In addition, participants who were willing to volunteer for our study may differ from the larger population of LGBTQ+ people who are in the closet (i.e., self-selection bias [4]). For example, they may be more conscious of privacy issues (and thus interested in discussing them with researchers) but not so private that they are unwilling to share information with researchers that they might not share with friends or family. Our broad definition of being in the closet may also have led to some people participating in the study who would not typically be defined as closeted. We could only recruit a small subset of survey participants for interviews, which may limit the validity of these results. We rely on users to self-report experiences, and the results may be influenced by social desirability bias [22] or poor recall of past events. Finally, our qualitative coding is necessarily subjective and influenced by the experience and attitude of the

Table 1: Summary of participant demographics collected via the survey. Some demographic category names are shortened for space, but the complete text can be found in appendix B.

Age (Years)		Race/Ethnicity		Education	
18 to 25	49.1%	American Indian or Alaska Native	1.8%	Less than high school	1.8%
26 to 33	32.5%	Asian	14.0%	Graduated high school	20.2%
34 to 41	7.0%	Black	15.8%	Some college education	28.1%
42 to 49	5.3%	White	65.8%	Associate's degree	6.1%
50 to 57	3.5%	Self-describe	7.9%	Bachelor's degree	26.3%
Above 57	2.6%	No response	0.9%%	Degree beyond bachelor's	17.5%
No response	0%			No Response	0%

Gender		Sexual Orientation		Household Income	
Agender	0.9%	Asexual	1.8%	Less than $25,000	24.6%
Women	25.4%	Bisexual	32.5%	$25,000 to $50,000	23.7%
Genderqueer	4.4%	Homosexual	34.2%	$50,000 to $100,000	22.8%
Men	57.9%	Pansexual	12.3%	$100,000 to $200,000	14.9%
Non-binary	7.9%	Queer	12.3%	More than $200,000	5.3%
Self-describe	3.5%	Self-describe	6.1%	No Response	8.8%
No response	0%	No Response	0.9%		

researchers. Another research team may have identified different codes after reviewing the data.

4 RESULTS

In this section, we present the results of our study. In order to contextualize our findings, we begin by summarizing the characteristics of our participants, including their demographics, usage of dating services, and responses to the OI questions. We then discuss the results concerning each research question. Critical takeaways regarding each research question are shown in bold.

4.1 Participant Characteristics

Table 1 summarizes the demographic characteristics of our participants. Our sample is primarily young men. The population of US-based dating service users is also mostly young men [46]; however, the demographic imbalance is less extreme than observed in our sample. The voices of women and those older than 33 are likely underrepresented in our results.

The most common dating service used by our participants was Grindr (66.7%), followed by Tinder (57.0%), Hinge (32.5%), Bumble (27.2%), and OkCupid (7.9%). The majority (68.4%) of participants used more than a single dating service. When asked why they used particular dating services, most interviewees gave answers related to the popularity or features of the service rather than privacy. For example, S102 stated that they use Grindr and Tinder the most because "I am more likely to be able to interact with someone and have that lead to a date or a hookup." When asked whether privacy considerations affected their choice of dating service, S102 stated, "Privacy hasn't factored into my consideration of which apps to use." Similarly, when asked why they use Grindr, S66 stated, "It seems more popular in the area in which I live."

S11, a non-binary person who identifies as queer, did mention a specific privacy feature as motivation for using a dating service. When asked in their interview why they use OkCupid, they wrote, "I've heard that OkCupid is great for LGBT people. It also has a well-developed web experience so I don't have to use it on my phone: using a dating app on my phone has always been nerve wracking since a notification (e.g. 'David sent you a message!') can easily out me. I used to use Tinder and would delete the app before seeing family. OkCupid sends message notifications over email so I don't have to worry as much..." S33, a woman who identifies as pansexual, also mentioned a privacy motivation for her selection of dating service, albeit as a reason not to use a particular app. When asked in her interview why she uses Bumble and Hinge, she mentioned having a positive experience with these services. She added that she does not use Tinder because her grandfather uses the application. She stated, "I know my grandpa only uses Tinder, so I think that gives me peace of mind because he's not on Hinge or Bumble. I don't think he really knows how to use them.... The rest of my family members, except for, like my cousins, aren't on dating apps, and I would be fine if my cousins found out."

The vast majority of our sample reported using dating services frequently and for an extended period. 73.7% of the participants reported using dating services a few times a week or daily. 84.2% of participants reported that they began using online dating services at least a year ago, with 50% of all participants using dating services for more than three years. Finally, 40.4% of participants reported that their primary purpose for using a dating service was "to have casual sex," 27.2% of participants reported that they wanted "to find a romantic partner," and 14.0% selected that they wanted "to meet new friends or acquaintances." Many users likely have multiple, overlapping purposes for engaging with dating services. For example, when asked in a follow-up interview about their reason for using dating services to find friends, S106 clarified that they look to "[meet] new friends and see if there's something more to it." They elaborated, "I wouldn't say I trust dating app[s] that much, so I wouldn't just go for a relationship... that quickly."

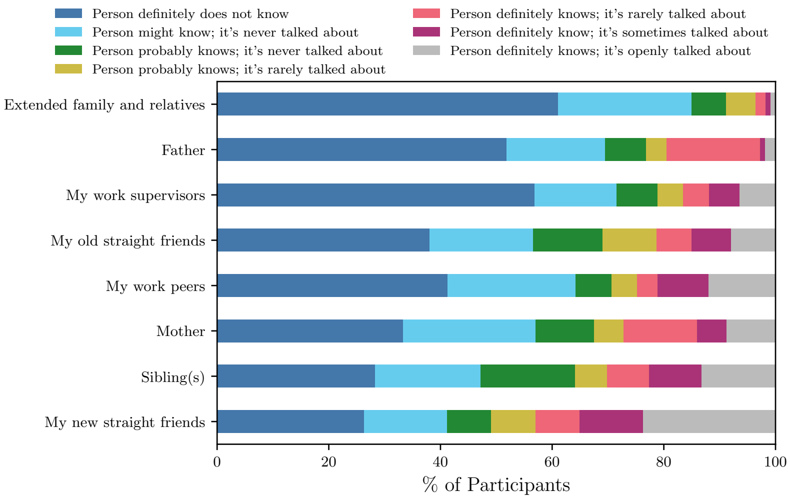


Figure 1: Summary of how "out" participants are to different types of social relations. The category labels are shortened to conserve space, but the complete text can be found in Appendix B. Categories are ordered from lowest to highest average OI value.

Figure 1 displays the results of the set of outness inventory questions. The participants were least likely to be open about their sexuality to their extended family/relatives, work supervisor(s), or father. Participants were most likely to be open about their sexuality to their "new straight friends." 24.6% of participants indicated that they rarely or never discussed their sexuality with any of the individuals or groups included in the OI. Only 1 participant indicated that all individuals or groups in the OI "probably" or "definitely [knew] about [their] sexual orientation."

The mean OI score was 2.74. Although the comparison is imperfect due to variations in implementation, this value is lower than that reported by other surveys with the general LGBTQ+ population in the US. For example, a 2007 study by Balsam et al. [2] reported an average OI of 4.89 with a community sample of 613 lesbian, gay, and bisexual (LGB) adults. In their 2014 online study of LGB adults, Meidlinger et al. [47] reported a mean OI score of 3.80 for 24 bisexual people, a mean OI score of 4.43 for 23 "mostly gay/lesbian" people, and a mean OI score of 5.10 for 102 gay or lesbian people. Insofar as the OI is an accurate measure of outness, this result suggests that we succeeded in recruiting a sample that is more closeted than the general LGBTQ+ population.

As previously stated, the OI does not capture how participants present their gender identity. The OI questionnaire focuses exclusively on sexual orientation. Some LGBTQ+ people may be more open about their sexual orientation than their gender identity. For example, we asked S102, a non-binary person who identifies as queer, to discuss how "out" they are about their sexual orientation and gender identity, respectively, in their interview. They wrote, "I am more 'out' about my sexual orientation... I only discuss the fact that I'm nonbinary with other nonbinary or queer people who can be more understanding, and I worry that people outside of the community will ask a lot of questions about what that identity means." In response to the same question in their interview, S1, a non-binary person who identifies as pansexual, wrote, "I wouldn't say I'm very out about either of [my identities] to anyone in my personal life... only my very best friends would know even one of [my identities], and even fewer would know both."

4.2 RQ1: Privacy Concerns

Eight of the Likert scale questions attempt to assess the extent to which our participants have specific privacy concerns (Q17.2-4, Q18.1-5). Figure 2 displays the proportion of participants agreeing or disagreeing with each statement, in order from statements with the highest to lowest proportion of disagreement. Two statements have opposite polarity and are therefore separated from the other statements by a dashed line. Additionally, 35.1% of participants reported that their privacy had been violated in some way (Q22). We discuss the results of the Likert scale questionnaire below, along with relevant descriptions of privacy violations.

Study participants expressed the strongest negative sentiment towards statements describing institutional data sharing practices. An equal proportion of participants (79.8%) disagreed or strongly disagreed that they are "fine with" non-dating websites purchasing anonymous information from dating services (Q18.4) and profile data being used for personalized advertising (Q18.5). Likely prompted by these statements, several participants expressed dissatisfaction with data sharing when asked what should be changed to protect their privacy better (Q24). S91, a woman who identifies as biromantic and demisexual, wrote, "I don't know if dating apps sell that data to personalise ads, but if they do I would prefer that they dont." Similarly, S60, a man who identifies as homosexual, responded to the same question by stating that he did not want to "...have info sold to companies as a means to show personal ads." When asked if his privacy had ever been violated (Q22), S64, a man who identifies as bisexual, described that he "...used to get YouTube ads that were clearly asking to take a gay test to see

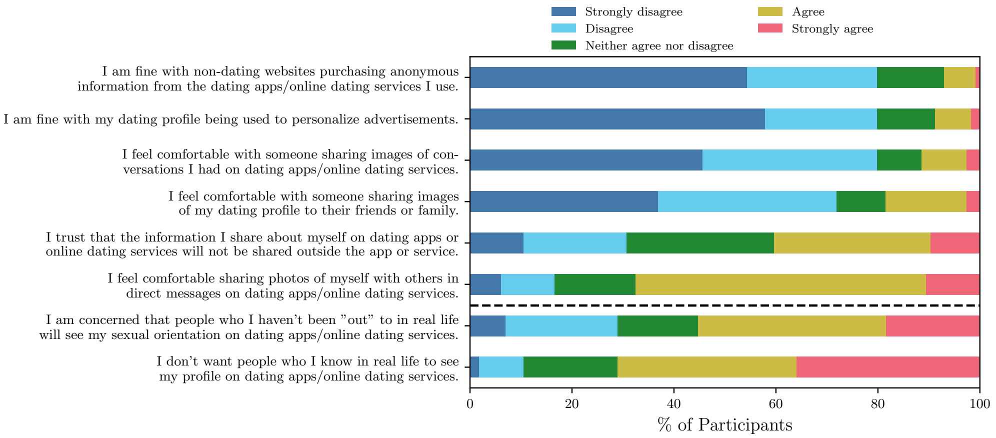


Figure 2: Proportion of participants selecting each response for Likert scale questions related to privacy concerns. Statements are organized from highest to lowest proportion of disagreement. A dashed line separates two statements with opposite polarity. The complete questions can be found in Appendix B.

how much of a gay someone could be....” While targeting based on sensitive attributes such as race or sexual orientation is generally prohibited by advertising platforms, advertisers may still target based on keywords or topics of interest that are closely related to one’s sexual orientation or gender identity [77].

Participants reacted negatively to statements describing someone taking and/or sharing images of activity on dating services. 79.8% of participants disagreed or strongly disagreed that they were comfortable with someone sharing images of conversations they had on an online dating service (Q18.3). 71.9% of participants disagreed or strongly disagreed that they were comfortable with someone sharing an image of their online dating service profile (Q18.2). Notwithstanding this adverse reaction, some participants indicated that they had engaged in similar behavior. The majority of participants (54.4%) agreed or strongly agreed that they had previously taken screenshots of images or messages they had received on online dating services (Q19.4). Half of the participants agreed or strongly agreed that they had shown conversations they had on online dating services to other people (Q20.1). Almost as many (43.0%) agreed or strongly agreed that they have shown other people’s dating profiles to their friends or family (Q19.5).

Most participants in Cobb et al.’s study [10] were also concerned by others taking screenshots of dating service activity. Around half of their participants also reported taking screenshots of others’ dating profiles or messages. Some users may wish to share images of other’s profiles for safety reasons (i.e., so the person they are meeting with can be identified if something goes wrong). Screenshots of messages may be taken for sentimental reasons [10], to publicly shame people perceived to be behaving badly (e.g., “West Elm Caleb” [63]), or for entertainment (e.g., [15, 43]). Closeted individuals may be more at risk for harm from people taking and sharing photos of activity dating services, but their concern about screenshot sharing is not unique.

Participants expressed a strong desire to avoid people they knew in real life while using dating services. The statement “I don’t want people who I know in real life to see my profile on dating apps/online dating services” had the strongest (negative) correlation with average OI ($\rho = -.449$, p-value $< .001$) with 71.1% of participants indicating that they agreed or strongly agreed with the statement. The negative correlation indicates that participants with a lower average OI score (i.e., participants who were less out) were more likely to agree with this statement. Similarly, responses to the statement “I am concerned that people who I haven’t been ‘out’ to in real life will see my sexual orientation on dating apps/online dating services.” had a weak, negative correlation with average OI score ($\rho = -.385$, p-value $< .001$). 55.3% agreed or strongly agreed with this statement. When asked if their privacy had ever been violated, a few participants (3) described incidents of “context collapse” where people they knew in real life found their dating profiles. For example, S86, a man who identifies as homosexual, shared, “A coworker approached me after finding one of my dating profiles and publicly asked questions about it.” S7, a man who identifies as bisexual, wrote, “...I’ve had people show friends I was on apps who didn’t know I was bisexual.” These experiences reflect the inability of users to control who sees their dating profiles fully.

Perhaps because of the risk of inadvertent disclosure, survey participants were pretty divided in their responses to the statement, “I trust that the information I share about myself on dating apps/online dating services will not be shared outside the app or service.” 40.4% of participants agreed or strongly agreed with the statement, 30.7% of participants disagreed or strongly disagreed, and 28.9% of participants neither agreed nor disagreed. In his interview S25 expressed trust that the LGBTQ+ community on dating services would not violate his privacy, stating, “I just like don’t expect any like queer person who is also on these apps to like, find this information, and share with, like my parents or my family, who I’m not... out to.”

The high degree of concern over encountering social relations on dating services seems to distinguish closeted individuals from the general population of users. For example, while inadvertent disclosure of profile information is discussed by Cobb et al. [10] as a potential privacy risk of using dating services, their respondents expressed both positive and negative sentiments towards encountering people they knew on dating services. Their participants were most strongly concerned about dating profiles being viewed by coworkers or employers, although some expressed concern about family or friends viewing their profiles.

Most participants felt comfortable sharing photos of themselves with others; however, this was also a common vector for harm. 67.5% of participants agreed or strongly agreed with the statement, "I feel comfortable sharing photos of myself with others in direct messages on dating apps/online dating services." The most frequently reported privacy harms related to the unauthorized saving or sharing of photos. Eight participants described how people shared their photos without permission. For example, S13, a man who identifies as bisexual, wrote that "...[someone] told me that he will share my videos and pics in websites." S39, a man who identifies as homosexual, shared that his privacy was violated when "...Someone [shared] photos and conversations to a person who then Messaged me telling me what had happened." Two other participants described people violating their privacy by downloading or taking screenshots without sharing them. S66, a man who identifies as homosexual, described how someone he met on Grindr took screenshots of photos he shared on the messaging app Snapchat. He stated, "...you get the message that a screenshot has been taken, and they don't ask. And that's just very unsettling because you don't know what they are going to do with that... picture that... you share with them."

In some cases, photos were used as a method of extortion. For example, when asked if their privacy had ever been violated, S63, a man who identifies as bisexual, wrote, "Someone used my photo and also threatened to blackmail me with an [in]appropriate video of me. I chose to ignore it and thankfully nothing happened." S74, a woman who identifies as pansexual, described a similar incident where someone tried to force them into interaction. In her survey response, she wrote, "...a couple of years ago I had someone who figured out who I really was get angry with me and they threatened to out me on social media." In her interview, she explained, "At the time I had only recently graduated from high school, and they recognized who I was by this half sliver of my face... I was like 'No... I don't really want to talk to anybody that I went to high school with' and they got angry by that, and they were like 'well, you know I know it's you and I already screenshot your picture... and if you don't hang out with me or continue to talk to me, I'm going to post your profile and this half picture of you online." Ultimately, S74 did not give in to the threat, and she faced no consequences. She shared, "I was like 'Well, I don't want you to do that, but I'm not going to hang out with you,' and they just never did anything, so I think they are really just trying to call my bluff. I suppose." Other survey participants described being threatened with outing, but did not describe a specific motive. For example, S85, a man who identifies as bisexual, shared that "Someone looked me up on Facebook and threatened to out me." In total, eight participants discussed either being extorted or threatened with outing.

Closeted users are especially vulnerable to extortion based on their LGBTQ+ identity; however, both closeted and non-closeted users alike may be threatened with extortion using intimate photos and videos shared on dating services. This "sextortion" is relatively common both on and off dating apps, including among individuals under 18 [50, 80]. It has even led to the death of victims [3].

Participants also discussed several other types of harm previously described in the literature. Four participants described some form of harassment or stalking. For example, S111 wrote in their survey response that a "stalker tried to message me across many accounts and somehow figured out the general area i live in, continually objectifying me and pleading me for favors until i threatened to contact law enforcement." In their interview, when asked if anything happened as a result, they added, "They messaged for the first time in years a month or two ago, and I immediately blocked." Two participants described someone impersonating them. S28, a man who identifies as homosexual, wrote, "People represented my intimate pics as their own." S70, a man who identifies as bisexual, wrote, "Someone recently used my profile name and pic claiming to be me."

The non-privacy harms discussed by our participants are not unique to closeted individuals. In a qualitative study with 20 sexual minority participants living in rural areas, Lauckner et al. [33] observed similar safety harms. In their sample of mostly men, they observed "catfishing" or impersonation, harassment, and sexual coercion. Similar concerns were among those raised by participants in Cobb et al. [10], suggesting that all users of dating services face these risks.

4.3 RQ2: Privacy-protecting Behavior

Six of the Likert scale statements were related to information disclosure and strategies that participants may use to protect their privacy (Q17.1, Q17.6, Q19.1-3, and Q20.2). Figure 3 displays the proportion of participants agreeing or disagreeing with each statement, in order from statements with the highest to lowest proportion of agreement. We discuss responses to these statements below, along with other participant responses related to privacy-protecting behavior.

Most participants try to protect their privacy in some way, often by restricting the information and photos they include in their profiles. The majority (71.1%) of participants answered "Yes" when asked if they did anything to protect their privacy on online dating services (Q15), with 43.9% of participants describing more than a single strategy. Unprimed, 36 participants shared that they do not use their full name; 22 participants indicated that they avoid disclosing their exact location; 6 participants avoid disclosing their occupation or educational institution; and 14 participants specified that they generally try to restrict the amount of information they share. An overwhelming majority (84.2%) of participants agreed or strongly agreed with the statement that they limit the amount of information they include in their dating profile (Q19.1).

We asked participants to select the information they typically include in their dating service profiles (although we realize that this may vary over time and by platform). The vast majority of study participants indicated that they include their gender (85.1%), age (81.6%), sexual orientation (71.1%), physical characteristics (68.4%), general location (67.5%), or photos of self (65.8%) in their profile. Of the 80 participants who saw the question about location permissions, 86.3% indicated that the dating service(s) they use requires access to location data. Less than half of participants use their first

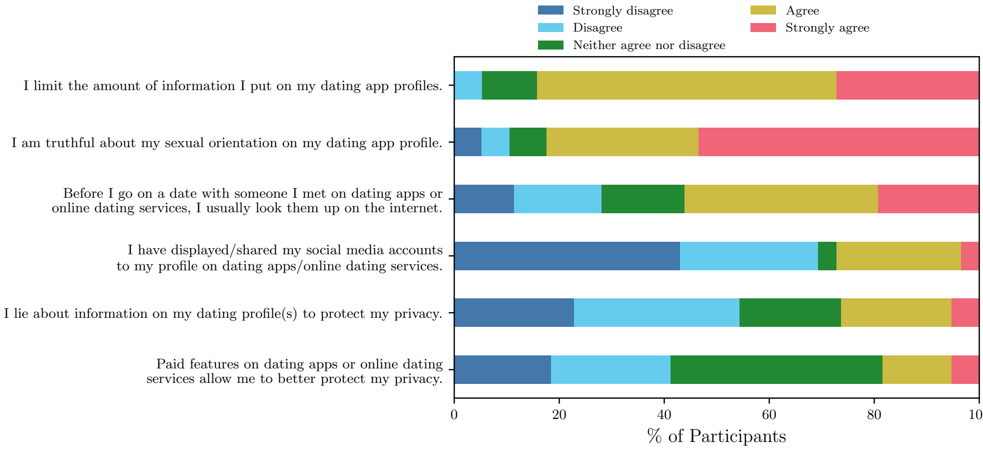


Figure 3: Proportion of participants selecting each response for Likert scale questions related to information disclosure and privacy-protecting behaviors. Statements are organized from highest to lowest proportion of agreement. The complete text can be found in Appendix B.

name (38.6%) or even just their initials or a nickname (24.6%). Less than 10% of participants indicated that they included their exact location (9.65%), full name (7.02%), or other information (4.39%). Finally, about a quarter (27.2%) of study participants agreed or strongly agreed with the statement that they have displayed links to other social media services in their dating service profiles (Q19.2). Some participants (five unprimed and seven primed) described not sharing their social media profiles as a strategy to protect their privacy. While linking a social media account associated with one's real-world identity may deanonymize users, linking to other social media platforms can provide utility. For example, a user might reference a profile on a platform with additional message privacy features (e.g., Snapchat or Telegram) to make it easy to move the conversation off the dating service.

Participants also discussed restricting the photos they share in various ways to protect their privacy. Participants most often wrote that they did not include their faces in photos they shared (12 unprimed, five primed). Some participants (seven unprimed, one primed) avoid including photos in their profile altogether. Two participants (unprimed) indicated that they avoid sharing publicly available photos. Two participants (unprimed) shared that they avoid including their tattoos in their photos. Some participants described restricting photos in other specific ways (nine primed, five unprimed). For example, S5, who identifies as non-binary and queer, wrote, "I make sure that you can't tell where I am in the pictures I take, so no scenic backgrounds or anything with street names in the background." Restricting photo-sharing was also observed as a privacy-protecting strategy in Waldman's study of intimate photo sharing practices with men who have sex with men [73, 75] and Lerner et al.'s study of the online computer security and privacy practices of transgender people [38]. Not sharing intimate images with identifying information may be an excellent way to avoid sextortion, as an attacker may not be able to prove that a photo shows the victim.

As one may expect, closeted users seem to include less identifying information in their profiles as compared to the general population of dating service users. For example, in Cobb et al. [10]'s survey, 63.9% of participants reported including their first name on their dating profile, and only a single participant reported not including pictures of their face. These information restriction strategies may help prevent the re-identification of users off of the dating services. Not including photos in one's profile or cropping one's face out of profile pictures likely prevents identification by a passive observer. Depending on the specific combination of information that a user includes in their profile, however, it may be possible for a determined adversary to identify them. Especially in geographic areas with few users of a particular service, one's age, gender, general location, and photos may be sufficient to permit re-identification [67]. If a user provides additional information in conversation, this may help an attacker to narrow their search.

In coordination with their strategy of information restriction, many participants (11 unprimed, five primed) discussed some form of screening process that they use to determine whether to share more information with another person on a dating service. For example, S111 said that they "crop out face on my profile [and] only share it with those i become comfortable with..." When asked in their interview to explain how they chose whom to share their full photos with, they wrote, "Usually all I require is a good vibe from the other person, a conversation to tell if they're nice and not weird right off the bat or an interaction to show i can trust them to be a real person. A picture of themselves is usually mandatory." Similarly, S66 shared on the survey that "I only share pictures when trust is developed. I also work to build trust!" When asked to describe how he built trust with others, he said he has "basically multiple conversations. Really trying to get to know someone in... that virtual world."

This strategy may not be effective against an active adversary (e.g., one planning to extort a user). An attacker may be willing and able to have a normal conversation long enough to elicit photos or other identifying information. If a photo is requested of them, the attacker could use photos available online or from other users to mimic an equitable exchange.

Most participants indicated that they do not lie to protect their privacy on their dating profiles. More than half (54.4%) of study participants disagreed or strongly disagreed with the statement that they lie about information on their profile to protect their privacy, with only 26.3% of participants agreeing or strongly agreeing with the statement. Additionally, a large majority of participants (82.5%) also agreed or strongly agreed with the statement that they are honest about their sexual orientation on dating app profiles (Q17.1).

Few participants indicated using paid dating service features to protect their privacy. 41.2% of participants disagreed or strongly disagreed with the statement that paid features help them protect their privacy. 40.4% neither agreed nor disagreed. Considering only the 27.2% of participants who agreed or strongly agreed with the statement, "I have paid to access additional features on dating apps/online dating services," a plurality of 45.2% still disagree or strongly disagree with the statement that paid features help protect their privacy. Only four participants, all primed by viewing the Likert-scale statements, indicated that they use premium features to protect their privacy. For example, S64 wrote, "When I was using the paid version [of Grindr], I used to unsend pictures if I didn't trust someone or block[ed] them."

Very few participants discussed using technical means to protect their privacy. Most often, participants described using different throwaway accounts either to register for dating services or to contact others outside the service. For example, S15 wrote, "Often I will use a fake # to chat with people off the app." S85 wrote that he "...uses a basic email that doesn't link directly to [him]." A few (two unprimed, one primed) mentioned using a VPN to protect their privacy, although they did not detail how they felt the VPN helped them protect their privacy. A VPN may be useful for preventing others on a network or the ISP from seeing their traffic. This functionality could be useful for closeted individuals who fear that accessing dating services may out them to network operators (e.g., their school, employer, family members, etc.)

4.4 RQ3: Improving Privacy Experiences

When asked in the survey what features they would like to protect their privacy better, users requested a wide variety of changes. We discuss the nature and frequency of suggestions made in survey free-response questions and participant interviews.

The most commonly requested type of feature (14 participants) was some form of enhanced profile visibility controls to help avoid inadvertent disclosure. Most often, this was expressed as a desire to prevent specific people from seeing their profiles. S102, who uses Tinder, Grindr, and Bumble, wanted platforms to "Give users more control over whom their profile is shown to. This would reduce the likelihood of someone they are not comfortable being out to happening upon their profile." When asked in their interview to explain how they imagine this feature working, they elaborated, "I imagine that this feature would allow you to block certain groups from seeing your profile. For example, options to 'only show my profile to: ____' would be helpful. I would love to be able to limit my profile's visibility to people within my age group, for example, or to limit my profile's visibility to other people who identify as queer on their account. It would also be nice to block your profile from other accounts that it can recognize in your contacts, so you could choose to restrict people you know from seeing your account." The idea of blocking contacts is implemented in Tinder but not the other services S102 uses. Some users requested the broader ability to hide one's profile entirely. S39, who uses Tinder, Grindr, Bumble, and OkCupid, requested the ability to "[allow] your profile to be shown or hidden." It is not entirely clear what enhancement he wants, as all four of the dating services he mentioned provide the ability to hide one's profile. He may be unaware of these settings or desire the ability to interact with others while remaining hidden.

The next most common feature request (13 participants) was a method to limit screenshotting or downloading photos to prevent their misuse. S14, who uses Tinder, Grindr, and Hinge, requested "An app that is completely bulletproof from people stealing other peoples' images." Similarly, in their survey response, S66 stated that Grindr should "[stop] the ability to screen shot... Scruff does not allow screen shots." When asked in his interview why he stopped using Scruff despite it having this feature, he stated, "...I live in a very rural area... there aren't a lot of people on [Scruff] in my area." While people may be able to circumvent restrictions, blocking screenshots would help protect users from all but the most determined attackers.

Some participants (13) expressed a desire for features that are currently only enabled by premium subscription to be available to free users. Several users opined about the unfairness of paid privacy features. For example, S15, who uses Tinder and Grindr, wrote, "I think it's crazy that you must pay for privacy features, they should be standard." Other users named specific features. For example, S108 and S87 requested that the "incognito mode" of Grindr, Tinder, Bumble, and OkCupid be free. While the specifics vary, incognito modes allow users to hide their profile from most users while still being able to speak with or match with new people. Other paid features that participants requested be made available for free include the feature to unsend messages (Grindr), expiring photos (Grindr), and the ability to share private photo albums (Grindr).

Some participants (8) requested the ability to disable or limit the use of their exact location. For example, S54, who uses Grindr, Hornet, and Blued, suggested, "Maybe [they] can support the feature of disabling GPS." Of the dating services we investigated, OkCupid and Hinge allow you to use the service without providing location permissions. Allowing users to provide only a general location, as permitted by OkCupid or Hinge, could protect users from triangulation attacks. However, Tinder, Bumble, and Grindr may be unwilling to allow disabling GPS, as each service offers a paid feature where you can input a city name and view profiles at that location. Allowing users to set their location manually would make this feature less useful.

Some participants who requested the ability to limit or turn off GPS services wanted the specific ability to hide their distance from other users. For example, S111 wrote on the survey that Grindr should "add an option to not show specific distance... (EG, 1,234 feet away is way too specific)." This feature is already available on

Grindr, Tinder, and Bumble, while Hinge and OkCupid only show the city or neighborhood in which a person lives. When informed that this feature does exist, S111 wrote, "Thanks! I assumed this was a premium feature, i had not been able to easily find it myself." This example reflects a trend where several users were seemingly unaware of existing privacy features.

This lack of knowledge, even among a population with high privacy concerns, may suggest that dating services should place greater emphasis on privacy education when onboarding users. Three participants explicitly requested improved privacy education. For example, S63, who uses Grindr and OkCupid, requested "More transparency in how the data is being used? Usually it's in the form of a T&C which people don't really read. It's not digestible." S86, who uses Tinder, wrote that the service could include "...maybe a quick tutorial before you add photos to remind you to be careful of adding photos with identifiable info or ones that could be easily imaged searched on google." Tinder highlights privacy and safety features by including a safety center with guides on configuring the application and staying safe in real life. During the registration process, Tinder also highlights the ability to block specific people from your contacts. In order to improve users' experience, other services could include similar privacy education measures.

Some participants (6) requested a form of user verification to reduce impersonation and fraud. S79, who uses Bumble, Hinge, HER, Zoe, and Taimi, wrote, "I think profiles should always be verified because there are a lot of scammers out there." Similarly, S49, who uses Tinder, Grindr, Bumble, and Hinge, requested "A feature to only see verified people and reduce the bots that message. Some services have this but I wish especially Grindr would add this." All of the services we investigated except Grindr have some form of selfie verification where a live photo or video of a user is compared to the photos in their profile. If the user matches, they receive a verified mark on their profile. S73, who uses Tinder, Bumble, and Hinge, wrote that to protect her privacy, "i verify my account and don't like anyone that isn't verified." In the interview, she further explained, "'I feel as though people who are verified are less likely to be stalkers or catfish or people that I know making fake accounts and that gives me a sense of peace."

In addition to requesting new features, some participants requested enhancements to existing features. Most frequently, participants requested improvements to how blocking other users works (5 participants). Grindr was the most frequent target for criticism as it limits the number of people a free user can block per day. For example, S71, who uses Tinder and Grindr, wrote that Grindr should "Allow unlimited blocking." This limitation represents a clear safety risk, as users may be prevented from blocking users who are harassing or stalking them. Some users also criticized Tinder's blocking. S46, who only uses Tinder, wrote that he wants "...easier ways to report and block profiles for misconduct that remove[s] your profile from their screens." You can block users encountered in the discovery queue, but you can only "unmatch" people whom you have already liked and matched with. While this appears to be functionally the same as blocking, it may improve usability if a block option is included.

Many of these feature requests directly relate to the risks closeted individuals face; however, they could benefit all users. For example, considering participants' adverse reactions to encountering social relations, it is understandable that many requested better profile visibility controls. If implemented, visibility controls could help all users avoid inadvertent disclosure, not just closeted users. Similarly, restricting the ability to download or screenshot photos would help all users avoid extortion and other unauthorized sharing.

5 DISCUSSION

In this section, we briefly summarize our results and then discuss changes that dating services could adopt that might improve the experience of closeted users.

Respondents expressed the most significant privacy-related concerns (RQ1) about non-dating websites purchasing anonymous information from dating sites, dating profiles being used to personalize advertisements, and the risk of encountering social relations while using dating services. A sizable minority of participants described some form of privacy harm they experienced while using a dating service. The most commonly described harms involved the unauthorized saving or sharing of photos sent to other users. Some users discussed being inadvertently forced out of the closet by encountering social relations on dating services. A few users described experiencing serious safety threats such as extortion, harassment, and stalking. Most participants discussed protecting their privacy in some way (RQ2), most often through limiting the amount of information and photos they share in their profile. Finally, users described a variety of features that may help improve their privacy (RQ3). The most common feature requests included enhanced profile visibility controls and limits on the ability to download or screenshot photos. Some participants also expressed dissatisfaction with privacy-enhancing features being available only to premium users.

Closeted users' desire to prevent inadvertent discovery by social relations is the privacy need that most distinguishes them from the general population. While non-closeted users may not want some people to see their dating service profiles, this need is typically less stringent. Tinder's feature that allows users to block specific contacts preemptively is the best tool we observed for helping users to prevent inadvertent outing. We believe other services should adopt it. It does have limitations, however, as the blocked contact must register with the phone number or email provided for their profile to be recognized. There is also some risk that dating services may misuse or inadvertently leak contact data users share. While Tinder states they only keep the contact data for contacts that users choose to block, users must still share their contact list to enable the feature.

Future work should investigate the feasibility of alternate blocking schemes. For example, a service might allow users to block any user from a particular location (e.g., a college campus or neighborhood) from seeing their account. This feature would technically enforce the practice of some participants to avoid using dating services in specific locations. Services might also add the feature suggested by S102: the ability to block other users by group identifiers, such as place of work and educational institution. An anonymous notification feature, as requested by S11, may also be helpful, as it would allow users to receive notifications for a dating service without fear that these alerts would out them to others nearby. None of these privacy features would be foolproof individually, but, used together, they may provide "defense in depth" against inadvertent exposure.

Participants' negative reactions to institutional data practices (e.g., dating services selling anonymized data and using profile information for targeted advertising) are similar to prior results with non-closeted populations [40]. The practice which participants reacted most negatively to—sales of profile information—was not disclosed in any of the privacy policies we reviewed and thus may not be a current practice. All the services use user data for advertising, a practice that most participants also disagreed with. While eliminating targeted advertising would reduce revenue, advertising represents a small portion of the revenue for the services we investigated. On a page describing their privacy policies, the Match Group states, "less than 3% of our revenue [comes] from advertising sales." [26] In Grindr's first-quarter 2023 financial fillings, indirect revenue, which primarily consists of advertising revenue, made up only 13.8% of Grindr's total revenue [24]. We could not find specific numbers for Bumble, but their first-quarter 2023 financial disclosure states that subscriptions are their primary source of revenue [6]. Future work could investigate the extent to which specific types of online advertising (e.g., contextual advertising, retargeting, etc.) may be acceptable in the context of online dating services, both with general users and other populations with privacy concerns.

The request to limit other users' ability to screenshot or download images on mobile dating apps is technically feasible and unambiguously positive. Grindr already limits screenshots for images shared via an album, although this feature is limited for free users.[3] Services with image sharing could allow users to opt in to allowing a conversation partner to download or screenshot a photograph. Although this would not eliminate the risk of others stealing images (e.g., by taking a photograph of an image using another device), this could reduce the risk of unauthorized pornography and extortion.

Other feature suggestions like user verification for Grindr offer both positives and negatives. By allowing users to create profiles with no information, Grindr is uniquely suited to facilitating private, online interactions between strangers. At the same time, the ability to remain anonymous makes it easier for fraudsters, spammers, and other malicious users to create accounts and evade bans. Adding a verification system to Grindr could allow some users to interact with others on the service more safely, but it may undermine the ability of others to use the service anonymously. Alternatively, services might consider verifying users by some form of ID, such as a driver's license. This feature would make it easier for dating services to identify and exclude malicious actors from using their services. Additionally, provided that users trust the dating service and are not required to share information from their ID publicly, this would provide a path for closeted users to be verified without exposing personal information to other users. ID-based age verification is increasingly used to restrict children's access to adult content online [59].

As with our proposal for more services to adopt contact-based blocking, ID-based verification comes with the risk of companies misusing or leaking ID data. Even if dating services do not handle ID data directly (i.e., by partnering with a service like id.me), users may still be uncomfortable with disclosing such data for the purpose of online dating. This form of ID-based verification would also not work for users with a mismatch between their legal name and gender and their preferred name and gender identity. Future work could investigate to what extent this type of user verification may be acceptable to closeted users or others with high levels of privacy concern. Services could potentially make verification optional and provide a profile badge for users who have been verified. They could also offer an option for those who have been verified to see and be seen by only other verified users.

It is also unclear to what extent paid privacy features could be made free. Dating services are businesses, and they must withhold some features from free users to make their paid service attractive. Some limitations on free users, like the daily block limit on Grindr, should be eliminated for safety reasons. Other features, like disappearing messages or incognito mode, may provide privacy benefits but are not necessarily essential. Users in our sample, like S66, reported using other services that provide messaging privacy features for free (e.g., Snapchat). Enabling these features for all users may allow users to avoid moving off platform to communicate with others.

Only about a quarter of users who indicated that they pay for a premium subscription also agreed that the premium features are useful for protecting their privacy. Extrapolating from this admittedly small and biased sample, it may be possible to make the premium privacy features available for free without harming subscription numbers. Some closeted users may refrain from using premium features due to a fear of financial transactions being viewed by others. For example, a "GOOGLE*Grindr LLC" charge could out a person due to the service's reputation as a dating service for LGBTQ+ people. If they cannot make privacy-preserving features available for free, dating services might consider billing under alternative names that are less likely to lead to scrutiny.

6 CONCLUSION

We conducted a survey with 114 participants and nine follow-up interviews to investigate three research questions: 1) What privacy concerns do individuals in the closet have in the context of online dating services? 2) How do individuals in the closet protect their privacy in the context of online dating services? and 3) How might online dating services better protect the privacy of individuals in the closet? Participants discussed a diverse range of experiences, including others downloading and sharing photos without their permission, inadvertent outing, extortion, and harassment. Most participants engaged in some form of privacy-protecting behavior, which typically involved limiting the information or photos they included in their public profiles. Respondents' most common feature requests include restricting the ability to download/screenshot their photos, better profile visibility controls, and making paid features available for free. We close by discussing the feasibility of these protection mechanisms and encourage work to improve the experience of closeted users.

[3] An album on Grindr is a private collection of photos that users can share with up to 5000 other users. Free users have limited access to albums [23].

ACKNOWLEDGMENTS

This research was supported in part by the Innovators Network Foundation, Meta, and the National Science Foundation under grant no. CNS-2150217. We would also like to thank Megan Li and Yanzi Lin, who helped to develop the study.

REFERENCES

[1] Haldun Akoglu. 2018. User's guide to correlation coefficients. *Turkish Journal of Emergency Medicine* 18, 3 (2018), 91–93. https://doi.org/10.1016/j.tjem.2018.08.001

[2] Kimberly F Balsam and Jonathan J Mohr. 2007. Adaptation to sexual orientation stigma: a comparison of bisexual and lesbian/gay adults. *Journal of counseling psychology* 54, 3 (2007), 306.

[3] Luke Barr. 2023. *Parents of teenager who died by suicide after sextortion scam urge 'tough' conversations with children.* ABC News. https://abcnews.go.com/US/parents-teenager-died-by-suicide-after-sextortion-scam-urge/story?id=99047305

[4] Jelke Bethlehem. 2010. Selection Bias in Web Surveys. *International Statistical Review* 78, 2 (2010), 161–188. https://doi.org/10.1111/j.1751-5823.2010.00112.x arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1751-5823.2010.00112.x

[5] Stacey M. Brumbaugh-Johnson and Kathleen E. Hull. 2019. Coming Out as Transgender: Navigating the Social Implications of a Transgender Identity. *Journal of Homosexuality* 66, 8 (2019), 1148–1177. https://doi.org/10.1080/00918369.2018.1493253 arXiv:https://doi.org/10.1080/00918369.2018.1493253 PMID: 30052497.

[6] Bumble. 2023. SEC Form 10-Q. Retrieved May 22nd, 2023 from https://ir.bumble.com/financials/sec-filings/default.aspx

[7] Logan S. Casey, Sari L. Reisner, Mary G. Findling, Robert J. Blendon, John M. Benson, Justin M. Sayde, and Carolyn Miller. 2019. Discrimination in the United States: Experiences of lesbian, gay, bisexual, transgender, and queer Americans. *Health Services Research* 54, S2 (2019), 1454–1466. https://doi.org/10.1111/1475-6773.13229 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.13229

[8] E. A. Cech and T. J. Waidzunas. 2021. Systemic inequalities for LGBTQ professionals in STEM. *Science Advances* 7, 3 (2021), eabe0933. https://doi.org/10.1126/sciadv.abe0933 arXiv:https://www.science.org/doi/pdf/10.1126/sciadv.abe0933

[9] Brad Sears Christy Mallory. 2016. *Evidence of Housing Discrimination Based on Sexual Orientation and Gender Identity: An Analysis of Complaints Filed with State Enforcement Agencies, 2008-2014.* Technical Report. UCLA School of Law Williams Institute. https://escholarship.org/uc/item/50c6h3qf

[10] Camille Cobb and Tadayoshi Kohno. 2017. How Public Is My Private Life? Privacy in Online Dating. In *Proceedings of the 26th International Conference on World Wide Web* (Perth, Australia) *(WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1231–1240. https://doi.org/10.1145/3038912.3052592

[11] Juliet Corbin and Anselm Strauss. 2014. *Basics of Qualitative Research Techniques and Procedures for Developing Grounded Theory* (4 ed.). SAGE, Thousand Oaks, CA, USA.

[12] Kimberlé Williams Crenshaw. 1994. Mapping the margins: Intersectionality, identity politics, and violence against women of color. In *The public nature of private violence*. Routledge, London, England, 93–118.

[13] Michael A. DeVito, Ashley Marie Walker, and Jeremy Birnholtz. 2018. 'Too Gay for Facebook': Presenting LGBTQ+ Identity Throughout the Personal Social Media Ecosystem. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 44 (nov 2018), 23 pages. https://doi.org/10.1145/3274313

[14] Valerie A. Earnshaw, Sari L. Reisner, Jaana Juvonen, Mark L. Hatzenbuehler, Jeff Perrotti, and Mark A. Schuster. 2017. LGBTQ Bullying: Translating Research to Action in Pediatrics. *Pediatrics* 140, 4 (10 2017), 20 – 29. https://doi.org/10.1542/peds.2017-0432 arXiv:https://publications.aap.org/pediatrics/article-pdf/140/4/e20170432/1097228/peds_20170432.pdf e20170432.

[15] Audrey Engvalson. 2019. *18 Dating App Convos That Are So Bad They're Funny.* Buzzfeed. https://www.buzzfeed.com/audreyworboys/tinder-convos-that-are-so-awkward-theyre-funny

[16] Brian A Feinstein and Roberto Rentería. 2023. Where Is the Line Between Being In versus Out of the Closet? *Archives of Sexual Behavior* 52 (2023), 1–5.

[17] Julia R. Fernandez and Jeremy Birnholtz. 2019. "I Don't Want Them to Not Know": Investigating Decisions to Disclose Transgender Identity on Dating Platforms. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 226 (nov 2019), 21 pages. https://doi.org/10.1145/3359328

[18] Jesse Fox and Rachel Ralston. 2016. Queer identity online: Informal learning and teaching experiences of LGBTQ individuals on social media. *Computers in Human Behavior* 65 (2016), 635–642.

[19] Karen I. Fredriksen-Goldsen, Hyun-Jun Kim, Chengshi Shiu, Jayn Goldsen, and Charles A. Emlet. 2014. Successful Aging Among LGBT Older Adults: Physical and Mental Health-Related Quality of Life by Age Group. *The Gerontologist* 55, 1 (09 2014), 154–168. https://doi.org/10.1093/geront/gnu081 arXiv:https://academic.oup.com/gerontologist/article-pdf/55/1/154/10309798/gnu081.pdf

[20] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, USA, 305–322. https://www.usenix.org/conference/usenixsecurity22/presentation/geeng

[21] Lorenzo Gios, Massimo Mirandola, Nigel Sherriff, Igor Toskin, Karel Blondeel, Sonia Dias, Danica Staneková, Cinta Folch, Susanne Barbara Schink, Christiane Nöstlinger, et al. 2021. Being in the closet. correlates of Outness among MSM in 13 European cities. *Journal of homosexuality* 68, 3 (2021), 415–433.

[22] Pamela Grimm. 2010. *Wiley international encyclopedia of marketing*. John Wiley & Sons, Ltd, Chichester, UK, Chapter Social desirability bias, 1.

[23] Grindr. 2023. Albums. Retrieved May 22nd, 2023 from https://help.grindr.com/hc/en-us/articles/4414580688787-Albums

[24] Grindr. 2023. SEC Form 10-Q. Retrieved May 23rd, 2023 from https://investors.grindr.com/financials/sec-filings/default.aspx

[25] Grindr. 2023. Unlimited. Retrieved May 30th, 2023 from https://help.grindr.com/hc/en-us/articles/1500008656741-Grindr-Unlimited-

[26] The Match Group. 2023. Privacy. Retrieved May 22nd, 2023 from https://match.com/privacy

[27] Oliver L. Haimson and Tiffany C. Veinot. 2020. Coming Out to Doctors, Coming Out to "Everyone": Understanding the Average Sequence of Transgender Identity Disclosures Using Social Media Data. *Transgender Health* 5, 3 (2020), 158–165. https://doi.org/10.1089/trgh.2019.0045 arXiv:https://doi.org/10.1089/trgh.2019.0045

[28] Audrey Heng, Clare Heal, Jennifer Banks, and Robyn Preston. 2018. Transgender peoples' experiences and perspectives about general healthcare: A systematic review. *International Journal of Transgenderism* 19, 4 (2018), 359–378. https://doi.org/10.1080/15532739.2018.1502711 arXiv:https://doi.org/10.1080/15532739.2018.1502711

[29] Nguyen Phong Hoang, Yasuhito Asano, and Masatoshi Yoshikawa. 2017. Your neighbors are my spies: Location and other privacy concerns in GLBT-focused location-based dating applications. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*. IEEE, New York, NY, USA, 851–860. https://doi.org/10.23919/ICACT.2017.7890236

[30] Susanna D Howard, Kevin L Lee, Aviva G Nathan, Hannah C Wenger, Marshall H Chin, and Scott C Cook. 2019. Healthcare experiences of transgender people of color. *Journal of general internal medicine* 34 (2019), 2068–2074.

[31] Shanna K. Kattari, Darren L. Whitfield, N. Eugene Walls, Lisa Langenderfer-Magruder, and Daniel Ramos. 2016. Policing Gender Through Housing and Employment Discrimination: Comparison of Discrimination Experiences of Transgender and Cisgender LGBQ Individuals. *Journal of the Society for Social Work and Research* 7, 3 (2016), 427–447. https://doi.org/10.1086/686920 arXiv:https://doi.org/10.1086/686920

[32] Brian Latimer. 2018. *Grindr security flaw exposes users' location data.* NBC News. https://www.nbcnews.com/feature/nbc-out/security-flaws-gay-dating-app-grindr-expose-users-location-data-n858446

[33] Carolyn Lauckner, Natalia Truszczynski, Danielle Lambert, Varsha Kottamasu, Saher Meherally, Anne Marie Schipani-McLaughlin, Erica Taylor, and Nathan Hansen. 2019. "Catfishing," cyberbullying, and coercion: An exploration of the risks associated with dating app use among rural sexual minority males. *Journal of Gay & Lesbian Mental Health* 23, 3 (2019), 289–306.

[34] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction.* Morgan Kaufmann, Burlington, MA.

[35] Ari Lazarus. 2021. How to spot extortion scams on LGBTQ+ dating apps. https://consumer.ftc.gov/consumer-alerts/2021/09/how-spot-extortion-scams-lgbtq-dating-apps

[36] Nicole Legate, Richard M. Ryan, and Netta Weinstein. 2012. Is Coming Out Always a "Good Thing"'? Exploring the Relations of Autonomy Support, Outness, and Wellness for Lesbian, Gay, and Bisexual Individuals. *Social Psychological and Personality Science* 3, 2 (2012), 145–152. https://doi.org/10.1177/1948550611411929 arXiv:https://doi.org/10.1177/1948550611411929

[37] Erica Lennon and Brian J. Mistler. 2014. Cisgenderism. *TSQ: Transgender Studies Quarterly* 1, 1-2 (05 2014), 63–64. https://doi.org/10.1215/23289252-2399623 arXiv:https://read.dukeupress.edu/tsq/article-pdf/1/1-2/63/485890/19.pdf

[38] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. 2020. Privacy and Activism in the Transgender Community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376339

[39] Leanna Lucero. 2017. Safe spaces in online places: social media and LGBTQ youth. *Multicultural Education Review* 9, 2 (2017), 117–128. https://doi.org/10.1080/2005615X.2017.1313482 arXiv:https://doi.org/10.1080/2005615X.2017.1313482

[40] Christoph Lutz and Giulia Ranzini. 2017. Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. *Social Media + Society* 3, 1 (2017), 2056305117697735. https://doi.org/10.1177/2056305117697735 arXiv:https://doi.org/10.1177/2056305117697735

[41] Jimmie Manning. 2015. Communicating sexual identities: A typology of coming out. *Sexuality & culture* 19, 1 (2015), 122–138.

[42] Joseph Marchia and Jamie M Sommer. 2019. (Re)defining heteronormativity. *Sexualities* 22, 3 (2019), 267–295. https://doi.org/10.1177/1363460717741801 arXiv:https://doi.org/10.1177/1363460717741801

[43] Hannah Marder. 2023. *31 Dating Profiles So Horribly Cringe-Worthy, I Can't Believe Someone Actually Posted Them.* BuzzFeed. https://www.buzzfeed.com/hannahmarder/terrible-dating-profiles

[44] Alice E Marwick and Danah Boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New media & society* 13, 1 (2011), 114–133.

[45] Edward McCann and Michael Brown. 2019. Homelessness among youth who identify as LGBTQ+: A systematic review. *Journal of Clinical Nursing* 28, 11-12 (2019), 2061–2072. https://doi.org/10.1111/jocn.14818 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/jocn.14818

[46] Colleen McClain and Risa Gelles-Watnick. 2023. *From Looking for Love to Swiping the Field: Online Dating in the U.S.* Technical Report. Pew Research Center, Washington, D.C., USA. https://www.pewresearch.org/internet/2023/02/02/from-looking-for-love-to-swiping-the-field-online-dating-in-the-u-s/

[47] Peter C Meidlinger and Debra A Hope. 2014. Differentiating disclosure and concealment in measurement of outness for sexual minorities: The Nebraska Outness Scale. *Psychology of Sexual Orientation and Gender Diversity* 1, 4 (2014), 489.

[48] Jonathan Mohr and Ruth Fassinger. 2000. Measuring Dimensions of Lesbian and Gay Male Experience. *Measurement and Evaluation in Counseling and Development* 33, 2 (2000), 66–90. https://doi.org/10.1080/07481756.2000.12068999 arXiv:https://doi.org/10.1080/07481756.2000.12068999

[49] Molly Olmstead. 2021. A Prominent Priest Was Outed for Using Grindr. Experts Say It's a Warning Sign. https://slate.com/technology/2021/07/catholic-priest-grindr-data-privacy.html

[50] Roberta Liggett O'Malley and Karen M. Holt. 2022. Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of Interpersonal Violence* 37, 1-2 (2022), 258–283. https://doi.org/10.1177/0886260520909186 arXiv:https://doi.org/10.1177/0886260520909186 PMID: 32146856.

[51] Jason Orne. 2011. 'You will always have to "out" yourself': Reconsidering coming out through strategic outness. *Sexualities* 14, 6 (2011), 681–703. https://doi.org/10.1177/1363460711420462 arXiv:https://doi.org/10.1177/1363460711420462

[52] John E Pachankis and Richard Bränström. 2019. How many sexual minorities are hidden? Projecting the size of the global closet with implications for policy and public health. *PLoS One* 14, 6 (2019), e0218084.

[53] John E Pachankis, Susan D Cochran, and Vickie M Mays. 2015. The mental health of sexual minority adults in and out of the closet: A population-based study. *Journal of consulting and clinical psychology* 83, 5 (2015), 890.

[54] John E Pachankis and Skyler D Jackson. 2023. A developmental model of the sexual minority closet: Structural sensitization, psychological adaptations, and post-closet growth. *Archives of Sexual Behavior* 52, 5 (2023), 1869–1895.

[55] John E Pachankis, Conor P Mahon, Skyler D Jackson, Benjamin K Fetzner, and Richard Bränström. 2020. Sexual orientation concealment and mental health: A conceptual and meta-analytic review. *Psychological Bulletin* 146, 10 (2020), 831.

[56] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball sampling. In *SAGE research methods foundations*. Sage, Thousand Oaks, CA, USA.

[57] Marc Eric S Reyes, Nickaella B Bautista, Gemaima Reign A Betos, Kirby Ivan S Martin, Sophia Therese N Sapio, Ma Criselda T Pacquing, and John Manuel R Kliatchko. 2023. In/out of the closet: Perceived social support and outness among LGB youth. *Sexuality & Culture* 27, 1 (2023), 290–309.

[58] Ellen DB Riggle, Sharon S Rostosky, Whitney W Black, and Danielle E Rosenkrantz. 2017. Outness, concealment, and authenticity: Associations with LGB individuals' psychological distress and well-being. *Psychology of Sexual Orientation and Gender Diversity* 4, 1 (2017), 54.

[59] Emma Roth. 2023. Online age verification is coming, and privacy is on the chopping block. https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety

[60] Shruti Sannon and Andrea Forte. 2022. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 455 (nov 2022), 33 pages. https://doi.org/10.1145/3555556

[61] Elissa L Sarno, Jonathan J Mohr, Skyler D Jackson, and Ruth E Fassinger. 2015. When identities collide: Conflicts in allegiances among LGB people of color. *Cultural Diversity and Ethnic Minority Psychology* 21, 4 (2015), 550.

[62] Eve Kosofsky Sedgwick. 2008. *Epistemology of the Closet.* Univ of California Press, Berkeley, CA, USA.

[63] Hannah Sparks and Samantha Ibrahim. 2022. Who is 'West Elm Caleb' and why do people on TikTok care about him? https://nypost.com/2022/01/21/who-is-west-elm-caleb-and-why-do-people-care-about-him/

[64] Katta Spiel, Oliver L. Haimson, and Danielle Lottridge. 2019. How to Do Better with Gender on Surveys: A Guide for HCI Researchers. *Interactions* 26, 4 (jun 2019), 62–65. https://doi.org/10.1145/3338283

[65] Jemimah Steinfeld. 2020. Forced out of the closet: As people live out more of their lives online right now, our report highlights how LGBTQ dating apps can put people's lives at risk. *Index on Censorship* 49, 2 (2020), 101–104. https://doi.org/10.1177/0306422020935360 arXiv:https://doi.org/10.1177/0306422020935360

[66] Alexandra Suppes, Jojanneke van der Toorn, and Christopher T. Begeny. 2021. Unhealthy closets, discriminatory dwellings: The mental health benefits and costs of being open about one's sexual minority status. *Social Science & Medicine* 285 (2021), 114286. https://doi.org/10.1016/j.socscimed.2021.114286

[67] Latanya Sweeney. 2000. Simple demographics often identify people uniquely. *Health (San Francisco)* 671, 2000 (2000), 1–34.

[68] Byron Tau and Georgia Wells. 2022. Grindr User Data Was Sold Through Ad Networks. https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800

[69] Samuel Hardman Taylor, Jevan Alexander Hutson, and Tyler Richard Alicea. 2017. Social Consequences of Grindr Use: Extending the Internet-Enhanced Self-Disclosure Hypothesis. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6645–6657. https://doi.org/10.1145/3025453.3025775

[70] Tinder. 2023. Block Contacts. Retrieved March 7th, 2023 from https://www.help.tinder.com/hc/en-us/articles/360039684672-Block-Contacts-

[71] Tinder. 2023. Boost. Retrieved May 30th, 2023 from https://www.help.tinder.com/hc/en-us/articles/115004506186-Boost

[72] Tinder. 2023. Super Like. Retrieved May 30th, 2023 from https://www.help.tinder.com/hc/en-us/articles/115004493543-Super-Like-

[73] Ari Ezra Waldman. 2019. Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities. *Law & Social Inquiry* 44, 4 (2019), 987–1018. https://doi.org/10.1017/lsi.2018.29

[74] Ari Ezra Waldman. 2019. Law, privacy, and online dating:"Revenge porn" in gay online communities. *Law & Social Inquiry* 44, 4 (2019), 987–1018.

[75] Ari Ezra Waldman. 2021. Navigating Privacy on Gay-Oriented Mobile Dating Applications. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, Bingley, United Kingdom, 369–381.

[76] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, USA, 2344–2360. https://doi.org/10.1109/SP46214.2022.9833643

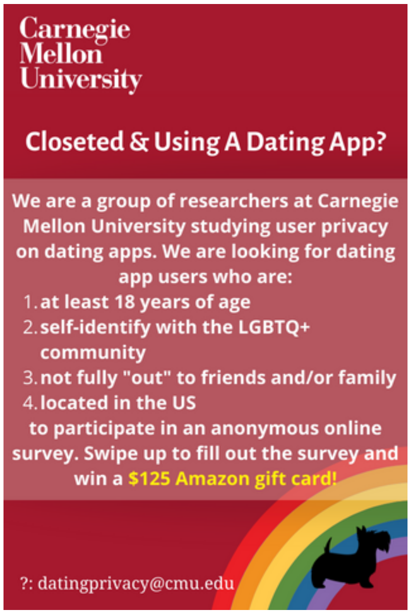
[77] Miranda Wei, Madison Stamos, Sophie Veys, Nathan Reitinger, Justin Goodman, Margot Herman, Dorota Filipczuk, Ben Weinshel, Michelle L. Mazurek, and Blase Ur. 2020. What Twitter Knows: Characterizing Ad Targeting Practices, User Perceptions, and Ad Explanations Through Users' Own Twitter Data. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Berkeley, CA, USA, 145–162. https://www.usenix.org/conference/usenixsecurity20/presentation/wei

[78] Zack Whittaker. 2020. A security flaw in Grindr let anyone easily hijack user accounts. https://techcrunch.com/2020/10/02/grindr-account-hijack-flaw/

[79] Kimberley Wilson, Katherine Kortes-Miller, and Arne Stinchcombe. 2018. Staying Out of the Closet: LGBT Older Adults' Hopes and Fears in Considering End-of-Life. *Canadian Journal on Aging* 37, 1 (2018), 22–31. https://doi.org/10.1017/S0714980817000514

[80] Janis Wolak, David Finkelhor, Wendy Walsh, and Leah Treitman. 2018. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health* 62, 1 (2018), 72–79.

A RECRUITMENT MATERIALS



Carnegie Mellon University

Closeted & Using A Dating App?

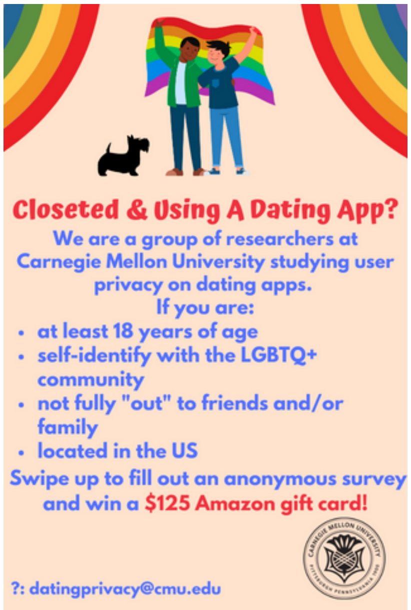
We are a group of researchers at Carnegie Mellon University studying user privacy on dating apps. We are looking for dating app users who are:

1. at least 18 years of age
2. self-identify with the LGBTQ+ community
3. not fully "out" to friends and/or family
4. located in the US

to participate in an anonymous online survey. Swipe up to fill out the survey and win a $125 Amazon gift card!

?: datingprivacy@cmu.edu

Figure 4: The first advertisement used to recruit participants on Grindr.



Closeted & Using A Dating App?

We are a group of researchers at Carnegie Mellon University studying user privacy on dating apps.

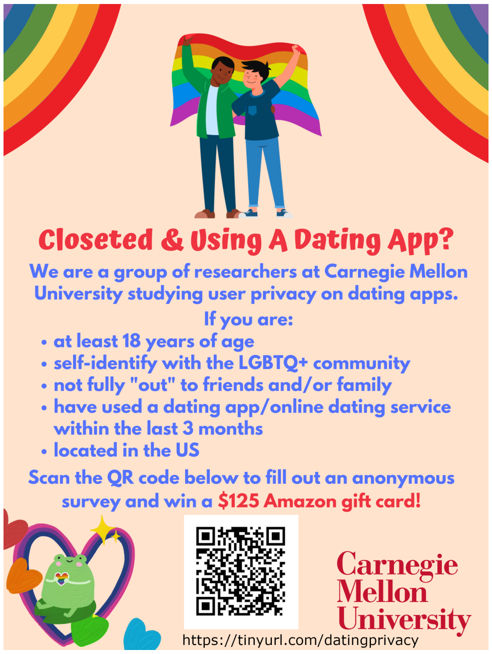
If you are:

- at least 18 years of age
- self-identify with the LGBTQ+ community
- not fully "out" to friends and/or family
- located in the US

Swipe up to fill out an anonymous survey and win a $125 Amazon gift card!

?: datingprivacy@cmu.edu

Figure 5: The second advertisement used to recruit participants on Grindr.



Closeted & Using A Dating App?

We are a group of researchers at Carnegie Mellon University studying user privacy on dating apps.

If you are:

- at least 18 years of age
- self-identify with the LGBTQ+ community
- not fully "out" to friends and/or family
- have used a dating app/online dating service within the last 3 months
- located in the US

Scan the QR code below to fill out an anonymous survey and win a $125 Amazon gift card!

Carnegie Mellon University

https://tinyurl.com/datingprivacy

Figure 6: The poster used for physical advertisements. This poster was also sent as a digital flier to LGBTQ+ oriented organisations at universities around the United States.

B SURVEY INSTRUMENT

The section headings were not visible to participants. Italicized text is used to indicate survey flow and response type. Answer choices are shown in bullets below each question. Answer responses with the text "please specify" or "please describe" included a free response box for participants' to explain their answer.

B.1 Demographics

Q1: How do you describe your gender identity?

- Male
- Female
- Non-binary
- Agender
- Genderqueer
- Prefer to self-describe (please specify)
- Prefer to not respond

Q2: How do you describe your sexual orientation?

- Homosexual
- Asexual
- Bisexual
- Pansexual
- Queer
- Prefer to self-describe (please specify)
- Prefer to not respond

Q3: Please select the age group you are in:

- 18-25
- 26-33
- 34-41

- 42-49
- 50-57
- Above 57
- Prefer to not respond

Q4: How do you describe your race or ethnic identity? (You may select more than one option.) *(participants can select multiple options)*

- White
- Black
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Prefer to self-describe (please specify)
- Prefer to not respond

Q5: What is the highest level of education you have completed?

- Less than high school degree
- High school graduate (high school diploma or equivalent including GED)
- Some college but no degree
- Associate degree in college (2-year)
- Bachelor's degree in college (4-year)
- Master's Degree
- Doctoral Degree
- Professional degree (JD, MD)
- Prefer not to respond

Q6: What is your annual household income?

- Less than $25,000
- $25,000 - $50,000
- $50,000 - $100,000
- $100,000 - $200,000
- More than $200,000
- Prefer not to respond

B.2 Outness Inventory Questionnaire

Q7: For each of the following statements, please select an option corresponding to how "out" you are with the people specified below. If you are more out with some people in a particular group than others, please provide the answer that applies to how out you are with the majority of people in that group.

- Mother
- Father
- Sibling(s)
- Extended family and relatives
- My old straight friends
- My new straight friends
- My work peers
- My work supervisors

For each statement, participants had the following options:

1. *Person definitely does not know about my sexual orientation status*
2. *Person might know about my sexual orientation status, but it is never talked about*
3. *Person probably knows about my sexual orientation status, but it is never talked about*
4. *Person probably knows about my sexual orientation status, but it is rarely talked about*
5. *Person definitely knows about my sexual orientation status, but it is rarely talked about*
6. *Person definitely knows about my sexual orientation status, and it is sometimes talked about*
7. *Person definitely knows about my sexual orientation status, and it is openly talked about*
8. *N/A*

B.3 Characterizing Use

Q8: Which of the following dating applications or online dating services have you used within the last 3 months (select all which apply)? *(participants can select multiple options)*

- Tinder
- Grindr
- Lex
- Bumble
- Hinge
- OkCupid
- Match.com
- eHarmony
- Other dating app/service not listed (please specify)

Q9: When was the first time you used a dating app or online dating service?

- In the last week
- In the last month
- In the last 3 months
- In the last 6 months
- In the last year
- In the last 2 years
- In the last 3 years
- More than 3 years ago

Q10: When was the last time you used a dating app or online dating service?

- Today
- In the last week
- In the two weeks
- In the last month
- In the last two months
- In the last three months

Q11: How often have you used dating apps or online dating services in the past 3 months?

- A few times a day
- Once a day
- A few times a week
- Once a week
- A few times a month
- Once a month
- Less than once a month

Q12: What is your primary purpose for using a dating app or online dating service?

- To meet new friends or acquaintances
- To have casual sex
- To find a romantic partner
- Other (please specify)
- No specific purpose/Unsure

B.4 Privacy Attitudes and Behaviors

Q13: What information do you include on your dating profile(s). Please select all that apply *(participants can select multiple options)*

- Full name
- First name only
- Nickname/Initials
- Age
- Sexual orientation
- Photos of self
- Gender
- Physical characteristics (e.g. height, weight, etc.)
- General location (e.g. the state or city you live in)
- Exact location (i.e. GPS or street address)
- Other (please specify)

Q14: Do any of the dating app(s)/service(s) you use require location permissions?

- Yes
- No
- Other (please specify)

Q15: Do you do anything to protect your privacy when using dating apps/online dating services?

- Yes
- No

Q16: How do you protect your privacy when using dating apps/online dating services? *(Free response field) Question displayed if answer to Q16 is "Yes"*

Q17: For each of the following statements, please select the option corresponding to how much you agree or disagree with the statement. *(Options for each statement: Strongly disagree, Disagree, Neither agree nor disagree, Agree, and Strongly agree)*

(1) I am truthful about my sexual orientation on my dating app profile.
(2) I trust that the information I share about myself on dating apps/online dating services will not be shared outside the app or service.
(3) I don't want people who I know in real life to see my profile on dating apps/online dating services.
(4) I am concerned that people who I haven't been "out" to in real life will see my sexual orientation on dating apps/online dating services.
(5) I find the paid features on dating apps/online dating services helpful.
(6) Paid features on dating apps/online dating services allow me to better protect my privacy.

Q18: For each of the following statements, please select the option corresponding to how much you agree or disagree with the statement. *(Options for each statement: Strongly disagree, Disagree, Neither agree nor disagree, Agree, and Strongly agree)*

(1) I feel comfortable sharing photos of myself with others in direct messages on dating apps/online dating services.
(2) I feel comfortable with someone sharing images of my dating profile to their friends or family.
(3) I feel comfortable with someone sharing images of conversations I had on dating apps/online dating services.
(4) I am fine with non-dating websites purchasing anonymous information from the dating apps/online dating services I use.
(5) I am fine with my dating profile being used to personalize advertisements.

Q19: For each of the following statements, please select the option corresponding to how much you agree or disagree with the statement. *(Options for each statement: Strongly disagree, Disagree, Neither agree nor disagree, Agree, and Strongly agree)*

(1) I limit the amount of information I put on my dating app profiles.
(2) I have displayed/shared my social media accounts to my profile on dating apps/online dating services.
(3) I lie about information on my dating profile(s) to protect my privacy.
(4) I have taken screenshots of images I saw or messages people sent me on dating apps/online dating services.
(5) I have shown other people's dating profiles to my friends or family.

Q20: For each of the following statements, please select the option corresponding to how much you agree or disagree with the statement. *(Options for each statement: Strongly disagree, Disagree, Neither agree nor disagree, Agree, and Strongly agree)*

- I have shown conversations I had on dating apps/online dating services to other people.
- Before I go on a date with someone I met on dating apps/online dating services, I usually look them up on the internet.
- I have paid to access additional features on dating apps/online dating services.
- People have sent me unsolicited intimate photos on dating apps/online dating services.
- I have found profiles of people who I know in real life on dating apps/online dating services.

Q21: Now that you have thought more about privacy issues on dating apps/online dating services, does anything come to mind that you have done to protect your privacy? *(Free response field)*

B.5 Improving User Experience

Q22: Has your privacy been violated while using a dating app/online dating service? If so, what happened? *(Free response field)*

Q23: Has someone threatened you on a dating app/service? If so, please describe what they threatened and what happened as a result. *(Free response field)*

Q24: Which features(s) do you think could be changed or added to better protect your privacy on dating apps/online dating services? Please reference the dating app or the online dating service you use in your answer. *(Free response field)*

B.6 Conclusion

Q25:Thank you for completing our survey. You will have the opportunity to enter the giveaway for an $125 Amazon gift card on the final screen, once you click "Submit." If you are interested in participating in a followup interview, for which you will be compensated $15 for 30 minutes of time, please select the appropriate checkbox below and enter your email address. Otherwise, select "No, I am not interested in participating in a follow-up interview" and proceed to the final screen.

- Yes, I am interested in participating in a follow-up interview, either by email exchange or Zoom, for a $15 Amazon gift card *(Free response field)*
- No, I am not interested in participating in a follow-up interview

C CODE BOOKS

The following subsections list the codes derived from inductive analysis of participants free response answers. Each code is accompanied by a definition, the frequency of use, and an example quote. For the privacy protecting behavior codes, the frequency is the sum of unprimed and primed instances of the code. If a participant gave the same answer both primed and unprimed, this was only counted as a single instance of the code.

C.1 Privacy Protecting Behaviors (Q16, Q21)

- **No response/irrelevant**: Participant does not have an answer or provides an answer that is irrelevant to the question. Almost exclusively applies to Q22 49 instances. (*"Nothing more than I initially stated."*)
- **No full name**: Participant indicates that they do not include their full name in their profile. This includes use of first name or initials only. 45 instances. (*"Not using my real name..."*)
- **No exact location** : Participant indicates that they do not share their exact location or address on the dating platform. 27 instances. (*"I do not give my exact location"*)
- **General information restriction**: Participant indicates that they limit the information they share on dating profile, but do not provide specifics. 25 instances. (*"...don't disclose too much personal info."*)
- **Other**: Participant protects their privacy in a way which is not specified by another code. 23 instances. (*"only meet people once we verify each other on social media."*)
- **No face photos**: Participant indicates that they do not include their face in pictures they publicly share. 17 instances. (*"Don't show full face photos"*)
- **Screen people**: Participant indicates that they interact with individuals, ask for information or otherwise "screen" people prior to sharing information. 16 instances. (*"...Asking for pictures before feeling comfortable to share..."*)
- **Restrict photos**: Participant indicates that they restrict or edit the type of photos they share on their profile in a non-specified way. Also includes specific photo restrictions that are not encompassed by the other codes. 14 instances. (*"No face photos with genitals..."*)
- **No social media**: Participant indicates that they do not link non-dating social media services to their dating profile. 12 instances. (*"...I don't link any of my social media platforms to the dating app"*)
- **No photos**: Participant indicates that they do not share any photos on their dating profile. 8 instances. (*"I not post my pics..."*)
- **No occupation/educational institution**: Participant indicates that they dod not share their occupation or educational institution on their dating profile. 7 instances. (*"Don't reveal my occupation"*)
- **Throwaway accounts**: Participant indicates that they use "throwaway" email addresses, phone numbers, social media accounts, etc. In other words, they create accounts disconnected from their identity to interact on dating applications. 6 instances. (*"...use a basic email that doesn't link directly to me"*)
- **No contact information** : Participant indicates that they do not share contact information such as phone number or email address. 4 instances. (*"By not giving out my.... phone number"*)
- **Purchase premium features**: Participant states that they paid for the application or purchased additional features in order to protect their privacy. 4 instances. (*"the upgraded tinder version allows me to put my location to anywhere so people in my hometown cannot see me"*)
- **VPN**: Participant indicates that they use a VPN when using a dating application. 3 instances. (*"VPN"*)
- **Avoid using public photos**: Participant indicates that they do not share pictures that they have publicly shared elsewhere online. 2 instances. (*"On one app I do not have a publicly available photo"*)
- **No tattoos**: Participant indicates that they avoid sharing photos that show their tattoos. 2 instances. (*"...I have tattoos and have photoshopped all of them out of my pictures..."*)

C.2 Privacy Violations (Q22)

- **No**: Participant indicates that their privacy has not been violated while using a dating service or app. 74 instances. (*"n/a"*)
- **Unauthorized sharing of use of dating application/service**: Participant indicates that someone shared that they use a dating application with others. This is specifically when sharing is done without criminal intent. 7 instances. (*"Other than talking about me to their friends, no"*)
- **Unauthorized sharing of photos**: Participant indicates that someone shared photos of the participant without their consent. May be paired with "unatuthorized screenshot/downloading of photos" but also includes the sharing of photos which were voluntarily sent. 7 instances. (*"My photos have been shared with others..."*)
- **Unauthorized screenshot/downloading of photos**: Participant indicates that someone took screenshots or saved their photos/videos/profile/messages without permission. 5 instances. (*"Yes. Someone sharing photos and conversations to a person who then Messaged me telling me what had happened"*)
- **Extortion**: Participant indicates that someone attempted to extort them. They may specify that they were extorted with

the threat of outing them or sharing explicit photos. 5 instances. (*"Attempted blackmail with photos of me, threatening to send to friends/family. I don't care very much though I just block them."*)

- **Other**: Participant describes a situation not covered by other codes. 4 instances. (*"It wasn't anyone's fault but my own but I screenshot my profile to send to my friend and the screenshot got put into a shared Google photos album I have with my mom because of facial recognition"*)
- **Harassment**: Participant describe digital or physical harassment. 4 instances. (*"stalker tried to message me across many accounts and somehow figured out the general area i live in, continually objectifying me and pleading me for favors until i threatened to contact law enforcement"*)
- **Context collapse**: Participant encountered someone who does not know about their LGBTQ+ identity while using a dating application. 4 instances. (*"A coworker approached me after finding one of my dating profiles and publicly asked questions about it."*)
- **Threatened with outing**: Participant incates that someone threatened to out them, but does not mention extortion or a financial motive. 3 instances. (*"Threatened to be outed/doxxed at work"*)
- **Unspecified**: Participant states that their privacy has been violated but does not explain what happened. 2 instances. (*"Yes and it caused significant stress in my personal life"*)
- **Impersonation**: Participant indicates that someone reused their photos or otherwise tried to impersonate the participant. 2 instances. (*"People represented my intimate pics as their own"*)

C.3 Features to Improve Privacy (Q24)

- **No answer**: Participant does not have a suggestion for another feature or says something incomprehensible. 33 instances. (*"Nothing I can think of right now."*)
- **Profile visibility controls**: Participant would like the ability to more precisely control who can view their profile. 14 instances. (*"For all services, only users with an active account can see your profile, so they can't be seen by the public"*)
- **Disable/limit screenshots or saving photos**: Participant would like the ability to prevent or limit the ability of others to take screenshots or save photos. 13 instances. (*""No screenshots.""*)
- **Other relevant**: Participant makes suggestion that does not fit with other codes, but does actually answer the question. 11 instances. (*"A safety feature would be nice."*)
- **Make paid features free**: Participant would like some or all of the paid features to be available for free. This code is sometimes accompanied by another code specifying the feature they would like to be made free. 11 instances. (*"Non-paid privacy options"*)
- **Other irrelevant**: Participant makes suggestion that does not fit with other codes and does not actually answer the question. 8 instances. (*"Tinder could add better features related to connecting people better"*)
- **Disable/limit exact location**: Participant would like the ability to disable or limit the ability to view exact location. 8 instances. (*"Maybe it can support the feature of disabling GPS"*)
- **User verification**: participant would like the dating service/application to verify the identity of users in someway. 7 instances. (*"Tinder requires a verification process, whereas Grindr does not. Grindr should take note"*)
- **Describes feature they like**: Participant describes a feature they like or used to protect their privacy. Always paired with another code corresponding to the feature type. 6 instances. (*"Actually, I turned off the tinder search when I was back at my college, so people wouldn't find me."*)
- **Improve blocking**: Participant specifies that they would like the platform to improve the ability to block people. 5 instances. (*"A block feature that actually works"*)
- **Disable/limit the sales of information**: Participant would like the dating service to limit or entirely stop sharing data with other companies. 4 instances. (*"Not have info sold to companies as a means to show personal ads"*)
- **Improve other existing feature**: Participant specifies an existing feature they would like to improve, other than blocking. 3 instances. (*"Better password locking for Scruff."*)
- **Improved privacy education**: Participant would like the dating service/application to improve the app's privacy education or otherwise make privacy features more visible to users. 3 instances. (*"...maybe a quick tutorial before you add photos to remind you to be careful of adding photos with identifiable info or ones that could be easily imaged searched on google"*)
- **Unsend messages**: Participant would like the ability to delete messages after they have been sent (*"Allow me to unsend messages..."*)
- **Better moderation**: Participant would like to have better moderation of users on the platform. 2 instances. (*"They need to definitely research when profiles are reported for various reasons"*)

D OUTNESS INVENTORY CORRELATIONS

Table 2: Spearman's rank order correlation (ρ) between the average OI score and each of the Likert scale questions. * indicates a weak correlation (absolute values between 0.2 and 0.4), ** indicates a moderate correlation (absolute values between 0.4 and 0.7)

	ρ	% Agree	% Disagree	p-value
Q17.1	$.260^*$	82.5%	10.5%	.005
Q17.2	.029	40.4%	30.7%	.760
Q17.3	$-.449^{**}$	71.1%	10.5%	$< .001$
Q17.4	$-.385^*$	55.3%	28.9%	$< .001$
Q17.5	$-.023$	19.3%	53.5%	.811
Q17.6	$-.018$	18.4%	41.2%	.849
Q18.1	$.229^*$	67.5%	16.7%	.0144
Q18.2	$.260^*$	18.4%	71.9%	.005
Q18.3	$.278^*$	11.4%	79.8%	.003
Q18.4	.029	7.0%	79.8%	.759
Q18.5	.169	8.8%	79.8%	.073
Q19.1	$-.137$	84.2%	5.3%	.145
Q19.2	$.307^*$	27.2%	69.3%	$< .001$
Q19.3	$-.272^*$	26.3%	54.4%	.003
Q19.4	.195	54.4%	36.0%	.038
Q19.5	$.272^*$	43.0%	50.9%	.003
Q20.1	$.316^*$	50%	42.1%	$< .001$
Q20.2	.190	56.1%	28.1%	.043
Q20.3	$-.160$	27.2%	68.4%	.089
Q20.4	$-.082$	73.7%	22.8%	.387
Q20.5	.187	87.7%	7.9%	.047

E INTERVIEW PARTICIPANTS

Table 3: List of interview participants and their gender and sexual orientation.

Participant ID	Age	Gender	Sexual Orientation
S11	26 to 33	Non-binary	Queer
S25	18 to 25	Man	Homosexual
S33	18 to 25	Woman	Pansexual
S66	34 to 41	Man	Homosexual
S73	18 to 25	Woman	Homosexual
S74	18 to 25	Woman	Pansexual
S102	18 to 25	Non-binary	Queer
S106	18 to 25	Woman	Bisexual
S111	18 to 25	Non-binary	Pansexual

F INTERVIEW GUIDE

The following text was used by interviewers to guide the interview procedure. The example questions were not in the original interview guide, but are included to illustrate our interview approach.

F.1 Introduction

Introduce yourself and study: "Good afternoon! Thank you for coming and participating in our interview study. I am… from Carnegie Mellon University. Today we're going to be asking you some questions about your experiences on dating services." Remind the participant of consent, confidentiality, and opt-out: "When taking our survey you signed a consent form. As stated in the consent form, what you say to us during the interview will be kept confidential. You can decline to answer any questions or you can stop participating at any time, while still receiving compensation." Ask "Do you consent to this interview being recorded for our internal use?" Once the participant confirms, begin the recording and ask them again to confirm that they have seen the consent form and consent to being recorded.

F.2 Interview

Ask questions based on the participant's survey responses. Prepare questions prior to the interview. Feel empowered to add new follow up questions as relevant. Examples:

- "Is there any particular reason you use hinge over other dating apps?" (from interview with S33)
- "In the survey you say that you use dating apps in order to connect... with people in general, but not looking for another relationship in particular. Could you explain more about why you use dating apps for this purpose rather than other social media applications?" (from interview with S25)
- "On the survey... you mentioned that people have taken screenshot photos without your permission. Can you describe an incident where this happened?" (from interview with S66)

- “On the survey you stated... that you’re cautious about who you give pictures of yourself to. Could you explain how you decide who you want to share photos with?” (from interview with S74)

F.3 Conclusion

When all the questions are complete or 30 minutes have elapsed, conclude the interview. End the recording of the interview. Thank the participants for their time. Check if the participant has any questions before ending the Zoom meeting. Remind them: “We will send you an Amazon gift card code through email over the next week, if you have trouble or do not receive payment please contact us and we will solve the issue. You can use the email of the principal investigator included in the consent form.”