Swipe Left for Identity Theft:
An Analysis of User Data Privacy Risks on Location-based Dating Apps

Karel Dhondt Victor Le Pochat Yana Dimova Wouter Joosen Stijn Volckaert
DistriNet, KU Leuven

Abstract

Location-based dating (LBD) apps enable users to meet new people nearby and online by browsing others' profiles, which often contain very personal and sensitive data. We systematically analyze 15 LBD apps on the prevalence of privacy risks that can result in abuse by adversarial users who want to stalk, harass, or harm others. Through a systematic manual analysis of these apps, we assess which personal and sensitive data is shared with other users, both as (intended) data exposure and as inadvertent yet powerful leaks in API traffic that is otherwise hidden from a user, violating their mental model of what they share on LBD apps. We also show that 6 apps allow for pinpointing a victim's exact location, enabling physical threats to users' personal safety. All these data exposures and leaks – supported by easy account creation – enable targeted or large-scale, long-term, and stealthy profiling and tracking of LBD app users. While privacy policies acknowledge personal data processing, and a tension exists between app functionality and user privacy, significant data privacy risks remain. We recommend user control, data minimization, and API hardening as countermeasures to protect users' privacy.

1 Introduction

Location-based dating (LBD) apps enable users to meet new people nearby and online, for relationships, casual encounters, or friendships. Since the launch of Grindr in 2009 and Tinder in 2012, these apps have become increasingly popular: for example, Match Group's app portfolio sees nearly 100 million monthly active users [75].

Users of these apps reveal highly personal and sensitive information in their profiles, making them susceptible to violations of their social privacy by other individuals [53, 54, 114]. Additionally, these LBD apps are unique in that users share this data with people they might not (yet) know, as opposed to other social networks where data sharing usually entails a prior social connection [48]. Adversaries in this scenario are focused on extracting personal information, including location data, of one or more LBD app users. They achieve this through normal interaction with the platform, regardless of whether the target is a prior acquaintance or an individual they encounter for the first time on the app. The adversary's malicious intentions can span a broad range. For example, they may want to gather identifying information, such as name, age, and photo, to engage in social engineering or steal a user's identity [30]. As another example, the adversary may want to learn a user's sexual orientation, to extort [90] or even prosecute them [17, 119]. Last but not least, sharing one's location is crucial to these apps, as users are shown profiles of people in their vicinity. However, the adversary can use that location to physically stalk people [30], and in extreme cases, carry out assaults and murder of LBD app users [106]. Given these potentially severe risks to a person's virtual and physical safety, and genuine user concerns about those risks [81], LBD apps must carefully protect users' personal data, in particular preventing any (inadvertent) leaks.

In this paper, we systematically analyze 15 popular LBD apps with at least 10 million downloads on the extent to which they cause privacy risks stemming from the sharing of personal and sensitive data with other users. We develop our evaluation in three steps. First, we analyze how easily the adversary can create an account on LBD apps to stealthily gather private user data. Then, we measure which personal data is shared by these apps, including sensitive attributes, dating-sensitive data, and users' exact locations. Finally, we examine how the privacy policies of these apps discuss the collection and potential leaking of personal data.

In our privacy risk analysis, we consider two types of data sharing. *Intended* sharing is known to an LBD app user, as the shared data is shown in the user interface (UI). Through our systematic manual traversal of each app's functionality, we find that LBD apps *expose* large amounts of *personal data* to other users, enabling the extraction of (sensitive) personal traits, including by our least sophisticated adversary who only uses the app's UI. Most apps *require* sharing identifying information such as name and age with others. Equally, the UI often displays legally protected *sensitive data* [115] such as ethnicity or sexual orientation.

Inadvertent sharing concerns data that is hidden in the UI but that the adversary can still retrieve, which stands in direct conflict with the user's perception of what they are sharing and what others can therefore learn about them, representing the most severe violations of the user's privacy expectations. We simultaneously examine the API traffic between the LBD app and its server, discovering several APIs that *leak* (sometimes explicitly hidden) personal data to an attacker who has capabilities to inspect or even modify traffic – or is aided by others or easy-to-use tools. API leaks are particularly prevalent for *app usage data related to the dating process*, which may cause particular embarrassment or stigma, e.g., by revealing another user's likes or preferences, or allow for fine-grained monitoring, e.g., by leaking the last activity time. Given its sensitivity, we extensively evaluate whether apps – again, unknowingly to users – allow extracting a user's exact location by being susceptible to one of three forms of trilateration. We find that 6 apps that do so, despite proven countermeasures that prevent such an attack, such as grid snapping on Tinder.

Together with the ability to retrieve multiple profiles at once, permanently request one user's profile at any time, and easily create accounts, all these data exposures and leaks enable targeted or large-scale, long-term, and stealthy profiling and tracking of LBD app users. While the privacy policies of these apps tend to be compliant with data protection law by outlining which data they process, and some even acknowledge the potential for leaks (including locations), they mostly place the burden of protecting privacy and cautious data sharing on the users themselves, with only some apps providing actionable privacy controls. To help users in preserving their privacy in light of our findings, our recommendations for countermeasures focus on two aspects. First, given the tension between app functionality and user privacy, where users may feel compelled to share data, and services nudge them to do so, LBD app users should gain more control over what they share and with whom. Apps could consider reducing data gathering, to improve user privacy regarding intended sharing. Second, given inadvertent sharing of potentially sensitive data, LBD apps should prevent data leaks by hardening APIs. After our analysis in January 2023, we disclosed our findings to all affected apps, leading to concrete fixes of our discovered leaks, therefore improving users' privacy and reducing the potential threats associated with using LBD apps.

In summary, our main contributions are:

- We conduct a systematic and broad privacy analysis of user data risks on 15 popular LBD apps, including how these risks are enabled by easy account creation and acknowledged by privacy policies.
- We find that the apps' UI exposes large amounts of personal and sensitive data to even unsophisticated adversaries.
- Particularly powerful API traffic leaks reveal very sensitive data that is otherwise hidden from users, violating their expectations of what they share with others.
- For 6 apps, these leaks include a user's exact location, enabling physical threats to personal safety.
- We propose countermeasures to better protect users' personal data and locations, and responsibly disclosed our discovered vulnerabilities to the LBD app vendors.

2 Background

2.1 Location-based Dating Apps

Location-based dating (LBD) apps [13, 58] are social matching systems [137] that recommend people to each other, usually based on their personal traits and preferences. These apps fall into the class of location-based social networks [26, 77, 159], location proximity services [103], or people-nearby applications [140, 143]. They tend to be accessed on mobile (although some services have web apps), and usually use the phone's GPS to determine the user's exact location and then show (only) other users in close proximity. While these apps are commonly referred to as 'dating apps', they allow users to search for and engage in a variety of interpersonal relationships, including long-term romantic relationships, casual sexual encounters, platonic friendships, or business networking. The motives for using these apps further extend to, a.o., entertainment, curiosity, social approval, and a sense of community [139, 143]. These apps differ from most (location-based) social networks, as LBD apps do not require a prior social connection to see another user's information – i.e., other users can be strangers –, whereas social networks usually only share such information with connected users [103].

Most LBD apps work as follows. A user registers with the platform and completes their profile, listing their own traits such as age, gender, or interests, and generally uploading one or more photos. They also set filters for the traits of others, such as maximum distance, gender, or age range. The app then displays other users' profiles, which often list their location or distance, with two possible ways of browsing profiles. In the *card stack* model, the app generates a queue of other users that fit the desired criteria. It then shows these users one by one as cards on a stack. The user indicates whether they (dis)like the currently shown other user (colloquially: "swiping"), requiring a decision before being able to move on to the next user. If the user likes another user, nothing happens until (and unless) that other user reciprocates the like, in which case the two users "match" and can start messaging each other through the app. In the *grid* model, the app shows all nearby other users at once, allowing the user to select and view profiles at their leisure. The user can usually immediately start a conversation with any user, without the need to explicitly match beforehand. Apps can offer both modes. Apps usually operate on a 'freemium' basis, with a paid subscription or individual purchases giving access to more features, some of which are privacy-related, such as hiding age or distance.

Table 1: Selected LBD apps, as of January 2023.
Legend: # DL: number of downloads on Google Play Store; C/G: Card stack/grid; W/M: Website/mobile app.

Name	# DL	C	G	W	M
Tinder	100M	✓		✓	✓
Badoo	100M	✓	✓	✓	✓
POF	50M	✓	✓	✓	✓
MeetMe	50M	✓	✓	✓	✓
Tagged	50M	✓	✓	✓	✓
Grindr	50M		✓		✓
Tantan	50M	✓			✓
Jaumo	50M	✓			✓
LOVOO	50M	✓	✓	✓	✓
happn	10M	✓		✓	✓
Bumble	10M	✓		✓	✓
Hinge	10M	✓	✓		✓
Hily	10M	✓			✓
OkCupid	10M	✓		✓	✓
Meetic	10M	✓	✓	✓	✓

2.2 Related Work

Location-based social networks, such as LBD apps, have long been shown to be vulnerable to inference attacks that reveal users' current or sensitive locations (e.g., a home). Early works treated the topic more theoretically and formally [26, 73, 87, 122, 123, 149, 159], mainly using simulated behavior to prove location leaks. Later on, location inference through trilateration was shown to be possible on various real-world services [77, 103, 157, 158]. Other forms of location inference were also shown to be feasible, such as triangulation [148], trace fitting [60, 89], probabilistic heuristics [33, 72], clustering [37], or machine learning [154]. In Section 5.5, we assess whether previously discovered vulnerabilities to location inference attacks specific to LBD apps are still present.

Outside our threat model, LBD apps may persist personal data on a user's device, which may become a (surveillance) privacy risk when that data is retrieved from that device in a forensic investigation. Several works analyzed these forensic artifacts that LBD apps leave behind, focusing on, a.o., Tinder [39, 61, 68], happn [69], Bumble [11, 61], Grindr [39, 61], and other popular dating apps [20, 39, 68, 88]. An adversary that can intercept a victim's network traffic can also gather sensitive data sent and received by LBD apps [100, 120]. LBD apps may also share personal data with third parties, as was shown on, a.o., Tinder [18, 27, 61, 98, 153], Grindr [61, 65, 153], happn [18, 98], Bumble [61], and OkCupid [27, 98, 153]. Social engineering through conversations can also be used to elicit personal data from LBD app users [92].

To the best of our knowledge, our work is the first extensive privacy analysis across a large number of LBD apps. The closest works on the topic of data exposure in LBD apps treated either only 5 LBD apps in 2015 across 7 attributes [110], or only 3 LBD apps in 2019 with very limited coverage of exposure to other users [153]. Cobb et al. [29] covered, a.o., 8 LBD apps in their analysis of online status indicators. Location leaks through trilateration on LBD apps have been described in various works over the past decade [22, 34, 65, 103, 111], but none systematically evaluated the issue across a similarly large set of highly popular LBD apps as ours (15 apps with over 10 million downloads each). Analyses of LBD app privacy policies focused on third-party data sharing [18, 61], while we assess their description of sharing with other users. Our work also integrates these privacy dimensions – data exposure, (location) leaks, privacy policy analysis – to comprehensively examine these apps' privacy posture, situating itself in the space of cross-dimensional privacy analyses for specific app ecosystems [42, 57, 99]. Finally, our work expands and updates the state-of-the-art knowledge, providing crucial insights into the manner in which these LBD apps continue to handle users' personal and sensitive data.

3 Scope and Motivation

3.1 LBD Apps Selection

For our analysis, we select the most popular LBD apps, based on their download count in the Google Play Store. Through an initial exploration, we observe that LBD apps are primarily listed under the *Dating*, *Lifestyle*, and *Social* categories. We crawl metadata, descriptions, and the ranking for all apps in these three categories in four countries[1] that are leading markets for LBD apps [2], through an internal Play Store API [5]. We filter on dating-related apps in the *Lifestyle* and *Social* categories by searching the keyword 'dating' in the name or description. We then manually review the top apps on whether they provide location-based dating. For our in-depth analysis, we retain all apps with more than 50 million downloads as well as those in the *Dating* category with more than 10 million downloads and a top 10 rank in at least one country, if they fit our definition of an LBD app and appear to be genuine; we omit two apps for the latter reason.[2] Table 1 lists the final selection. Our analysis reflects the most recent versions of these apps as of January 2023 (Appendix A). We only analyze dating-related modes, i.e., not other modes such as *Bumble BFF* for finding friends. Almost all apps cater to a general audience; Tantan targets an Asian or Asian American audience, and Grindr targets LGBTQ users.

3.2 Threat Model and Analysis Scope

Our goal is to analyze which private information the adversary can obtain about another person who uses an LBD app. This differs from models where the adversary is the platform itself or an affiliated third party (e.g., improperly storing or forwarding private data) [18, 91, 98], an intermediate party on the network (intercepting the traffic containing private data) [8, 100, 120], or an outsider exploiting platform vulnerabilities (e.g., breaching databases or stealing credentials to retrieve private data) [16, 32, 86]. As such, we primarily study

[1] France, Germany, United Kingdom, United States.

[2] Despite their apparent popularity, we omit *iHappy* and *SweetMeet*, both operated by FlintCast, as they appear to contain mostly fake profiles with a gift-giving monetization model, appear to have fake positive app store reviews, and otherwise have no mainstream online recognition.

breaches of *social* privacy, i.e., towards other individuals, instead of *institutional* or *surveillance* privacy, i.e., towards service providers, governments, etc. [54, 114]. The adversary uses only the information that a regular user can retrieve through client-side interactions with the service, and as such cannot use any other means to retrieve the information, e.g., infiltrating the platform's servers or escalating the privilege of their account. The malicious intentions of the adversary can be diverse and can relate to both virtual and physical privacy and safety [30]: using personal data for social engineering or identity theft [21, 30, 35, 48, 117], stalking or harassing a person online or physically [21, 30, 38, 48, 109], monitoring their partner [25], searching real-life acquaintances [28, 30, 139], up to nation-state surveillance and prosecution of at-risk populations [17, 90, 119] or physical violence [106].

We assume an adversary can access both the web and mobile app when both exist, since some data may be exclusive to either one. We consider three levels of technical sophistication for the adversary, with the required abilities affecting the extent to which they can gather personal data:

1. The least sophisticated adversary only observes personal data that is readily visible in the (web or mobile) *user interface*. This adversary type has been called a "no-tech hacker" [80] or "UI-bound adversary" [46]. This adversary requires no special technical skills, i.e., *everyone* could fit this adversary model.
2. A more technically sophisticated adversary *inspects the network traffic* to discover additional data. For web apps, this is easily achieved using browser developer tools, regardless of whether traffic is TLS-encrypted. For mobile-only apps, the adversary will need to capture (possibly TLS-encrypted) mobile web requests, which may require circumventing measures such as certificate pinning [108].
3. The most technically sophisticated adversary *modifies and injects network traffic*, which requires reverse engineering the app's API and circumventing integrity checks, e.g., in the form of message signatures.

Our own analysis proves that, even despite the mentioned protection mechanisms, these adversary models are nearly always feasible for the apps in our scope, as we could inspect and modify network traffic for both web and mobile apps.[3] Moreover, adversaries who are less technically skilled themselves could receive support or use existing tools for inspecting and/or modifying traffic and thereby extract hidden private data from LBD apps. This model has been shown to exist in practice. In the context of intimate partner surveillance, which is a potential motivation for our adversary, discussions where users share tools and tactics to collaborate on technically sophisticated attacks have been observed on online infidelity forums [141] and TikTok [152]. (Proof-of-concept) apps previously executed trilateration for Tinder [144] and Grindr [94] users, while a browser extension displayed additional features hidden in OkCupid's API [67], all through an easy interface without requiring technical skills.

The adversary can target either one specific user or the entire (local) service user base for mass data collection [21, 117]. We assume that the adversary can discover a victim's profile, but not that they match. In case the adversary has a specific target, this may require (roughly) knowing where the target is located, such that the adversary can put themselves sufficiently close to see the target's profile. This is not an unreasonable assumption: stalkers and their victims usually know each other [126], and people often share their current city online [24]. Given the ability to spoof the location data sent to a service, the adversary does not need to be physically near the target(s).

We assume that the adversary is able to create one or more profiles on the service. In Section 4, we determine whether services verify that a user is real, and see that services may require a working phone number or a verified photo, but overall, the account requirement is not a high barrier for an adversary. In order to parallelize requests and speed up data gathering, the adversary may opt to create and deploy multiple Sybil accounts [145, 156], but only one account is required as a strict minimum for our attacks to work. The adversary sets up a minimally complete profile, to be maximally stealthy. This allows them to collect data while the target is not aware that they are being observed. Our victim can fill in their profile entirely, but will configure it to be as privacy-conscious as possible, i.e., hiding data whenever allowed by the service. We assume both our adversary and victim to use a free account, though we note that premium services often include additional privacy features, such as hiding additional fields.

3.3 Ethical Considerations

As we will show, users share very sensitive and personal data on dating apps. We therefore design our experiments to be as ethical and privacy-conscious as is feasible, while still allowing for executing our study. We abide by ethical standards that are established in our community, focused on providing maximal benefits while minimizing harm [10, 56, 85]. Our study was approved by our university's privacy and ethics board. Due to the lack of meaningful interactions with or data collection on real users, our study was not considered to be human subjects research.

For each service, we set up at least two fresh profiles,[4] using dedicated email addresses and phone numbers. After these profiles discover each other, we collect their metadata and possibly have them interact (e.g., like each other) to gather additional data. We do not gather or analyze any data on real

[3] Only for two apps (Tantan and Jaumo), we were unable to reverse-engineer the message signature with reasonable effort (i.e., without extensive disassembly), preventing the analysis of exfiltration leaks.

[4] We sometimes need more than two accounts, to validate all possible interactions, e.g., (dis)likes or colluding accounts, or when profiles are taken down between initial account creation and the final exploration, possibly because of us disclosing our research purpose.

Table 2: Overview of account creation requirements.
Legend: ● Required, ◐ Optional, ○ Not available.

	Tinder	Badoo	POF	MeetMe	Tagged	Grindr	Tantan	Jaumo	LOVOO	happn	Bumble	Hinge	Hily	OkCupid	Meetic
Email address	●	◐	●	●	●	●	○	◐	●	●	○	●	●	●	●
Phone number	●	◐	●	○	○	●	●	○	○	●	●	●	◐	●	○
Real data (ToS)	○	○	●	●	○	○	○	●	●	○	●	●	●	●	○
Photo	●	●	●	○	○	○	●	●	●	●	●	●	●	●	●
Face photo	○	●	●	○	○	○	●	●	●	●	●	●	●	●	●
Face verification	◐	◐	◐	◐	○	○	◐	◐	◐	◐	●	◐	◐	◐	◐

users and do not meaningfully engage with them. We disclose our academic research purposes on the profile picture and/or in the biography, and request to ignore the profile to discourage users from interacting with us. The only interaction we possibly have with real users is to dislike their profile in order to continue onto our self-made profiles. This also means we do not deploy meaningful deception towards the services or their users. While our fake accounts might violate the services' Terms of Service, we believe that this is warranted as our research is in the public interest and its benefits for user privacy and safety outweigh the potential minimal harm to the platforms or their users [104]. We responsibly disclosed our findings to the services that we study and worked with them to resolve their issues (Section 7.3).

3.4 Limitations

Our scope definition and ethical protocol limit which privacy breaches we (can) analyze. We do not analyze whether (free-form text) self-descriptive biographies or photos contain any personal data [96], nor do we attempt to understand whether profile data can be used to cross-reference users between services or with other social media platforms [22, 71, 130], in particular as this would entail collecting real user data.

We cannot be certain that our analysis or reverse engineering process fully uncovers all data leaks, e.g., if we miss an API endpoint through which such a leak would occur. In addition, we analyze apps in a European Union country, where the General Data Protection Regulation (GDPR) is in force, which may affect the extent of private data collection and exposure by apps. Our findings may therefore not fully reflect the data leaks that happen in other jurisdictions.

4 Account Creation Security

We first assess **how easy it is for an adversary to create a (fake) account** to browse profiles on an LBD app. Sufficient protections and requirements for account creation can *expose* the adversary to other users, and therefore reduce the adversary's ability to easily and stealthily gather private user data. We consider two types of undesirable exposure: the adversary may want to remain *anonymous* and limit the information held by the platform (institutional privacy), e.g., to avoid that platforms can share this with law enforcement agencies when actions may be prosecutable (e.g., stalking); and they may want to remain *hidden* from other users (social privacy) to avoid awareness that they are present on the platform. In this section, we analyze the account creation requirements from the *adversary*'s perspective, seeing them as *security measures*. Evidently, these requirements also cause friction for *legitimate users*, as they impose personal data sharing; in the next section, we therefore approach them as *privacy risks*. Table 2 lists our detailed analysis of account creation security across the 15 LBD apps in our scope.

All services require an email address, except Tantan and Bumble which do not support email login, Badoo which requires either an email address or a phone number, and Jaumo which only requires an email address once a user wants to log out (to create a persistent account identifier to log in again). An email address is easy to acquire (anonymously), yet for 7 services it is a sufficient identifier to create an account, access the service, and view other user profiles. The other 8 services require a valid phone number, which will be verified through an SMS One-Time Password [83]. Phone numbers are more cumbersome to acquire, and pose a higher barrier for the adversary to create accounts. In particular, most countries implement mandatory SIM card registration [1], making it impossible to legally acquire a phone number fully anonymously there, breaking institutional privacy.

Once the account has been registered, the adversary must complete the account's profile. While 8 apps require in their terms of service that the provided profile data such as a name must be real, no app appears to verify the user-provided data, therefore posing no barrier to an adversary. 12 apps require that a user uploads a photo, with all except Tinder requiring that it is a face photo. Of course, an adversary could upload any person's face photo to maintain social privacy. As an additional safety feature, 13 apps then provide face verification, although this is optional except on Bumble. This step results in a profile badge, increasing trustworthiness [3, 31]. A user needs to complete an app-specific challenge while showing their face to get verified: for example, on Tinder or Bumble they must strike a given random pose, and on LOVOO they must hold a piece of paper with their name and a unique code. This image is also compared to the user's profile photo; the verification is invalidated if the profile photo is later changed. This requirement for a genuine profile photo can expose the adversary to other users, breaking social privacy.

Overall, the strictest service appears to be Bumble with mandatory phone and face verification. Conversely, some apps enable the adversary to browse other profiles anonymously, e.g., by allowing a profile to be empty (Grindr), and/or stealthily, e.g., by only requiring an email address and not a photo (MeetMe and Tagged) or by hiding one's own profile from others because it is incomplete (Hinge).

5 User Data Privacy Risks

With our accounts, we can now examine **what private data an adversary can learn about one or all other users**. We consider four data categories: personal data, sensitive data, app usage data, and location. For each category, we distinguish three modes of data exposure and leaks, mapping to our three levels of adversary sophistication (Section 3.2):

1. *user interface (UI) exposure*, where the data is readily shown in the UI to a technically unskilled adversary.
2. a *traffic leak*, where additional data is included in network traffic that is automatically sent to the user, but not shown anywhere in the UI. Such leaks require that adversaries can (or are helped to) passively intercept and view traffic.
3. an *exfiltration leak*, where the adversary must actively extract data from the service. This can be achieved programmatically by forging network requests, or using automated API requests that are chained to use previous responses (e.g., extracting profile properties using filters).

These modes also map to our distinction between *intended* sharing, i.e., UI exposure, and *inadvertent* sharing, i.e., traffic and exfiltration leaks. For the former, intended sharing, LBD app users can observe this data themselves for other users, and can therefore reasonably be assumed to be aware that their own data is also shared with others. Nevertheless, there are still significant privacy risks attached to this data sharing, as the adversary can abuse this data for purposes such as social engineering, identity theft, or extortion. We evaluate the UI exposure of data fields based on their incidence: whether apps make the fields mandatory and then *always* show these to other users, whether apps either display fields but make them optional or provide the choice to show/hide a mandatory field (*if set/shown*), or whether apps do not display or support the field and it is thus *never* shown. This represents the agency users have regarding what data they want to share, and the extent to which the app desires to collect data.

The latter, inadvertent sharing, represents data hidden in the UI for which users are therefore not aware of the data being shared. This results in a severe violation of their expectations of privacy towards other users, and an information asymmetry, as only adversaries with the capability to discover this data can abuse this data. These leaks also represent genuine vulnerabilities in the implementation of LBD apps.

For Tables 3 to 6, we use the following symbols to represent each mode's incidence:

Incidence	UI Exposure	Traffic Leak	Exfiltration Leak
Always	◇	⟐	◈
If set/shown	○	⊙	⊕
Never	–		

5.1 Analysis Methods

We design our systematic app analysis to elicit the three types of data exposure and leaks that we consider. We opt for manually reverse engineering each app's API, rather than (semi-)automatically searching leaks [70, 78], to achieve maximum coverage across potentially leaked attributes, API endpoints, message formats, and possible obfuscation techniques. First, we interact with the various functionalities of the app and list the data displayed in the UI (searching *user interface exposure*). Simultaneously, we capture the associated API traffic and examine whether it contains additional data that is not displayed in the UI (searching *traffic leaks*). We also examine any API calls that access the user's own profile for any enumeration of fields that are not leaked to others by default (e.g., email). Then, we add these fields to requests for API endpoints that retrieve data on other users and observe whether the API then exposes the additional fields (searching *exfiltration leaks*). These exfiltration leaks also include the automation of the location attacks that we perform on the 15 services (Section 5.5), by developing scripts that reliably and repeatedly spoof our location with modified API requests. Lastly, we upload a photo with EXIF data and check whether the photo as seen by another user contains the original EXIF data (e.g., GPS data) [47]. Two authors independently conducted this process for each application and compared results, serving to minimize potential errors. The conclusive set of features, along with their respective sensitivity levels, was settled upon after a discussion with all authors. Where necessary, app analyses were (partially) repeated to verify results.

If the service provides a feature-complete web app, we use Google Chrome's browser developer tools to directly monitor the LBD app's API traffic. If the service or some of its core features are only available on mobile, we run the mobile app either in an emulator or on a real device running Android. We use HTTP Toolkit [101] to intercept and decrypt Android HTTPS traffic, using Frida [113] to circumvent certificate pinning where necessary. For the exfiltration attacks, we use the Python Requests library [116] to automate API traffic.

5.2 Personal Data

We first consider leaks of personal data or personally identifiable information (PII), which can lead to identifying a specific person, either on its own or when combined with other data. Services are required to adhere to legal principles before they are allowed to process such personal data. For example, article 5 of the European General Data Protection Regulation (GDPR) requires that personal data is "processed lawfully, fairly, and in a transparent manner" [115]. More broadly, users may have various levels of comfort in sharing such personal data with others [95]. Finally, knowledge of these attributes enables in part the malicious intents within our threat model (Section 3.2), e.g., social engineering or

Table 3: Overview of data leaks for personal data.

	Tinder	Badoo	POF	MeetMe	Tagged	Grindr	Tantan	Jaumo	LOVOO	happn	Bumble	Hinge	Hily	OkCupid	Meetic
First name	◇	◇	○	◇	⟐	–	–	◇	◇	◇	◇	◇	◇	◇	◇
Last name	–	–	–	○	–	–	–	–	–	–	–	–	–	–	–
Gender	○	⟐	○	◇	⟐	○	⟐	⟐	⟐	⟐	◇	○	⟐	◇	⟐
Age	◇	◇	◇	◇	◇	○	◇	◇	◇	◇	◇	◇	◇	◇	◇
Date of birth	–	–	–	–	⟐	–	–	–	–	–	–	○	–	–	–
Education	○	○	◇	○	–	–	○	⊙	○	○	○	○	◇	○	○
Employment	○	○	◇	–	–	–	○	⊙	○	○	○	○	◇	○	○
Languages spoken	–	○	○	–	○	–	–	⊙	○	–	○	○	○	○	○
Nationality	–	–	–	–	–	–	–	–	–	–	–	–	–	–	○
Place of residence	○	–	◇	–	◇	–	○	◇	◇	⊙	○	◇	–	–	◇
Hometown	–	–	–	–	–	–	–	–	–	–	○	○	–	–	–
Relationship status	–	⟐	○	○	○	○	–	⊙	○	–	–	–	–	○	○
Marital status	–	–	○	○	○	○	–	⊙	–	–	–	–	–	○	○
Having children	○	⟐	○	○	–	–	–	⊙	○	○	○	○	◇	○	○
Having siblings	–	–	◇	–	–	–	–	–	–	–	–	–	–	–	–
Email address	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Phone number	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Other platforms	–	–	–	–	–	○	–	–	–	–	–	–	⟐	–	–
Photos	◇	◇	○	○	○	○	◇	◇	◇	◇	◇	◇	◇	◇	◇
Interests	○	○	○	○	○	–	○	⊙	–	○	○	○	○	○	○
Income	–	–	–	–	–	–	○	–	–	–	–	–	–	–	○

identity theft. Table 3 lists our detailed analysis of leaks of personal data across the 15 LBD apps in our scope. We now summarize the main findings of this analysis.

5.2.1 User Interface Exposure

Name 11 services require that users provide their first name and show this to other users, immediately providing one important piece of identifying information. POF, Tantan, and Grindr only use a nickname; on Grindr, this can be an empty string. Tagged requires both a (unique) nickname that is shown to others, and a first name that is not shown. On MeetMe, the user has the option to set and make their last name visible to other users.

Gender All services require the user to set their gender[5], except for Grindr (but it will show the gender if set). Only Bumble and OkCupid will always show the gender. Tinder, POF, and Hinge let users explicitly show or hide their gender.

Age All services require setting a date of birth. All but Grindr will then always show the user's age. Hinge offers the option to show the date of birth in the UI.

Curriculum vitae 13 services ask about a user's education (usually level and institution); 12 do so for employment (usually job title and employer). For POF and Hily, these fields are mandatory and will always be shown to others. Otherwise, they are usually optional but shown if set. In terms of languages spoken, 8 apps have it as an optional field that will then be shown. On POF it is again mandatory. Only Meetic allows setting and optionally showing a user's nationality. 6 services require that users set and show their current place of residence (at town level). 3 more services let this field be optional but will show it if set. Bumble and Hinge optionally show a user's hometown (where they grew up).

Family status 9 services allow a user to optionally set their current relationship status, and will then show it; in 7 of these, being married is among the relationship options. 11 services optionally show whether someone has children; on Hily, a user is required to set and show this. Finally, POF requires a user to set and show their number of siblings and birth order.

Miscellaneous We do not find any app that shows or leaks the email address or phone number used for registration. 9 apps integrate with other social networks such as Instagram, but usually only show the contents of profiles there without the possibility to visit them. Only Grindr lets users (optionally) show their identifiers on other platforms. As mentioned in Section 4, 12 services require photos and will show these to others; the remaining 3 show them if provided. Photos on MeetMe still contain the original EXIF metadata, therefore potentially leaking the time when or location where the photo was made. All other services properly strip (sensitive) EXIF metadata. 13 services optionally show any personal interests the user has set. On 8 apps, these interests comprise personal values: for example, Bumble users can select feminism, voting rights, or Black Lives Matter. Tantan and Meetic optionally allow to set and show one's income.

5.2.2 Traffic Leaks

Beyond UI exposure, several apps leak certain fields as part of API traffic leaks. Tagged leaks the (required) *first name* and the first letter of the (optional) *last name*. Most services that do not display *gender* leak it. Tinder leaks specifically non-binary gender identities, as these are represented by a different field from the gender field. Tagged leaks the (mandatory) *date of birth*. happn leaks the (optional) *place of residence*. On Jaumo, *employment*, *education*, *relationship status*, *marital status*, *children*, and *interests* are purportedly only shown to others if those have also set these fields themselves, but they are leaked in API traffic to all users. Similarly, on Badoo, the *relationship status* and *having children* are only shown to others if they have a sufficiently complete profile, but the fields leak. Finally, Hily leaks identifiers for *other platforms*.

[5] Note that most international data protection legislation does not recognize gender identity as "sensitive data" [44], even though it may be particularly sensitive for users with a non-binary gender identity or those who changed gender, or if gender could be a basis for discrimination.

Table 4: Overview of data leaks for sensitive data.

	Tinder	Badoo	POF	MeetMe	Tagged	Grindr	Tantan	Jaumo	LOVOO	happn	Bumble	Hinge	Hily	OkCupid	Meetic
Racial or ethnic origin	–	–	○	–	○	○	–	–	–	–	○	○	○	○	○
Political opinions	–	–	–	–	–	–	–	–	–	–	○	○	○	○	–
Religious/philos. beliefs	–	–	◇	–	○	–	–	⊙	–	–	○	○	○	○	○
Health data															
Height	–	⟐	◇	○	–	○	○	⊙	○	○	○	◇	○	○	○
Weight	–	–	–	–	–	○	–	–	–	–	–	–	–	–	○
Figure	–	–	○	○	–	○	–	⊙	–	–	–	–	○	○	–
Fitness	○	–	–	–	–	–	–	⊙	–	○	○	–	○	–	○
Diet	○	–	–	–	–	–	–	⊙	–	○	○	–	◇	○	○
Eye color	–	⊙	◇	–	–	–	–	–	–	–	–	–	–	–	○
Hair color	–	⊙	◇	–	–	–	–	–	–	–	–	–	–	–	○
Smoking	○	⟐	◇	○	–	–	–	⊙	○	○	○	○	◇	○	○
Alcohol	○	⟐	○	○	–	–	–	⊙	–	–	○	○	◇	○	–
Recreational drugs	–	–	◇	–	–	–	–	–	–	–	○	○	–	○	–
(COVID) vaccination	○	–	–	○	–	○	–	–	–	–	–	○	○	–	–
HIV status	–	–	–	–	–	○	–	–	–	–	–	–	–	–	–
Sexual orientation	○	⟐	⟐	⟐	○	–	–	–	–	–	–	○	–	⟐	–
Sex life	–	–	–	–	–	○	–	–	–	–	–	–	–	◇	–

5.3 Sensitive Data

Certain personal information is considered particularly sensitive, for example, because it could enable discrimination [160] or because users simply feel uncomfortable sharing it [95]. Such data also enjoys explicit legal protection: for example, article 9 of the GDPR generally prohibits the processing of "special categories of personal data" [115]; we use these categories for our analysis. However, LBD apps enable and sometimes encourage users to share such information, as they also form a basis upon which users may want to select potential partners. Table 4 lists our detailed analysis of leaks of sensitive data across the 15 LBD apps in our scope. We now summarize the main findings of this analysis.

5.3.1 User Interface Exposure

Racial or ethnic origin 8 services let a user optionally set their racial or ethnic origin, although for Tagged and Bumble this is not possible in all countries. 7 of these will then show it if set, while on Hinge a user can explicitly hide it.

Opinions and beliefs 4 apps allow users to optionally set and show their political leaning. 7 apps allow users to optionally set or show their religious or philosophical beliefs, with POF requiring it to be set and shown.

Health data Data related to a user's physical health is required for some services, including height, diet, eye or hair color, and smoking, alcohol, and recreational drug habits. Further attributes that are (only) optional are a user's figure, exact weight, and fitness level. 5 apps allow to optionally set and show whether a user is vaccinated; on all these services, this can be for COVID-19, while Grindr also supports mpox and meningitis. Grindr also has an optional field for a user's HIV status, including their last test date.

Table 5: Overview of data leaks for app usage data.

	Tinder	Badoo	POF	MeetMe	Tagged	Grindr	Tantan	Jaumo	LOVOO	happn	Bumble	Hinge	Hily	OkCupid	Meetic
Other was recently active	◇	◇	◇	◇	◇	◇	◇	◇	◇	◇	◈	◇	◇	◇	◇
Last activity time	–	◈	⟐	⟐	◇	◇	◇	⟐	⟐	⟐	◈	⟐	–	⟐	◇
Account creation time	–	–	–	–	◇	–	⟐	–	–	–	–	⟐	–	⟐	⟐
Relationship type sought	⟐	○	◇	◇	○	○	–	○	◇	○	○	○	◇	◇	○
Wanting children	○	⟐	○	–	–	–	–	⊙	–	○	○	○	◇	○	○
Filters	–	⟐	◇	⟐	–	–	⟐	◇	–	–	◈	–	–	⟐	◇
# profiles per API request															
Card stack	10	20	69	1	20	–	5	10	30	20	10	20	15	1	30
Grid	–	20	42	30	24	100	–	–	40	–	–	10	–	–	20
Permanent profile access	⟐	◇	◇	◇	◇	◇	⟐	⟐	◇	⟐	⟐	⟐	⟐	◇	◇
See profiles while paused	⟐	–	◇	–	◇	–	–	⟐	–	⟐	–	⟐	–	–	–
Other has liked you	–	⟐	⟐	⟐	⟐	–	⟐	⟐	–	⟐	⟐	⟐	⟐	⟐	⟐
Other has disliked you	–	⟐	–	–	⟐	–	–	–	–	–	⟐	–	–	⟐	⟐
Popularity score	–	⟐	–	–	–	–	⟐	–	–	–	–	–	–	–	–
Number of likes/dislikes	–	◈	–	–	–	–	⟐	–	–	–	–	–	–	–	–

Sexual orientation and sex life 4 apps require that a user sets a sexual orientation but will then not show it in the UI. 3 apps let a user optionally set a sexual orientation, and will then show it. Grindr and OkCupid support optionally setting and showing labels related to a user's sex life, such as their preferred roles during sex or specific sexual practices. OkCupid only provides this option to LGBTQ users.

5.3.2 Traffic Leaks

As with personal data leaks, Jaumo leaks *health-related fields* to users for whom these fields are otherwise hidden in the UI as they have not set these themselves, and Badoo leaks *health-related fields* to those with an incomplete profile for whom the fields are hidden in the UI. The 4 apps that require to set a *sexual orientation* yet do not display it in the UI all leak it in API traffic.

5.4 App Usage Data

Next, we consider leaks of data that are related to app usage and the dating process, such as likes of others, recent activity, or the type of relationship sought. This data is strictly speaking not personal data, as they would not allow identifying a particular person. However, they are sensitive in the sense that users may not want (certain) other people to be aware of this data, e.g., to avoid stigma about their reasons for using LBD apps. Table 5 lists our detailed analysis of leaks of dating-sensitive data across the 15 LBD apps in our scope. We now summarize the main findings of this analysis.

5.4.1 User Interface Exposure

Activity All apps except Bumble show in their UI whether a user was recently active, which can be abused to track whether someone is actively using an LBD app (e.g., for stalking or monitoring a partner). 4 apps also display when the user was last active. Tagged displays when a user created their account.

Preferences All apps except Tantan allow a user to set the type of relationship they are searching for, such as a long-term relationship, casual encounter, or friendship. 5 apps require it and will always display it; 8 other apps will always display it if the user (optionally) sets it. Badoo and Hily require that a user sets whether they want children; Hily always displays it. 8 apps provide the option to set this field. 3 apps show in the UI what gender and age filters the other user has set. All these fields reveal the other's dating intentions and preferences, which they may not feel comfortable sharing.

Profile access 8 apps offer the ability to revisit a user's full profile using the UI at any time, as a user gets a link to a profile page. Some services also allow pausing the visibility of a profile to others. Of the 8 apps where this feature is free, 2 still display other profiles even when one's own profile is paused, allowing for stealthy browsing of other profiles.

5.4.2 Traffic Leaks

Profile access Even though the card stack model suggests that users can only see one profile at a time, in the background all apps except OkCupid receive data for more than one user in one API response. In the grid model, Grindr is the outlier by requesting 100 full and 500 partial (i.e., without distance) profiles at once. Given a user ID that is contained within the received profile data, all services then have a manner to request a user's full profile permanently and at any time. Next to the 8 apps that have full profile access in the UI (as discussed above), the 7 other apps offer a specific API endpoint that also enables continuous profile access. Only Badoo and Bumble generate a unique user ID for each other user, meaning user IDs cannot be shared between users (e.g., between the adversary's Sybil accounts). However, Bumble offers the option to share a profile with another user, circumventing this unique user ID. 4 apps that offer pausing profile visibility to others will display an error message in the UI, but still fetch profiles in background API traffic. All these leaks enable and simplify large-scale, long-term, and stealthy profiling: for the many users that are returned with few API requests, the adversary can continuously request their profile, and sometimes even while remaining invisible to other users.

User votes 12 apps leak in API traffic whether another user has liked the user,[6] before having voted oneself. (Only Tinder and LOVOO truly protect this field; Grindr does not have a truly similar concept of liking.) This leak of likes contrasts with users' perception that another (free) user must first vote before they can know whether the other likes them. Badoo, Bumble, and Hinge leak this in the user profiles of the card stack. The other apps leak the like by embedding user IDs or full profiles in the data retrieved for showing the blurred profile photos of users who like them. (13 apps show full profiles of likers only to premium users.) The API responses of POF, Tagged, Hinge, and Hily contain the timestamp of the like. POF's API additionally leaks how long the other user looked at a profile. Badoo, Tagged, Bumble, OkCupid, and Meetic leak whether another user disliked the user. Badoo and Tantan also leak another user's popularity score and (for Tantan) their number of likes/dislikes in API traffic.

Table 6: Overview of data leaks for location.

	Tinder	Badoo	POF	MeetMe	Tagged	Grindr	Tantan	Jaumo	LOVOO	happn	Bumble	Hinge	Hily	OkCupid	Meetic
Exact location	–	⊕	–	–	–	⊕	–	–	–	⊕	⊕	⊕	⊕	–	–
Trilateration type	–	O	–	–	–	E	–	–	–	R	O	O	O	–	–
Distance to other user	◇	◇	–	⟐	⟐	⊕	⟐	◇	◇	◇	◇	–	–	⟐	◇
City of recent location	–	◇	–	◇	◇	–	◇	◇	◇	–	◇	◇	◇	◇	–

Other fields 7 apps leak the *last activity time* and 4 apps leak the *account creation time* in API traffic. Tinder will show the (optional) type of relationship to others only if they have also set the field, but leaks the value to all. For the *wanting children* field, Badoo leaks it to users with an incomplete profile, and Jaumo leaks it to users who have not set the field themselves. 4 apps leak gender and age *filters* in API traffic.

5.4.3 Exfiltration Leaks

Badoo and Bumble are vulnerable to an exfiltration leak where the 'projections' field in an API request can be altered to force the fetching of additional data fields. Through this avenue, Bumble then leaks whether a user was *recently active*, their *last activity time*, and their *filters*; for Badoo, this leaks the *last activity time* and *number of (dis)likes*.

5.5 Location

The apps in our scope rely on a user's location and the proximity to others to select those other users that will be presented. This implies that the service receives and stores the user's (usually exact) location. A leak of this location can be particularly sensitive [14, 41, 52], e.g., if it reveals that a user visited locations such as clinics that might cause embarrassment [12]. Tracking a user's location over time can also reveal frequently visited locations, which combined with temporal patterns may reveal, e.g., a user's home or workplace [37, 41]. Moreover, the transition into the physical world can make such a leak outright dangerous [36]. A location leak

[6] We only consider regular likes, not 'superlikes', which is a usually paid feature to force the display of one's like to the other in their UI.

enables personal safety threats (Section 3.2) such as stalking, harassment, physical violence, or prosecution.

While early versions of some LBD apps leaked exact coordinates to others [63, 77], our analysis shows that by now, only Tantan suffers such a leak, and then only the coordinates at the (one) time of matching someone, with only that match. Instead, apps use the distance between users, which they will display (Table 6) and/or provide as filters. However, lacking sufficient protections, the availability of distances can still lead to the inference of a user's location. This is done through *trilateration*: given three tuples of positions P and their distances D to the user's location L, L will be at the intersection of the three circles with radius D and center P.

We define three types of trilateration, and apply these definitions throughout the rest of the section:

1. *Exact distance trilateration*: Services reveal the *exact* distance (accurate to the meter) to other users. Adversaries can then spoof their location to three random positions. Using those locations and the distances to the victim as revealed by the service, the adversary can trilaterate the victim [66].
2. *Rounded distance trilateration*: As a countermeasure, some services only reveal *rounded* distances to another user (e.g., to 1 km). Adversaries then spoof their location to some random starting position, and then incrementally shift in a certain direction until the reported rounded distance changes, doing so three times [103]. If attackers can determine the rounding method (i.e., flooring, rounding, or ceiling) – e.g., by first trying the attack on their own controlled accounts –, they will subsequently know the corresponding *exact* distances to a victim, namely at the three positions where the reported distance changed. With these locations and exact distances, the adversary can trilaterate the victim.
3. *Oracle trilateration*: Adversaries use an *oracle* that indicates through a binary signal whether a victim is located within proximity, i.e., when they are within a defined "proximity distance" from the attacker. This distance can either be a fixed distance set by the service, or a distance that the attacker can select (e.g., through a filter). Initially, the adversary roughly estimates the victim's location (e.g., the city of the victim as displayed in the UI, Table 6), and places themselves in this location to be within proximity. The attacker then incrementally moves themselves until the oracle indicates that the victim is no longer within proximity, and this for three different directions. The attacker now has three positions with a known exact distance, i.e., the preselected proximity distance, and can trilaterate the victim. In our approach, we deviate from the state of the art [103] by using a simpler method. Our argument is that, in the context of LBD apps, we do not need to resolve the "Disk Coverage Problem" as we have an approximate location, leading to a reduction in API requests. Furthermore, we avoid any unusually large movements, as this could trigger detection [55]. The combination of these factors decreases the risk of malicious activity being detected.

Historically, LBD apps had a bad track record in terms of enabling trilateration and leaking users' exact locations. Exact distance trilateration was shown to work on Tinder (in 2014 [144]), POF (2014 [111]), Grindr (2014 [51, 138] and 2018 [74]), and LOVOO (2019 [135]). Rounded distance trilateration used to work on Bumble (in 2021 [64]). We now (re)evaluate these attacks to observe whether LBD apps have since reduced their location privacy risks. We find that we can successfully retrieve a (quasi) exact location for 6 apps.

Exact distance trilateration Grindr is susceptible to exact distance trilateration, accurate to at least a 111 m by 111 m square (at the equator). This accuracy is reduced by local generalization, implemented by rounding user (latitude/longitude) coordinates to three decimal places before sending them to Grindr's servers, meaning they will never know a user's exact location. Nevertheless, we consider this rounding insufficient, especially in sparsely populated areas. Moreover, while users can enable hiding their distance from other users, this distance can still be inferred as the grid is sorted by distance. It was previously known that two colluding accounts can put themselves before and after a user to bound the distance [65]. We find a novel way that enables distance inference with only one account, by iteratively manipulating the minimum distance parameter of the grid retrieval endpoint. This enables exact distance trilateration even for users with hidden distances, including in countries such as Egypt where Grindr considers the safety of its LGBTQ users at high risk and therefore always hides distances [59].

Rounded distance trilateration happn displays a rounded distance in the UI, while leaking a higher-precision distance in their API, rounded up to the nearest value in a set of incrementing distances: 249, 499, 999, 1999, . . . m. Both enable rounded distance trilateration, the latter with fewer iterations.

Oracle trilateration Badoo, Bumble, Hinge, and Hily are all susceptible to oracle trilateration. In all these apps, the distance filters serve as the proximity oracle, as the filters use exact distances. For Hinge and Hily, this happens despite distances being hidden in the UI, highlighting how one cannot assume that hiding distances solves trilateration vulnerability, as subtle 'side channels' may still enable trilateration.

No vulnerability discovered Tinder and LOVOO thwart trilateration by implementing "grid snapping" [77, 103, 125] to significantly reduce the accuracy of displayed distances. This grid system divides the physical space into smaller grid cells (for Tinder: 1×1 mile, for LOVOO: 1×1 km). All coordinates inside a cell are then mapped to its center (Tinder) or right side (LOVOO), and these mapped approximate coordinates are used for distance calculation, making all forms of accurate trilateration impossible. This was previously confirmed for Tinder [22, 63] and LOVOO [135].

POF and Meetic do not access the exact GPS location, instead relying on user input for their location at the town level. MeetMe, Tagged, and OkCupid do access the exact GPS location, but convert it to the closest town. The distances used on these services are therefore between two users' town centers, making all forms of accurate trilateration impossible. We could not reverse engineer the API message signatures for Tantan and Jaumo. As a result, we could not systematically spoof our location to test trilateration.

5.6 App-centric Summary

We now summarize our findings from the perspective of the per-app privacy posture. In terms of *intended sharing*, we compare the extent of collecting personal and sensitive data, and the user freedom in doing so. Profiles on POF, Meetic, OkCupid can contain the largest amount of data, supporting up to 23 different fields, of which up to 11 fields are sensitive. This may be due to their origins as traditional online dating platforms that use more extensive profiles. All these apps are also owned by the same owner, Match Group (Appendix A), as is the app with the next largest amount of fields (Hinge, 21 fields). Comparatively, Tantan (9 fields) and LOVOO (12), and Tagged (13) support the fewest (sensitive) fields. Tagged also stands out in supporting no health-related fields. While Grindr also has few (13) fields, these comprise very sensitive attributes, including HIV status and sexual preferences. Nevertheless, disclosure of these fields is seen as beneficial by Grindr's primary audience of gay and bisexual men [143, 151]. Moreover, privacy and anonymity on Grindr may be preserved through other means: notably, all fields are optional. This may result in a lower prevalence of data sharing: for example, only 13% of Grindr users used their real name [127] (compared to 70% on Tinder [19]). However, from the perspective of the adversary, the possibility to leave their profile empty also increases their stealth. In terms of a user's choice to share data, POF, Hily, and Badoo go the furthest in requiring many fields that are optional or missing on other services, including sensitive data such as smoking, alcohol or drug use, and religious beliefs. All other apps except Grindr require 3 to 6 fields. Note that even if fields remain optional, other users might still expect that these are disclosed [150], potentially reducing the actual user choice.

In terms of *inadvertent sharing*, API leaks introduce privacy breaches, even though excessive leakage through APIs is a well-known issue, e.g., being part of the OWASP API Security Top 10 [155]. Even the largest apps are not immune to such vulnerabilities. Non-binary genders leak on Tinder, while Badoo (and Bumble) are vulnerable to exfiltration leaks. The latter two services have been aware of these leaks since 2020 [117], but do not appear to have fully fixed them. Apps do protect personal and sensitive data relatively well, with most traffic or exfiltration leaks affecting only app usage data. Notable exceptions that are leaked relatively often are gender (8 apps), and sexual orientation (4 apps), a sensitive field. Interestingly, almost all implementations of data sharing reciprocity fail. Tinder, Badoo, and Jaumo leak attributes that are hidden for other users while one's own profile is incomplete. Similarly, if the adversary hides their profile, they can still fetch profiles on 6 apps, enabling stealthy data gathering.

These privacy postures extend to *location data*. Oracle trilateration is the most powerful inference method: while most apps have implemented measures to protect distances, the ability to do binary proximity testing causes them to remain vulnerable. For all services where we were able to execute our experiments but that were not vulnerable to trilateration, users' locations were protected by calculating distances to a generalized point, i.e., a nearby town center or a point on a grid, therefore omitting exact location from the distance computation and making its retrieval impossible. Finally, all apps except OkCupid will also fetch multiple profiles at once. This may be for efficiency reasons, i.e., to reduce the number of server requests. However, together with the ability to permanently request a user's profile at any time, and easily create accounts, these data exposures and leaks enable large-scale, long-term, and stealthy profiling of LBD app users, allowing the adversary to collect personal data on many users at once as well as data that is presumed to be hidden.

6 Privacy Policies

In our final analysis, we examine **how privacy policies of LBD apps discuss and acknowledge personal data collection and potential leaks** and compare this with real-world behavior. One aspect of the lawful processing of personal data in the GDPR is transparency [115]. Articles 13 and 14 lay out the information that the data controller (here the LBD app's provider) must communicate to the data subject (here the user), such as the categories of personal data being processed and the legal basis. Typically, web services and applications include this type of information in a privacy policy. Together with the Terms of Service (ToS), the privacy policy is displayed to users before they create an account.

This raises the question of how LBD apps inform their users about the collection, sharing, and security of personal and sensitive data. To determine this, we read the privacy policies, ToS, and related documents for all 15 LBD apps in scope. We systematically check whether the documents meet the information requirements in the GDPR and whether they contain any information about the processing of personal data including special categories (per the GDPR's article 9), the use of location data, and (controls for) the potential risks of sharing personal data with the application or with other users.

Processing of personal data of users All apps have a privacy policy, and these policies generally meet legal requirements for informing users. However, the level of detail differs between apps. For instance, the privacy policy of Hily displays a detailed table with each specific piece of processed information, along with the source, purpose, and legal basis for the processing, while Tinder includes a non-exhaustive list of pieces of information being processed for each listed purpose. 12 privacy policies mention that the LBD app will be processing sensitive data. The legal basis for processing is mostly consent, and sensitive attributes are stated to be optional. However, it seems highly likely that the user would need to provide at least their sexual orientation in order for the app to properly function, contradicting that this sensitive attribute would be optional.

Location data For 9 LBD apps, the privacy policy contains information about revoking consent for the processing of personal data. Out of those apps, 3 mention that the user is free to decline geolocation permissions but that some services might then not work properly. happn and LOVOO's privacy policies state that an alternative way to determine location will be used if the application cannot access the GPS location of the phone. MeetMe and Tagged mention the possibility of hiding a user's exact location from others in the profile settings. Finally, the privacy policies of 6 apps do not inform users about the consequences of revoking the geolocation permission. When testing this in practice, only 3 applications will not show other profiles without the geolocation permission. For the other 12 apps, the user is proposed to manually specify the town they live in as an alternative location. Interestingly, Grindr's privacy policy warns users that a location inference attack might be possible; other than that, no application discusses the privacy risks or potential mitigations specifically for inference attacks on location data.

Privacy controls Some LBD apps provide more guidelines and control for privacy than others. 6 apps mention in their privacy policy that users can set at least part of their profile to private. This benefits the users' privacy in the sense that the user matching process is improved without making additional data visible to other users. In practice, 2 of those 6 apps allow the user to hide (at least part of) their profile, and POF provides the option to hide one specific attribute from other users (i.e., gender). The remaining 3 apps also include some profile hiding features, but only upon payment as part of their premium subscription. Additionally, the user can hide a single attribute in 3 more apps, but do not mention this possibility in their privacy policies.

Next to this, 7 privacy policies warn about sharing data with other users. They mostly advise users to be cautious when sharing personal information on their public profile or with other users. Only LOVOO and Bumble explicitly list which types of user data might be visible to other users. Some other apps discourage users from sharing certain types of personal information such as their address, full name, or email, and even prohibit the sharing of financial information such as credit card numbers in their ToS.

7 Discussion

7.1 Functionality versus Privacy

In LBD apps, there is an inherent tension between maintaining one's privacy and engaging in sufficient self-disclosure to enable forming relationships [48]. LBD app users find it important that profiles contain certain information [6], and use the (sensitive) profile data to filter potential partners on desired traits [28] and search for more information about them [48], to ultimately decrease uncertainty, increase trust, and improve feelings of personal safety [28, 30, 109, 140]. In return, users readily share information themselves [28, 45]. Information disclosure may also (be believed to) result in more success on the platform [58, 118, 142], potentially further encouraging data sharing. Some may opt to self-disclose even sensitive information upfront: e.g., transgender users to avoid physical danger when meeting in-person [43], and users with disabilities to filter out potential partners who would be uncomfortable with their disability [107]. Expectations on information disclosure depend on the context [112], and arguably, online dating is a context where a large amount of disclosure may be expected, not perceived as concerning, and even perceived as beneficial.

Nevertheless, LBD apps entail specific privacy risks [131, 132], and privacy has been found to be a main concern for LBD app users [30, 50, 84]. Users' concepts of social privacy violations were more concrete compared to institutional privacy [15, 49, 82, 97, 134], aligning with our adversary model. Users actively limit the information they disclose on LBD apps to maintain their (social) privacy [15], or provide false information for privacy reasons [19], e.g., if they worry about being recognized by people they know [15, 28, 48], or that an unknown individual tracks them down [109]. User sensitivity to data exposure also differs for each attribute [6]. Limiting disclosure may be particularly pertinent to certain (higher-risk) populations [102]. For example, women are at higher risk of online stalking and harassment [23], and were more concerned about (location) privacy than men [4, 50]. LGBTQ people also face higher risks [128], and they may not want to be discovered on LBD apps if they are not out [13, 30, 49, 143] or face prosecution [129]. In general, online dating represents a very sensitive context, encompassing intimate relationships and data sharing with strangers [48], with users generally being unaware of who is observing their data, due to the adversary's potential stealth.

LBD app users may also experience pressure to disclose data. On the one hand, they may feel forced by other users [48, 146], even for very sensitive data such as HIV status [151]. On the other hand, LBD apps nudge towards data sharing, purportedly to improve matching others [147]. For example, Hinge tells users that "the more you share, the better your matches will be". Default visibility may also lead to additional sharing: for example, out of Hinge's 20 hideable fields, 12 are visible by default; this is particularly important as the majority of users tend to not change default settings [53].

Ultimately, LBD apps users desire the choice to disclose personal or sensitive information [150]. We believe LBD apps should enable users to consciously make that choice (controlling intended sharing) as well as maximally protect users' data if they choose not to disclose (preventing inadvertent sharing). In this light, we consider our findings to be important in that they make users better aware of the actual data sharing practices on LBD apps. While (intended) data sharing is a crucial part of the functionality of LBD apps and may align with users' privacy expectations [79], and there are genuine benefits regarding safety, these must be balanced with the genuine privacy concerns and risks that users may face when using LBD apps. An interesting avenue for future work would therefore be to analyze users' privacy perceptions of LBD apps given awareness of our findings, both in terms of exposure (intended sharing) and leaks (inadvertent sharing). For example, such a user study has previously shown that mobile users find opaque data sharing with third parties "creepy" [121]. Similarly, our findings may make users reconsider their privacy stance regarding these apps and use more caution in sharing their personal data – including their location – on these apps, helping to reduce the mismatch between perceived privacy risks and actual behavior [28, 112, 130]. At the same time, we hope that our findings will lead to improved privacy precautions by the LBD apps themselves, including applying additional countermeasures to prevent user data leaks in the future.

7.2 Countermeasures

Our analysis shows that the APIs for several apps suffer traffic and exfiltration leaks that cause privacy breaches that users are unlikely to be aware of. To prevent these inadvertent data leaks that violate users' privacy expectations about LBD apps [79, 134], services should harden their APIs [155] by limiting the exposed API endpoints, enforcing proper access control, and ensuring that no unnecessary (i.e., not displayed) attributes are sent in API responses. Specifically for locations, services should implement techniques to prevent trilateration and other attacks that reveal a user's exact location. For example, they could apply spatial cloaking, such as snapping to grids [77, 103, 125] or nearby towns before computing distances between users; the real-world deployment of this mitigation (Section 5.5) shows that this does not overly impede functionality. A suite of academic work develops protocols for privacy-preserving proximity testing that allow for approximate location information to be released while protecting an exact location, see, e.g., [7, 93, 124, 136].

LBD apps could also increase friction for adversaries to gather data (at a large scale). This can range from requiring a phone number and email address, requiring account or face verification, rate limiting [105] or verifying API requests, detecting fake or rapidly shifting locations [9, 55, 105], to detecting malicious accounts [62, 133]. However, these techniques mostly serve to annoy the adversary, and may not meaningfully prevent a motivated attacker from executing their attack. For example, the advent of deepfakes and AI-generated images may make face verification decreasingly robust [76]. Some services sign messages to verify authenticity, although the inherent fact that this must occur client-side makes these signatures vulnerable to reversing (as we observed ourselves). Rate limiting is also easily circumvented by multiple (Sybil) accounts [145, 156], especially since there is no need for establishing a social connection beforehand [103]. Concurrently, these countermeasures increase friction for legitimate users to create accounts, and force them to share more data, defeating the privacy goals.

LBD app users should have maximal visibility and control over what they share with others. Profile data could be hidden by default, requiring that users consciously enable sharing it. Users could also have the option to show sensitive data only in a second phase (e.g., after matching), as to not broadcast this data to all users. Apps could also add the option to only see and be seen by verified accounts (as already exists on, e.g., Jaumo). All apps should clearly, explicitly, and repeatedly ask if users want to share their current location (especially if that location might be sensitive) [40], or provide the option to only share an approximate location (e.g., town center).

In the end, the most effective strategy is to not have data in the first place. The most popular LBD app, Tinder, lacks certain sensitive data attributes that are common on other apps, such as height, racial or ethnic origin, political opinions, and religious or philosophical beliefs, and snaps user locations to a grid, making the displayed distance only a coarse approximation; yet people still use it. By protecting data before it is sent to the service, it is impossible to expose or leak it, and users' privacy is maximally protected.

7.3 Responsible disclosure

We responsibly disclosed our findings to the vendors of all 15 apps, sending a draft of this paper and a list of concrete vulnerabilities (i.e., traffic and exfiltration leaks) for that app, by email to designated security addresses if available or else a general support address. Vendors for 10 out of the 15 apps immediately acknowledged receipt, indicating their responsiveness to security and privacy matters; after retrying our disclosure after five months, two more apps acknowledged receipt. Of these 12 apps, 9 engaged in substantial and productive discussions regarding our discovered leaks, and indicated that they had deployed concrete fixes. These interactions emphasize the tangible results of our collaborative engagement with these vendors, underscoring the concrete strides taken to enhance the overall privacy of the LBD app ecosystem.

8 Conclusion

Through a systematic analysis of 15 popular LBD apps, we find that they routinely expose personal data to other users. While users may feel compelled to share such data, there is a particular risk when APIs leak data hidden in the UI as well as exact user locations, as users will not be aware that they are sharing this data, which can lead to additional harm. Additionally, the apps' privacy policies generally fail to inform users about these privacy threats and leave the burden of protecting personal (sensitive) data to the users. We hope that the awareness that we bring of these issues will lead LBD app providers to reconsider their data gathering practices, protect their APIs from data leaks, prevent location inference, and give users control of their data and therefore ultimately their privacy.

Acknowledgments

We thank the anonymous reviewers and shepherd for their valuable feedback. This research is partially funded by the Research Fund KU Leuven, and by the Cybersecurity Research Program Flanders. This research was supported by an in-kind donation from the De Roeck family.

References

[1] *Access to Mobile Services and Proof of Identity 2021. Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19*. GSM Association, Apr. 2021.

[2] Airnow. *Leading markets based on Tinder iOS revenue as of June 2021*. Statista. July 3, 2021.

[3] K. Albury et al. *Safety, risk and wellbeing on dating apps: final report*. Swinburne University of Technology, Dec. 2019. DOI: 10.25916/5DD324C1B33BB.

[4] H. K. Aljasim and D. Zytko. "Foregrounding Women's Safety in Mobile Social Matching and Dating Apps: A Participatory Design Study". In: *Proceedings of the ACM on Human-Computer Interaction* 7.GROUP (Dec. 2022). DOI: 10.1145/3567559.

[5] B. Altpeter. *parse-play*. Version 2.1.0. Sept. 2022.

[6] M. Anderson, E. A. Vogels, and E. Turner. *The Virtues and Downsides of Online Dating*. Pew Research Center, Feb. 6, 2020.

[7] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi. "Geo-Indistinguishability: Differential Privacy for Location-Based Systems". In: CCS. 2013, pp. 901–914. DOI: 10.1145/2508859.2516735.

[8] *Are You on Tinder? Someone May Be Watching You Swipe*. Checkmarx, Jan. 23, 2018.

[9] G. Argyros, T. Petsios, S. Sivakorn, A. D. Keromytis, and J. Polakis. "Evaluating the Privacy Guarantees of Location Proximity Services". In: *ACM Transactions on Privacy and Security* 19.4 (Feb. 2017). DOI: 10.1145/3007209.

[10] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan. "The Menlo Report". In: *IEEE Security & Privacy* 10.2 (Mar. 2012), pp. 71–75. DOI: 10.1109/msp.2012.52.

[11] A. Barros, R. Almeida, T. Melo, and M. Frade. "Forensic Analysis of the Bumble Dating App for Android". In: *Forensic Sciences* 2.1 (2022), pp. 201–221. DOI: 10.3390/forensicsci2010016.

[12] A. R. Beresford and F. Stajano. "Location privacy in pervasive computing". In: *IEEE Pervasive Computing* 2.1 (2003), pp. 46–55. DOI: 10.1109/MPRV.2003.1186725.

[13] C. Blackwell, J. Birnholtz, and C. Abbott. "Seeing and being seen: Co-situation and impression formation using Grindr, a location-aware gay dating app". In: *New Media & Society* 17.7 (2015), pp. 1117–1136. DOI: 10.1177/1461444814521595.

[14] A. J. Blumberg and P. Eckersley. *On Locational Privacy, and How to Avoid Losing it Forever*. Aug. 2009.

[15] E. Bouma-Sims et al. "Out of Their Control: Investigating Privacy Attitudes and Behaviors Among Tinder Users". In: *18th Symposium on Usable Privacy and Security – Posters*. 2022.

[16] A. Boxiner and E. Vaknin. *Hacker, 22, seeks LTR with your data: vulnerabilities found on popular OkCupid dating app*. Check Point Research. July 29, 2020.

[17] R. Brandom. "Designing for the crackdown". In: *The Verge* (Apr. 25, 2018).

[18] P. B. Brandtzaeg, A. Pultier, and G. M. Moen. "Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy". In: *Social Science Computer Review* 37.4 (May 2018), pp. 466–488. DOI: 10.1177/0894439318777706.

[19] V. Breitschuh and J. Göretz. "User Motivation and Personal Safety on a Mobile Dating App". In: *11th International Conference on Social Computing and Social Media*. SCSM. 2019, pp. 278–292. DOI: 10.1007/978-3-030-21902-4_20.

[20] N. D. W. Cahyani, K.-K. R. Choo, N. H. Ab Rahman, and H. Ashman. "An Evidence-based Forensic Taxonomy of Windows Phone Dating Apps". In: *Journal of Forensic Sciences* 64.1 (2019), pp. 243–253. DOI: 10.1111/1556-4029.13820.

[21] D. Cameron and S. Wodinsky. "70,000 Tinder Photos of Women Just Got Dumped on a Cyber-Crime Forum". In: *Gizmodo* (Jan. 16, 2020).

[22] M. Carman and K.-K. R. Choo. "Tinder Me Softly – How Safe Are You Really on Tinder?" In: *12th International Conference on Security and Privacy in Communication Networks*. SecureComm. 2017, pp. 271–286. DOI: 10.1007/978-3-319-59608-2_15.

[23] V. Centelles, R. A. Powers, and R. K. Moule. "An Examination of Location-Based Real-Time Dating Application Infrastructure, Profile Features, and Cybervictimization". In: *Social Media + Society* 7.3, (July 2021). DOI: 10.1177/20563051211043218.

[24] A. Chaabane, G. Acs, and M. A. Kaafar. "You Are What You Like! Information Leakage Through Users' Interests". In: NDSS. 2012.

[25] R. Chatterjee et al. "The Spyware Used in Intimate Partner Violence". In: SP. 2018, pp. 441–458. DOI: 10.1109/SP.2018.00061.

[26] H. Cheng, S. Mao, M. Xue, and X. Hei. "On the Impact of Location Errors on Localization Attacks in Location-Based Social Network Services". In: SpaCCS. 2016, pp. 343–357. DOI: 10.1007/978-3-319-49148-6_29.

[27] A. Claesson and T. E. Bjørstad. *Out of Control. A review of data sharing by popular mobile apps*. Norwegian Consumer Council / mnemonic, Jan. 14, 2020.

[28] C. Cobb and T. Kohno. "How Public Is My Private Life? Privacy in Online Dating". In: WWW. 2017, pp. 1231–1240. DOI: 10.1145/3038912.3052592.

[29] C. Cobb, L. Simko, T. Kohno, and A. Hiniker. "A Privacy-Focused Systematic Analysis of Online Status Indicators". In: *Proceedings on Privacy Enhancing Technologies* 2020.3 (July 2020), pp. 384–403. DOI: 10.2478/popets-2020-0057.

[30] E. F. Corriero and S. T. Tong. “Managing uncertainty in mobile dating applications: Goals, concerns of use, and information seeking in Grindr”. In: *Mobile Media & Communication* 4.1 (2015), pp. 121–141. DOI: 10.1177/2050157915614872.

[31] V. Das. “Designing Queer Connection: An Ethnography of Dating App Production in Urban India”. In: *Ethnographic Praxis in Industry Conference Proceedings* 2019.1 (Nov. 2019), pp. 384–397. DOI: 10.1111/1559-8918.2019.01295.

[32] *Data Breach: Thousands Exposed as Dating App Leaks Private Data*. Nov. 25, 2019.

[33] K. Dhondt, V. Le Pochat, A. Voulimeneas, W. Joosen, and S. Volckaert. “A Run a Day Won’t Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks”. In: CCS. 2022, pp. 801–814. DOI: 10.1145/3548606.3560616.

[34] A. Di Luzio, A. Mei, and J. Stefa. “Uncovering hidden social relationships through location-based services: The Happn case study”. In: *2018 IEEE Conference on Computer Communications Workshops*. INFOCOM WKSHPS. 2018, pp. 802–807. DOI: 10.1109/INFCOMW.2018.8406866.

[35] M. Di Martino et al. “Personal Information Leakage by Abusing the GDPR ‘Right of Access’”. In: SOUPS. 2019, pp. 371–386.

[36] P. Doerfler. “Something you have and someone you know: Designing for interpersonal security”. USENIX Enigma. 2019.

[37] K. Drakonakis, P. Ilia, S. Ioannidis, and J. Polakis. “Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data”. In: NDSS. 2019. DOI: 10.14722/ndss.2019.23151.

[38] B. Eterovic-Soric, K.-K. R. Choo, H. Ashman, and S. Mubarak. “Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review”. In: *Computers & Security* 70 (2017), pp. 278–289. DOI: 10.1016/j.cose.2017.06.008.

[39] J. Farnden, B. Martini, and K.-K. R. Choo. “Privacy Risks in Mobile Dating Apps”. In: *21st Americas Conference on Information Systems*. AMCIS. 2015,

[40] K. Fawaz, H. Feng, and K. G. Shin. “Anatomization and Protection of Mobile Apps’ Location Privacy Threats”. In: USENIX Security. 2015, pp. 753–768.

[41] K. Fawaz and K. G. Shin. “Location Privacy Protection for Smartphone Users”. In: CCS. 2014, pp. 239–250. DOI: 10.1145/2660267.2660270.

[42] Á. Feal, P. Calciati, N. Vallina-Rodriguez, C. Troncoso, and A. Gorla. “Angel or Devil? A Privacy Study of Mobile Parental Control Apps”. In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (Apr. 2020), pp. 314–335. DOI: 10.2478/popets-2020-0029.

[43] J. R. Fernandez and J. Birnholtz. ““I Don’t Want Them to Not Know”: Investigating Decisions to Disclose Transgender Identity on Dating Platforms”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019). DOI: 10.1145/3359328.

[44] B. Fico, G. H. Sicuto, and H. Meng. *Does Brazil’s LGPD recognize gender identity, sexual orientation as sensitive personal data?* International Association of Privacy Professionals. Mar. 10, 2021.

[45] C. Fitzpatrick, J. Birnholtz, and J. R. Brubaker. “Social and Personal Disclosure in a Location-Based Real Time Dating App”. In: *48th Hawaii International Conference on System Sciences*. HICSS. 2015, pp. 1983–1992. DOI: 10.1109/HICSS.2015.237.

[46] D. Freed et al. ““A Stalker’s Paradise”: How Intimate Partner Abusers Exploit Technology”. In: CHI. 2018, pp. 1–13. DOI: 10.1145/3173574.3174241.

[47] G. Friedland and R. Sommer. “Cybercasing the Joint: On the Privacy Implications of Geo-Tagging”. In: *5th USENIX Conference on Hot Topics in Security*. HotSec. 2010.

[48] J. L. Gibbs, N. B. Ellison, and C.-H. Lai. “First Comes Love, Then Comes Google: An Investigation of Uncertainty Reduction Strategies and Self-Disclosure in Online Dating”. In: *Communication Research* 38.1 (2011), pp. 70–100. DOI: 10.1177/0093650210377091.

[49] C. Giles, C. Ashford, and K. J. Brown. “Online safety and identity: navigating same-sex male social “dating” apps and networks”. In: *Information & Communications Technology Law* 31.3 (June 2022), pp. 269–286. DOI: 10.1080/13600834.2022.2088061.

[50] M. Griffin, A. Canevello, and R. D. McAnulty. “Motives and Concerns Associated with Geosocial Networking App Usage: An Exploratory Study Among Heterosexual College Students in the United States”. In: *Cyberpsychology, Behavior, and Social Networking* 21.4 (2018), pp. 268–275. DOI: 10.1089/cyber.2017.0309.

[51] *Grindr: A chronicle of negligence and irresponsibility*. 2014.

[52] F. Groeneveld, B. Borsboom, and B. van Amstel. *Over-sharing and Location Awareness*. Center for Democracy & Technology. Feb. 24, 2010.

[53] R. Gross and A. Acquisti. “Information Revelation and Privacy in Online Social Networks”. In: *2005 ACM Workshop on Privacy in the Electronic Society*. WPES. 2005, pp. 71–80. DOI: 10.1145/1102199.1102214.

[54] S. Gürses and C. Diaz. “Two tales of privacy in online social networks”. In: *IEEE Security & Privacy* 11.3 (2013), pp. 29–37. DOI: 10.1109/MSP.2013.47.

[55] P. Hallgren, M. Ochoa, and A. Sabelfeld. “MaxPace: Speed-constrained location queries”. In: *2016 IEEE Conference on Communications and Network Security*. CNS. 2016. DOI: 10.1109/cns.2016.7860479.

[56] J. van der Ham and R. van Rijswijk-Deij. “Ethics and Internet Measurements”. In: *Journal of Cyber Security and Mobility* 5.4 (2017), pp. 287–308. DOI: 10.13052/jcsm2245-1439.543.

[57] C. Han et al. “The Price is (Not) Right: Comparing Privacy in Free and Paid Apps”. In: *Proceedings on Privacy Enhancing Technologies* 2020.3 (July 2020), pp. 222–242. DOI: 10.2478/popets-2020-0050.

[58] M. J. Handel and I. Shklovski. “Disclosure, Ambiguity and Risk Reduction in Real-Time Dating Sites”. In: *17th ACM International Conference on Supporting Group Work*. GROUP. 2012, pp. 175–178. DOI: 10.1145/2389176.2389203.

[59] J. Harrison-Quintana. *Assessing and Mitigating Risk for the Global Grindr Community*. Grindr. Oct. 21, 2021.

[60] W. U. Hassan, S. Hussain, and A. Bates. “Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide?” In: USENIX Security. 2018, pp. 497–512.

[61] D. R. Hayes and C. Snow. “Privacy and Security Issues Associated with Mobile Dating Applications”. In: *Conference on Information Systems Applied Research*. 2018.

[62] X. He et al. “DatingSec: Detecting Malicious Accounts in Dating Apps Using a Content-Based Attention Network”. In: *IEEE Transactions on Dependable and Secure Computing* 18.5 (2021), pp. 2193–2208. DOI: 10.1109/TDSC.2021.3068307.

[63] R. Heaton. *How Tinder keeps your exact location (a bit) private*. July 9, 2018.

[64] R. Heaton. *Vulnerability in Bumble dating app reveals any user’s exact location*. Aug. 25, 2021.

[65] N. P. Hoang, Y. Asano, and M. Yoshikawa. "Your neighbors are my spies: Location and other privacy concerns in GLBT-focused location-based dating applications". In: *19th International Conference on Advanced Communication Technology*. ICACT. 2017, pp. 851–860. DOI: 10.23919/ICACT.2017.7890236.

[66] M.-S. Huang and R. M. Narayanan. "Trilateration-Based Localization Algorithm Using the Lemoine Point Formulation". In: *IETE Journal of Research* 60.1 (Jan. 2014), pp. 60–73. DOI: 10.1080/03772063.2014.890826.

[67] B. Jaffe. *chrome-okc-plugin*. 2020.

[68] K. Kim, T. Kim, S. Lee, S. Kim, and H. Kim. "When Harry Met Tinder: Security Analysis of Dating Apps on Android". In: *23rd Nordic Conference on Secure IT Systems*. NordSec. 2018, pp. 454–467. DOI: 10.1007/978-3-030-03638-6_28.

[69] S. Knox, S. Moghadam, K. Patrick, A. Phan, and K.-K. R. Choo. "What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps". In: *Computers & Security* 94 (2020), p. 101833. DOI: 10.1016/j.cose.2020.101833.

[70] W. Koch, A. Chaabane, M. Egele, W. Robertson, and E. Kirda. "Semi-Automated Discovery of Server-Based Information Oversharing Vulnerabilities in Android Applications". In: *26th ACM SIGSOFT International Symposium on Software Testing and Analysis*. ISSTA. 2017, pp. 147–157. DOI: 10.1145/3092703.3092708.

[71] B. Krishnamurthy and C. E. Wills. "On the Leakage of Personally Identifiable Information via Online Social Networks". In: *2nd ACM Workshop on Online Social Networks*. WOSN. 2009, pp. 7–12. DOI: 10.1145/1592665.1592668.

[72] J. Krumm. "Inference Attacks on Location Tracks". In: *5th International Conference on Pervasive Computing*. 2007, pp. 127–143. DOI: 10.1007/978-3-540-72037-9_8.

[73] L. Kulik. "Privacy for Real-Time Location-Based Services". In: *SIGSPATIAL Special* 1.2 (July 2009), pp. 9–14. DOI: 10.1145/1567253.1567256.

[74] B. Latimer. "Grindr security flaw exposes users' location data". In: *NBC News* (Mar. 28, 2018).

[75] *Letter to Shareholders. Q1 2022*. Match Group, May 3, 2022.

[76] C. Li et al. "Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era". In: USENIX Security. 2022, pp. 2673–2690.

[77] M. Li et al. "All Your Location Are Belong to Us: Breaking Mobile Social Networks for Automated User Location Tracking". In: *15th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. MobiHoc. 2014, pp. 43–52. DOI: 10.1145/2632951.2632953.

[78] S. Li et al. "Collect Responsibly But Deliver Arbitrarily? A Study on Cross-User Privacy Leakage in Mobile Apps". In: CCS. 2022, pp. 1887–1900. DOI: 10.1145/3548606.3559371.

[79] J. Lin et al. "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing". In: UbiComp. 2012, pp. 501–510. DOI: 10.1145/2370216.2370290.

[80] J. Long. *No Tech Hacking. A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress, 2008. ISBN: 9781597492157. DOI: 10.1016/b978-1-59749-215-7.x0001-7.

[81] *Love in an algorithmic age*. Kaspersky. July 6, 2021.

[82] C. Lutz and G. Ranzini. "Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder". In: *Social Media + Society* 3.1, (2017). DOI: 10.1177/2056305117697735.

[83] S. Ma et al. "An Empirical Study of SMS One-Time Password Authentication in Android Apps". In: ACSAC. 2019, pp. 339–354. DOI: 10.1145/3359789.3359828.

[84] X. Ma, E. Sun, and M. Naaman. "What Happens in Happn: The Warranting Powers of Location History in Online Dating". In: CSCW. 2017, pp. 41–50. DOI: 10.1145/2998181.2998241.

[85] K. Macnish and J. van der Ham. "Ethics in cybersecurity research and practice". In: *Technology in Society* 63, (Nov. 2020). DOI: 10.1016/j.techsoc.2020.101382.

[86] S. Mansfield-Devine. "The Ashley Madison affair". In: *Network Security* 2015.9 (2015), pp. 8–16. DOI: 10.1016/S1353-4858(15)30080-5.

[87] S. Mascetti, L. Bertolaja, and C. Bettini. "A Practical Location Privacy Attack in Proximity Services". In: *14th International Conference on Mobile Data Management*. Vol. 1. 2013, pp. 87–96. DOI: 10.1109/MDM.2013.19.

[88] N. Mata, N. Beebe, and K.-K. R. Choo. "Are Your Neighbors Swingers or Kinksters? Feeld App Forensic Analysis". In: *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. TrustCom. 2018, pp. 1433–1439. DOI: 10.1109/TrustCom/BigDataSE.2018.00199.

[89] J. Mink, A. R. Yuile, U. Pal, A. J. Aviv, and A. Bates. "Users Can Deduce Sensitive Locations Protected by Privacy Zones on Fitness Tracking Apps". In: CHI. 2022. DOI: 10.1145/3491102.3502136.

[90] D. Myles. "Grindr? it's a "Blackmailer's goldmine"! The weaponization of queer data publics Amid the US-China trade conflict". In: *Sexualities*, (Dec. 2022). DOI: 10.1177/13634607221148137.

[91] Y. Nan et al. "Finding Clues for Your Secrets: Semantics-Driven, Learning-Based Privacy Discovery in Mobile Apps". In: NDSS. 2018. DOI: 10.14722/ndss.2018.23092.

[92] M. Nandwani and R. Kaushal. "Evaluating User Vulnerability to Privacy Disclosures over Online Dating Platforms". In: *11th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IMIS. 2017, pp. 342–353. DOI: 10.1007/978-3-319-61542-4_32.

[93] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh. "Location Privacy via Private Proximity Testing". In: NDSS. 2011.

[94] N. Nguyen. "There's A Simple Fix, But Grindr Is Still Exposing The Location Of Its Users". In: *BuzzFeed News* (Sept. 14, 2018).

[95] J. S. Olson, J. Grudin, and E. Horvitz. "A Study of Preferences for Sharing and Privacy". In: *Extended Abstracts of the 2005 CHI Conference on Human Factors in Computing Systems*. CHI EA. 2005, pp. 1985–1988. DOI: 10.1145/1056808.1057073.

[96] T. Orekondy, B. Schiele, and M. Fritz. "Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images". In: *2017 IEEE International Conference on Computer Vision*. ICCV. 2017, pp. 3706–3715. DOI: 10.1109/ICCV.2017.398.

[97] J. Ostheimer and S. Iqbal. "Privacy in Online Dating: Does It Matter?" In: *3rd International Conference on Cryptography, Security and Privacy*. ICCSP. 2019, pp. 71–75. DOI: 10.1145/3309074.3309085.

[98] *Out of Control. How consumers are exploited by the online advertising industry*. Forbrukerrådet, Jan. 14, 2020.

[99] K. Owens, A. Alem, F. Roesner, and T. Kohno. "Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives". In: USENIX Security. 2022.

[100] C. Patsakis, A. Zigomitros, and A. Solanas. "Analysis of Privacy and Security Exposure in Mobile Dating Applications". In: *1st International Conference on Mobile, Secure, and Programmable Networking*. MSPN. 2015, pp. 151–162. DOI: 10.1007/978-3-319-25744-0_13.

[101] T. Perry. *HTTP Toolkit*. Version 1.12.2. Dec. 2022.

[102] A. Phan, K. Seigfried-Spellar, and K.-K. R. Choo. "Threaten me softly: A review of potential dating app risks". In: *Computers in Human Behavior Reports* 3 (Jan. 2021), p. 100055. DOI: 10.1016/j.chbr.2021.100055.

[103] I. Polakis, G. Argyros, T. Petsios, S. Sivakorn, and A. D. Keromytis. "Where's Wally? Precise User Discovery Attacks in Location Proximity Services". In: CCS. 2015, pp. 817–828. DOI: 10.1145/2810103.2813605.

[104] I. Polakis, F. Maggi, S. Zanero, and A. D. Keromytis. "Security and Privacy Measurements in Social Networks: Experiences and Lessons Learned". In: *3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*. BADGERS. 2014, pp. 18–29. DOI: 10.1109/BADGERS.2014.9.

[105] I. Polakis, S. Volanis, E. Athanasopoulos, and E. P. Markatos. "The Man Who Was There: Validating Check-Ins in Location-Based Services". In: ACSAC. 2013, pp. 19–28. DOI: 10.1145/2523649.2523653.

[106] K. Pooley and H. Boxall. *Mobile dating applications and sexual and violent offending*. Trends & issues in crime and criminal justice 612. Australian Institute of Criminology, Nov. 2020. DOI: 10.52922/ti04862.

[107] J. R. Porter, K. Sobel, S. E. Fox, C. L. Bennett, and J. A. Kientz. "Filtered Out: Disability Disclosure Practices in Online Dating Communities". In: *Proceedings of the ACM on Human-Computer Interaction* 1.CSCW (Dec. 2017). DOI: 10.1145/3134722.

[108] A. Pradeep et al. "A Comparative Analysis of Certificate Pinning in Android & iOS". In: IMC. 2022, pp. 605–618. DOI: 10.1145/3517745.3561439.

[109] U. Pruchniewska. ""I Like That It's My Choice a Couple Different Times": Gender, Affordances, and User Experience on Bumble Dating". In: *International Journal of Communication* 14 (2020), pp. 2422–2439.

[110] S. Puglisi, D. Rebollo-Monedero, and J. Forné. "Potential Mass Surveillance and Privacy Violations in Proximity-Based Social Applications". In: *2015 IEEE Trustcom/BigDataSE/ISPA*. Vol. 1. 2015, pp. 1045–1052. DOI: 10.1109/Trustcom.2015.481.

[111] G. Qin, C. Patsakis, and M. Bouroche. "Playing Hide and Seek with Mobile Dating Applications". In: *29th IFIP TC 11 International Conference – ICT Systems Security and Privacy Protection*. SEC. 2014, pp. 185–196. DOI: 10.1007/978-3-642-55415-5_15.

[112] A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang. "Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online". In: SOUPS. 2016, pp. 77–96.

[113] O. A. V. Ravnås. *Frida*. 2022.

[114] K. Raynes-Goldie. "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook". In: *First Monday* 15.1 (Jan. 2010). DOI: 10.5210/fm.v15i1.2775.

[115] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". In: *Official Journal of the European Union* L 119 (May 4, 2016), pp. 1–88.

[116] K. Reitz et al. *Requests*. Version 2.28.1. June 2022.

[117] S. Sarda. *Reverse Engineering Bumble's API*. Independent Security Evaluators. Nov. 14, 2020.

[118] L. L. Sharabi. "The Enduring Effect of Internet Dating: Meeting Online and the Road to Marriage". In: *Communication Research* (2023). DOI: 10.1177/00936502221127498.

[119] C. Sheils. "Egyptian Cops Using Grindr To Hunt Gays". In: *Cairo Scene* (Aug. 31, 2014).

[120] R. Shetty, G. Grispos, and K.-K. R. Choo. "Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In)Security of Android Dating Apps". In: *IEEE Transactions on Sustainable Computing* 6.2 (2021), pp. 197–207. DOI: 10.1109/TSUSC.2017.2783858.

[121] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use". In: CHI. 2014, pp. 2347–2356. DOI: 10.1145/2556288.2557421.

[122] R. Shokri, G. Theodorakopoulos, G. Danezis, J.-P. Hubaux, and J.-Y. Le Boudec. "Quantifying Location Privacy: The Case of Sporadic Location Exposure". In: PETS. 2011, pp. 57–76. DOI: 10.1007/978-3-642-22263-4_4.

[123] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux. "Quantifying Location Privacy". In: SP. 2011, pp. 247–262. DOI: 10.1109/SP.2011.18.

[124] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec. "Protecting Location Privacy: Optimal Strategy against Localization Attacks". In: CCS. 2012, pp. 617–627. DOI: 10.1145/2382196.2382261.

[125] L. Šikšnys, J. R. Thomsen, S. Šaltenis, M. L. Yiu, and O. Andersen. "A Location Privacy Aware Friend Locator". In: *11th International Symposium on Spatial and Temporal Databases*. SSTD. 2009, pp. 405–410. DOI: 10.1007/978-3-642-02982-0_29.

[126] S. G. Smith, K. C. Basile, and M.-j. Kresnow. *The National Intimate Partner and Sexual Violence Survey: 2016/2017 Report on Stalking – Updated Release*. National Center for Injury Prevention, Control, Centers for Disease Control, and Prevention, Apr. 2022.

[127] Smith Boonchutima, Sopon Sriwattana, Rungroj Rungvimolsin, and Nattanop Palahan. "Gays Dating Applications: Information Disclosure and Sexual Behavior". In: *Journal of Health Research* 30.4 (2016), pp. 231–239. DOI: 10.14456/JHR.2016.32.

[128] N. Sriram. "Dating Data: LGBT Dating Apps, Data Privacy, and Data Security". In: *University of Illinois Journal of Law, Technology & Policy* 2020.2 (Fall 2020), pp. 507–528.

[129] J. Steinfeld. "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". In: *Index on Censorship* 49.2 (2020), pp. 101–104. DOI: 10.1177/0306422020935360.

[130] C. Stenson, A. Balcells, and M. Chen. "Burning Up Privacy on Tinder". In: *11th Symposium on Usable Privacy and Security – Posters*. 2015.

[131] M. Stoicescu and C. Rughiniş. "Perils of digital intimacy. A classification framework for privacy, security, and safety risks on dating apps". In: *23rd International Conference on Control Systems and Computer Science*. CSCS. 2021, pp. 457–462. DOI: 10.1109/CSCS52396.2021.00081.

[132] M.-V. Stoicescu, S. Matei, and R. Rughinis. "Sharing and Privacy in Dating Apps". In: *22nd International Conference on Control Systems and Computer Science*. CSCS. 2019, pp. 432–437. DOI: 10.1109/CSCS.2019.00079.

[133] G. Suarez-Tangil et al. "Automatically Dismantling Online Dating Fraud". In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 1128–1137. DOI: 10.1109/TIFS.2019.2930479.

[134] M. Tanner and S. Singh. "The Influence of Locus of Control in the Actualisation of Mobile Dating Applications Affordances to Mitigate Privacy and Security Concerns". In: *18th European, Mediterranean, and Middle Eastern Conference on Information Systems*. EMCIS. 2022, pp. 333–345. DOI: 10.1007/978-3-030-95947-0_23.

[135] H. Tanriverdi, O. Schnuck, and R. Schöffel. "Nutzer der Dating-App Lovoo können geortet werden". In: *Bayerischen Rundfunk* (Aug. 13, 2019).

[136] M. Terrovitis. "Privacy Preservation in the Dissemination of Location Data". In: *ACM SIGKDD Explorations Newsletter* 13.1 (Aug. 2011), pp. 6–18. DOI: 10.1145/2031331.2031334.

[137] L. Terveen and D. W. McDonald. "Social Matching: A Framework and Research Agenda". In: *ACM Transactions on Computer-Human Interaction* 12.3 (July 2005), pp. 401–434. DOI: 10.1145/1096737.1096740.

[138] *The Do's and Don'ts of Location Aware Apps; A Case Study*. Synack. Sept. 5, 2014.

[139] E. Timmermans and E. De Caluwé. "Development and validation of the Tinder Motives Scale (TMS)". In: *Computers in Human Behavior* 70 (2017), pp. 341–350. DOI: 10.1016/j.chb.2017.01.028.

[140] E. Toch and I. Levi. "Locality and Privacy in People-Nearby Applications". In: UbiComp. 2013, pp. 539–548. DOI: 10.1145/2493432.2493485.

[141] E. Tseng et al. "The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums". In: USENIX Security. 2020, pp. 1893–1909.

[142] G. Tyson, V. C. Perta, H. Haddadi, and M. C. Seto. "A first look at user activity on Tinder". In: *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. ASONAM. 2016, pp. 461–466. DOI: 10.1109/ASONAM.2016.7752275.

[143] C. Van De Wiele and S. T. Tong. "Breaking Boundaries: The Uses & Gratifications of Grindr". In: UbiComp. 2014, pp. 619–630. DOI: 10.1145/2632048.2636070.

[144] M. Veytsman. *How I was able to track the location of any Tinder user*. Include Security. Feb. 19, 2014.

[145] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. "An Analysis of Social Network-Based Sybil Defenses". In: *ACM SIGCOMM Computer Communication Review* 40.4 (Aug. 2010), pp. 363–374. DOI: 10.1145/1851275.1851226.

[146] A. E. Waldman. "Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities". In: *Law & Social Inquiry* 44.4 (2019), pp. 987–1018. DOI: 10.1017/lsi.2018.29.

[147] A. E. Waldman. "Navigating Privacy on Gay-Oriented Mobile Dating Applications". In: *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. June 2021, pp. 369–381. DOI: 10.1108/978-1-83982-848-520211027.

[148] G. Wang et al. "Whispers in the Dark: Analysis of an Anonymous Social Network". In: IMC. 2014, pp. 137–150. DOI: 10.1145/2663716.2663728.

[149] J. Wang, H. Cheng, M. Xue, and X. Hei. "Revisiting Localization Attacks in Mobile App People-Nearby Services". In: SpaCCS. 2017, pp. 17–30. DOI: 10.1007/978-3-319-72389-1_2.

[150] M. Warner, A. Gutmann, M. A. Sasse, and A. Blandford. "Privacy Unraveling Around Explicit HIV Status Disclosure Fields in the Online Geosocial Hookup App Grindr". In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018). DOI: 10.1145/3274450.

[151] M. Warner, J. F. Maestre, J. Gibbs, C.-F. Chung, and A. Blandford. "Signal Appropriation of Explicit HIV Status Disclosure Fields in Sex-Social Apps Used by Gay and Bisexual Men". In: CHI. 2019, pp. 1–15. DOI: 10.1145/3290605.3300922.

[152] M. Wei, E. Zeng, T. Kohno, and F. Roesner. "Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships". In: SOUPS. 2022, pp. 447–462.

[153] E. Weltevrede and F. Jansen. "Infrastructures of Intimate Data: Mapping the Inbound and Outbound Data Flows of Dating Apps". In: *Computational Culture* (7 Oct. 2019).

[154] M. Xue et al. "You Can Yak but You Can't Hide: Localizing Anonymous Social Network Users". In: IMC. 2016, pp. 25–31. DOI: 10.1145/2987443.2987449.

[155] E. Yalon, I. Shkedy, and P. Silva, eds. *OWASP API Security Project*. The OWASP Foundation. 2019.

[156] Z. Yang et al. "Uncovering Social Network Sybils in the Wild". In: *ACM Transactions on Knowledge Discovery from Data* 8.1 (Feb. 2014). DOI: 10.1145/2556609.

[157] F. Zhao et al. "You Are Where You App: An Assessment on Location Privacy of Social Applications". In: *29th IEEE International Symposium on Software Reliability Engineering*. ISSRE. 2018, pp. 236–247. DOI: 10.1109/ISSRE.2018.00033.

[158] S. Zhao et al. "Exploiting Proximity-Based Mobile Apps for Large-Scale Location Privacy Probing". In: *Security and Communication Networks* 2018 (2018), pp. 1–22. DOI: 10.1155/2018/3182402.

[159] X. Zhao, L. Li, and G. Xue. "Checking in without worries: Location privacy in location based social networks". In: INFOCOM. 2013, pp. 3003–3011. DOI: 10.1109/INFCOM.2013.6567112.

[160] I. Žliobaitė and B. Custers. "Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models". In: *Artificial Intelligence and Law* 24.2 (May 2016), pp. 183–201. DOI: 10.1007/s10506-016-9182-5.

A LBD App Versions

Table 7 lists the version numbers used for testing our LBD apps in scope, as of January 2023. For web apps, we search a version number on the web page or in its HTML source; we mark the version as 'unknown' if we do not find such a version number. For mobile apps, we use the version number of the APK downloaded from the Google Play Store.

Table 7: Tested version numbers of the LBD apps.

Name	Owner	Web app	Mobile app
Tinder	Match Group	4.3.1	14.1.0
Badoo	Bumble Inc.	1.0.00.28116	5.304.1
POF	Match Group	2.8.0-b9961	4.85.1.1510401
MeetMe	The Meet Group	5.44.3	14.49.0.3795
Tagged	The Meet Group	unknown	9.58.0
Grindr	Grindr LLC	N/A	9.0.0
Tantan	Hello Group Inc	N/A	5.6.1.4
Jaumo	Joyride GmbH	N/A	202301.1.0
LOVOO	The Meet Group	unknown	141.1
happn	happn SAS	2022.9.1	26.29.1
Bumble	Bumble Inc.	1.0.0.28116	5.300.0
Hinge	Match Group	N/A	9.13.1
Hily	Hily Corp.	N/A	3.6.9
OkCupid	Match Group	unknown	73.1.0
Meetic	Match Group	unknown	5.86.4