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

USENIX Security, 16 August 2024

sky news

Finding love online: More than half of couples set to meet via the internet

Wednesday 27 November 2019 03:42, UK

CNBC

How singles are meeting up on dating apps like Tinder, Bumble, Hinge during coronavirus pandemic

PUBLISHED TUE, MAR 24 2020•12:14 PM EDT | UPDATED TUE, MAR 31 2020•10:42 AM EDT

Cameron Costa
@CAMERONCOSTANY

FORTUNE

Activity on dating apps has surged during the pandemic

BY FORTUNE EDITORS

February 12, 2021 at 5:30 PM GMT+1

Bloomberg

A Record Number of Americans Used Dating Apps in July

By Akayla Gardner +Follow

3 augustus 2021 om 19:15 CEST

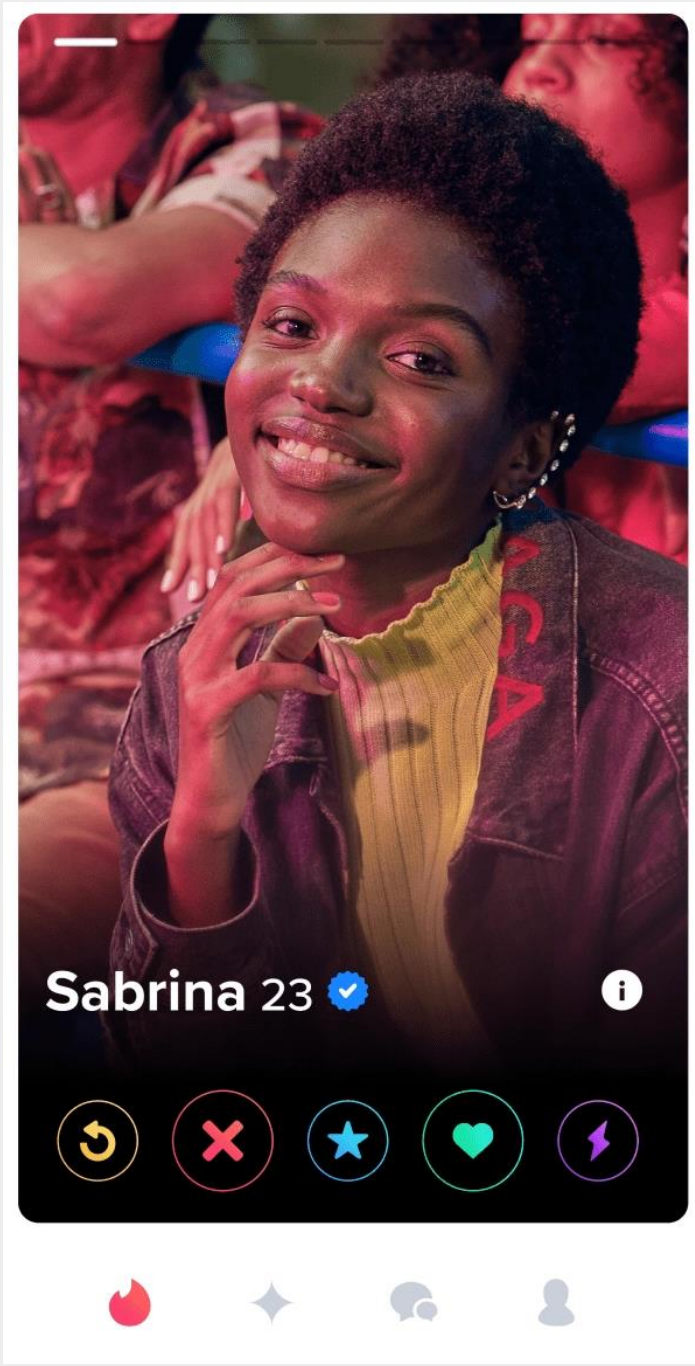
BBC

Tinder: More pay for dating app despite cost-of-living crisis

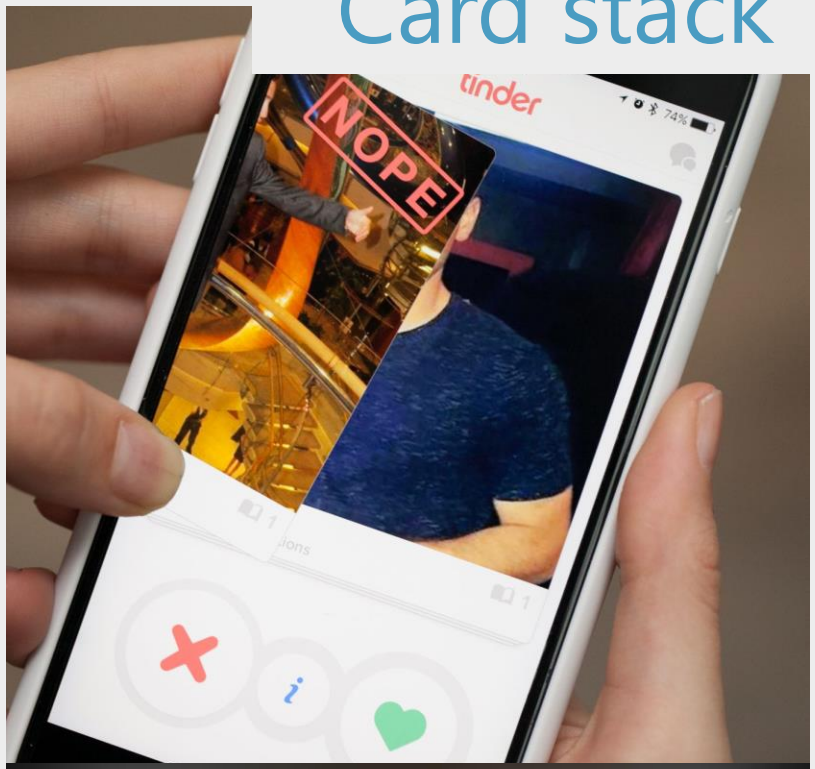
2 November 2022

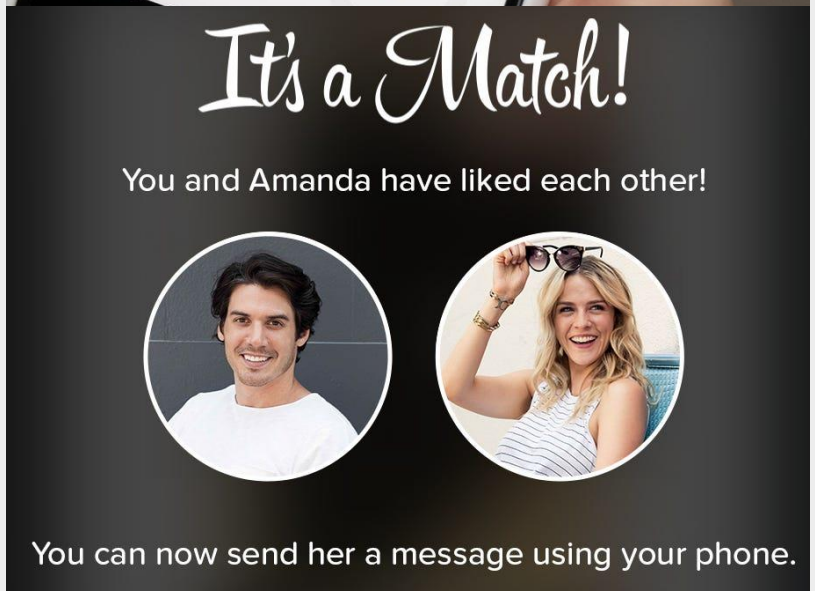
By Noor Nanji

Business reporter, BBC News

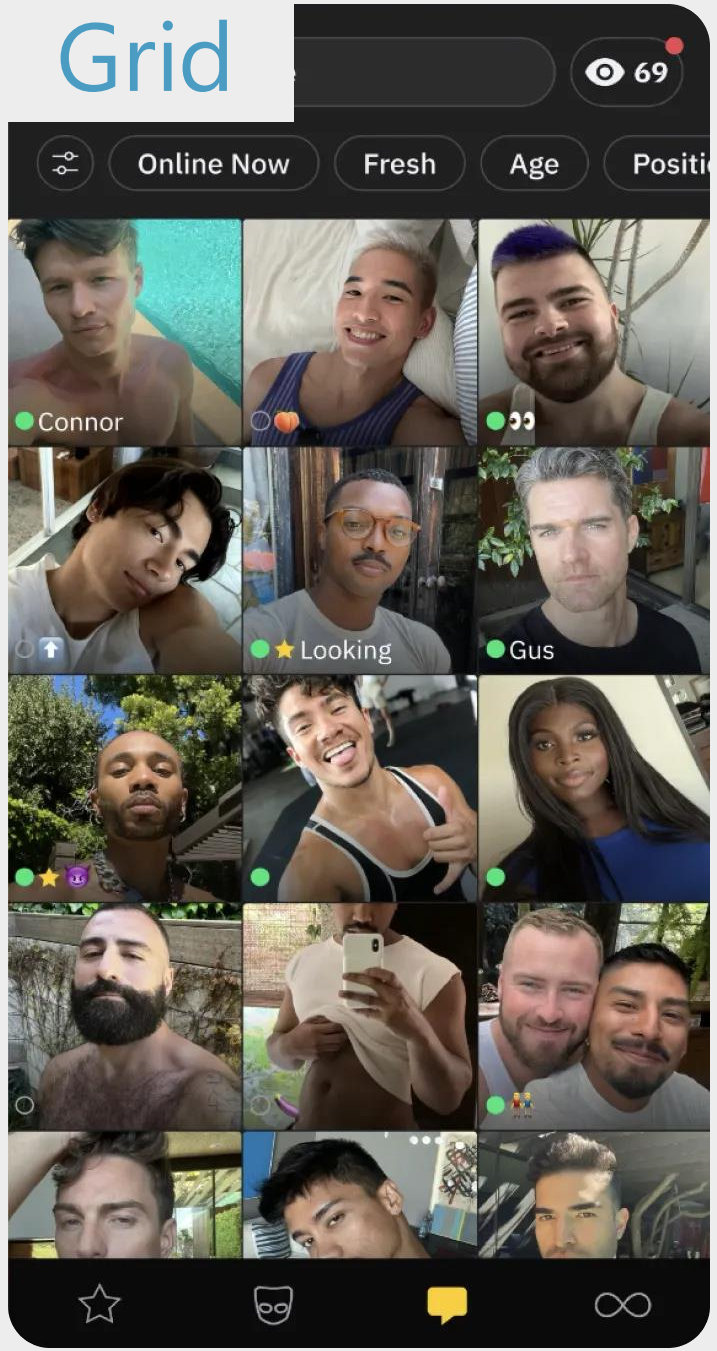


Card stack





Grid



LBD apps elicit **peculiar privacy behavior**

- Users **willingly** share
  highly personal and sensitive data
  (including **exact locations**)
- Users **expect** others to share data
- Users share data with **strangers**

Sufficient (self-)disclosure ↔ Maintaining privacy

What are the **privacy risks** in sharing personal data with **other users**?

Social privacy (↔ institutional privacy)

Our adversary focuses on collecting *personal* data about *one or more other users* of the LBD app using only *client-side* interactions as a *regular* user

Adversaries can have diverse **malicious intentions**

ABC NEWS

A quick scan of your dating profile could provide a scammer with exactly what they want. Here's how to keep your personal details safe

yahoo!news

Rape, stalking and blackmail: the dark side of dating apps revealed

INDEPENDENT

News > World > Middle East

Egypt police 'using dating apps' to find and imprison LGBT+ people

What is the extent of

data exposure & leaks

in **LBD apps**?

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

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

Personal data

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

Sensitive data (GDPR art. 9)

Other has liked you
Other has disliked you
Popularity score
Number of likes/dislikes

Other was recently active
Last activity time
Account creation time

Relationship type sought
Wanting children
Filters

profiles per API request
- Card stack
- Grid

Permanent profile access
See profiles while paused

App usage data

Three modes of data exposure & leaks

UI Exposure
readily visible
in the *UI*

***Intended** sharing*

Three modes of data exposure & leaks

UI Exposure
readily visible in the *UI*

Traffic leak
automatically sent in *API* network traffic

Exfiltration leak
sent after *altering* traffic or behavior

***Intended** sharing*

***Inadvertent** sharing*

Highlights across 15 LBD apps

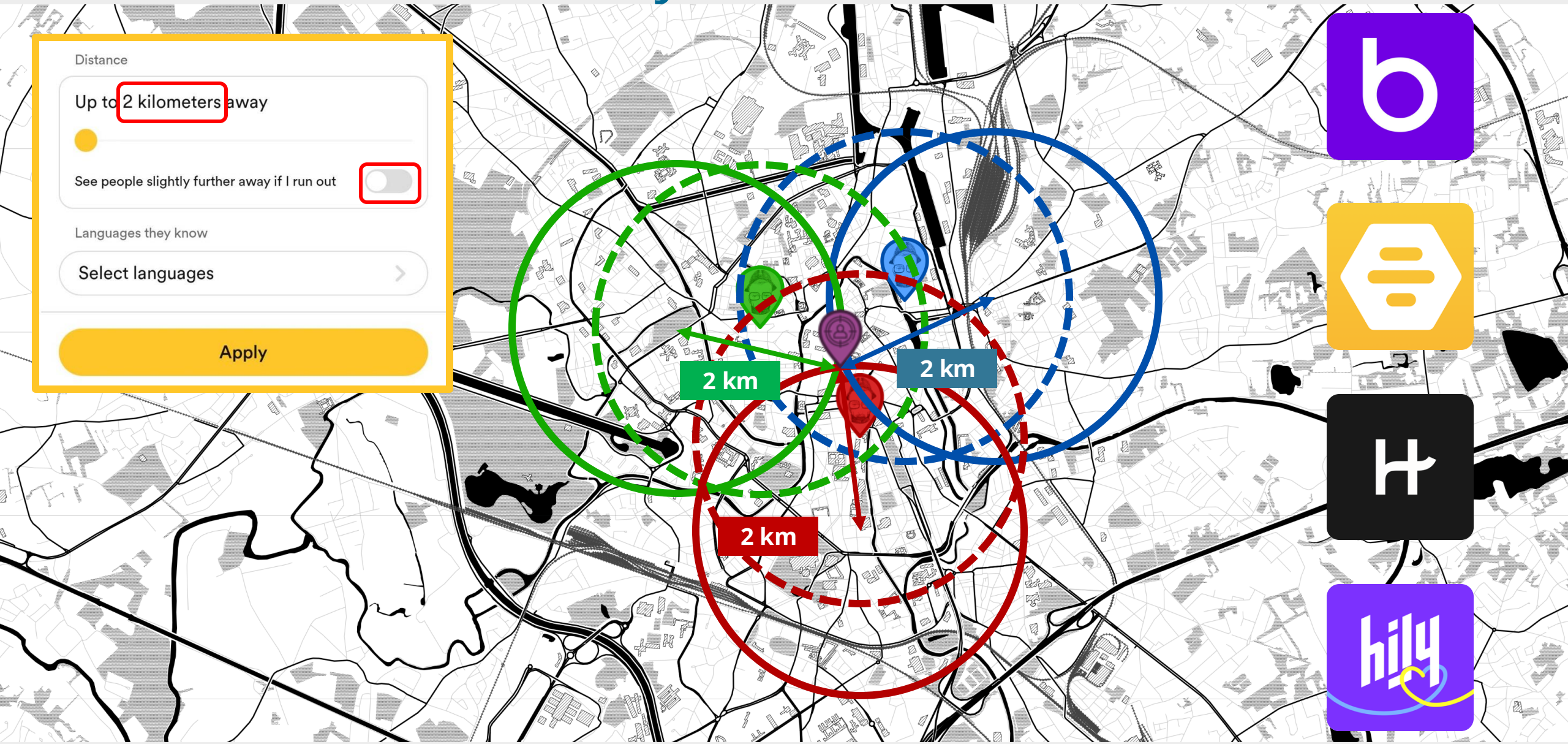
Highlights across 15 LBD apps

- ***Intended sharing:*** broad differences: **9** ↔ **23** fields
  - *Grindr:* **13** fields *but* very sensitive (HIV status, sexual preference)
    - ▶ *seen as beneficial*
    - ▶ *all fields optional > risk of stealthy adversary*
  - *POF, Hily, Badoo:* **requiring** fields optional in other apps
    - ▶ *others might still expect disclosure, reducing agency*

Highlights across 15 LBD apps

- ***Intended sharing:*** broad differences: **9** ↔ **23** fields
  - *Grindr:* **13** fields *but* very sensitive (HIV status, sexual preference)
    - ▶ *seen as beneficial*
    - ▶ *all fields optional > risk of stealthy adversary*
  - *POF, Hily, Badoo:* **requiring** fields optional in other apps
    - ▶ *others might still expect disclosure, reducing agency*
- ***Inadvertent sharing:*** **APIs** leak data for all apps
  - *All apps:* **99 leaks**: app usage data, gender, sexual orientation
  - *All apps:* **reciprocity** nearly always fails (hidden attributes/profiles)
  - *6 apps:* leak exact user **locations** through trilateration

Trilateration: Proximity Oracle

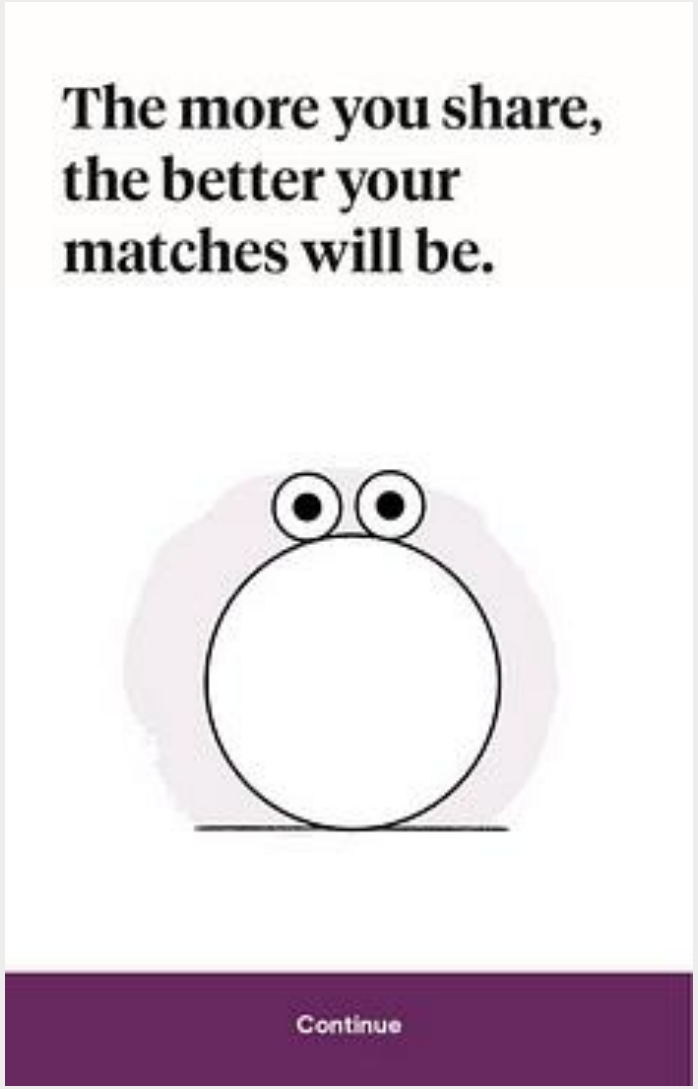


Bulk **account creation** enables large-scale, long-term, stealthy tracking

Privacy policies of LBD apps fall short in giving control

LBD apps should give users ***control, choice, agency***

- Avoid nudging users to share data
- Inform users properly about sharing
- Hide profile data by default
  - Make data sharing a conscious decision
- Request location update explicitly
  - Give option to share approximate location



LBD apps should ***protect*** user data

- Fix inadvertent **API** leaks
  - Match UI and API: avoid unnecessary extra data in API responses
- Prevent **location** inference
  - Implement solutions such as spatial cloaking *(rounding coordinates)*
- Avoid having data in the first place *(**data minimization**)*
- ***Tinder*** has fewer sensitive fields, rounds coordinates

Conclusion

- LBD apps harbor a **sensitive privacy context**
  - *Users feel compelled to share data, but **social privacy** is important*
- (Intended) data **exposure** varies significantly between apps
- **Inadvertent leaks/inference** reveal hidden data/locations
  - ***APIs** are an important cause of privacy breaches*
- Apps put **burden** of protecting privacy **on users**
  - *Need for **technical audits** of UI and API, compared with privacy policy*

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

victor.lepochat@kuleuven.be
https://lepoch.at/ @VictorLePochat

KU LEUVEN DistriNet Cyber Security Flanders

Full paper: