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

KU LEUVEN DistriNet Cyber Security Flanders

black hat USA 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

BBC

Dating apps found 'leaking' location data

19 January 2015

Forbes

Dating App Insiders Remain 'Highly Concerned' About User Security, According To A Recent Survey

Mark Travers Contributor

Jul 15, 2021, 11:10am EDT

INDEPENDENT

News > World > Middle East

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

Victims thrown into jail and tortured, claims HRW

Gemma Fox Deputy International Editor • Thursday 01 October 2020 17:05

The Washington Post
Democracy Dies in Darkness

'Tinder Swindler' con artist, subject of new Netflix documentary, banned from dating app

Tinder has also issued new guidelines to protect users from would-be romance scammers

By Jennifer Hassan

Updated February 7, 2022 at 12:09 p.m. EST | Published February 6, 2022 at 10:32 a.m. EST

yahoo!news

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

Joanna Morris

3 July 2022 · 3-min read

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

By Dannielle Maguire

Posted Wed 4 Jan 2023 at 7:41pm, updated Thu 5 Jan 2023 at 12:48am

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

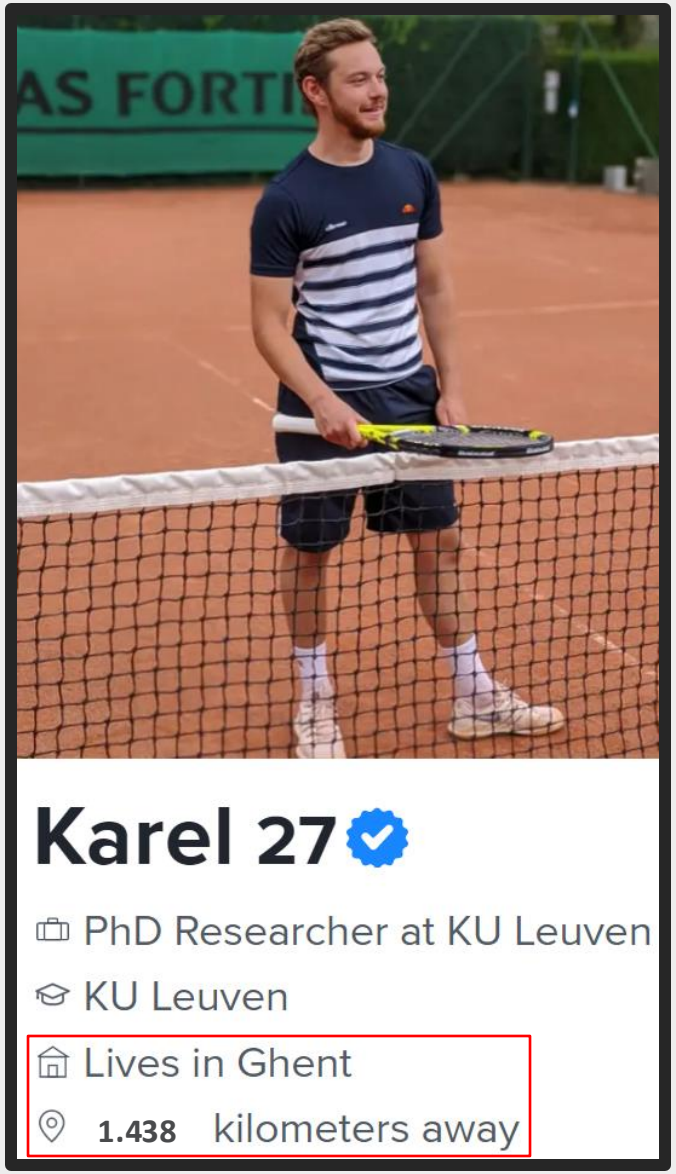
10M

OKCUPID

10M

MEETIC

10M


AS FORTI
Karel 27
PhD Researcher at KU Leuven
KU Leuven
Lives in Ghent
1.438 kilometers away

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

Adversary 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

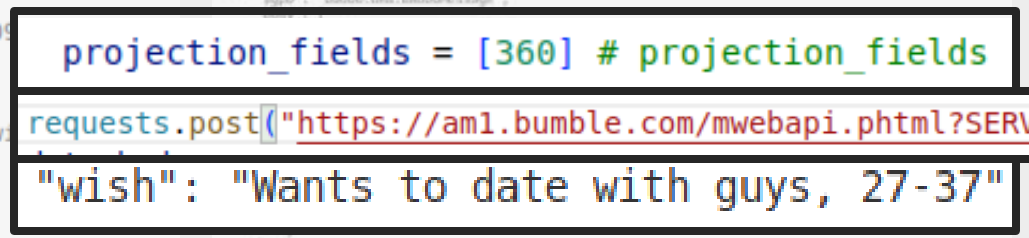
in **LBD apps**?

Data exposure & leaks

UI Exposure
readily visible
in the *UI*

***Intended** sharing*

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*

Private Data Leaks

- 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

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

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

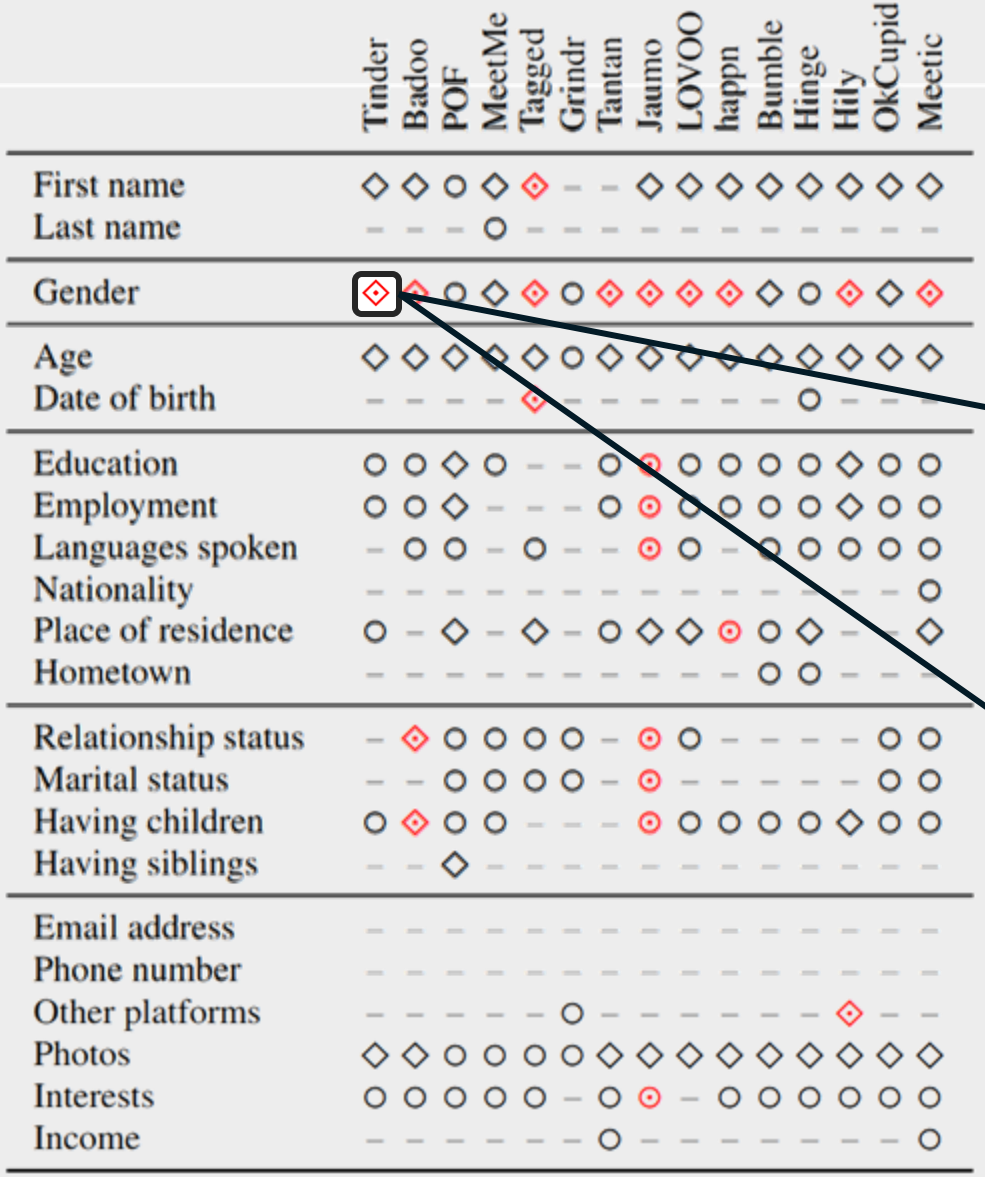
Permanent profile access
See profiles while paused

App usage data

APIs leak data for **all** apps

99 leaks in total

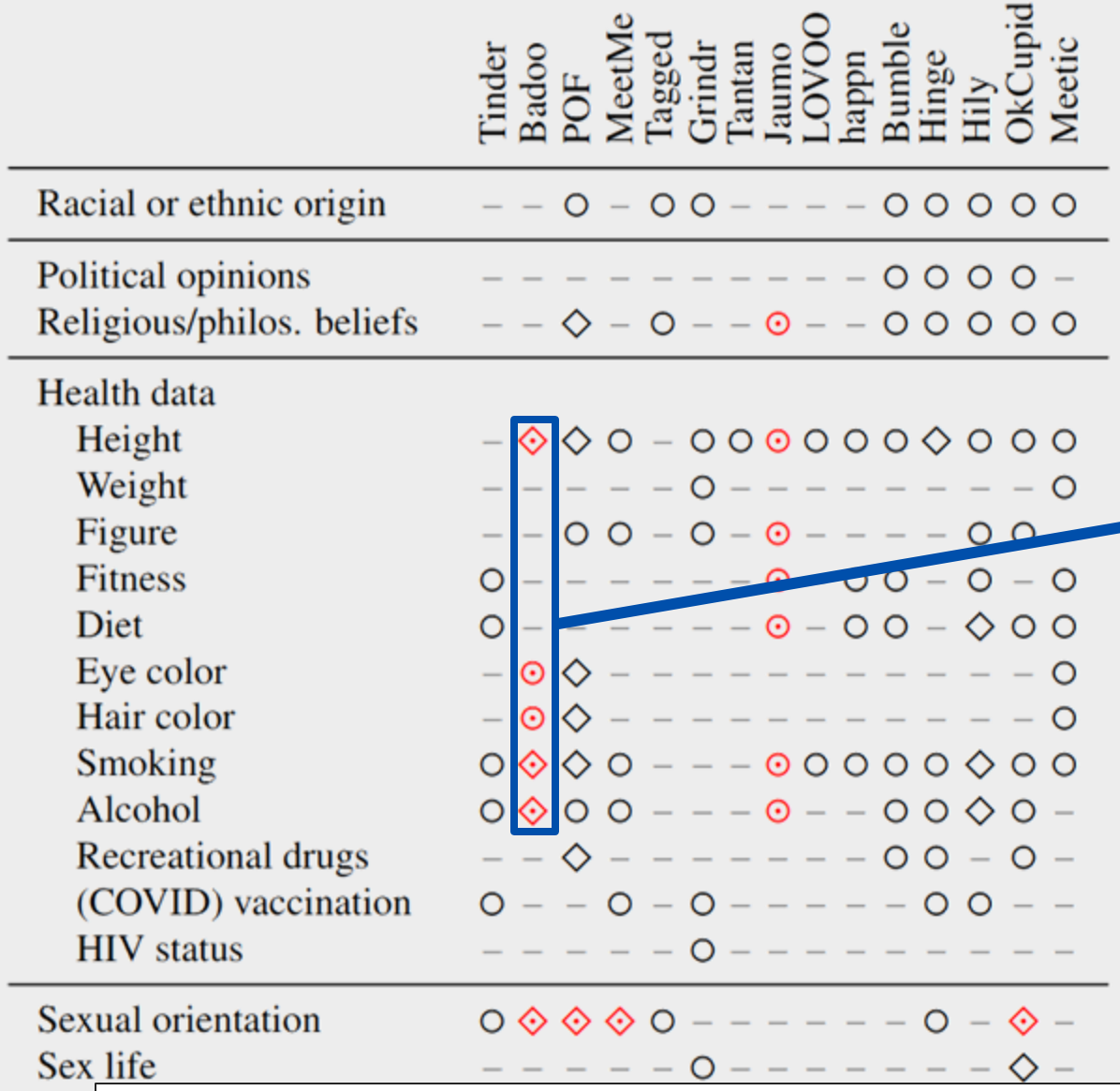
Personal Data Leaks

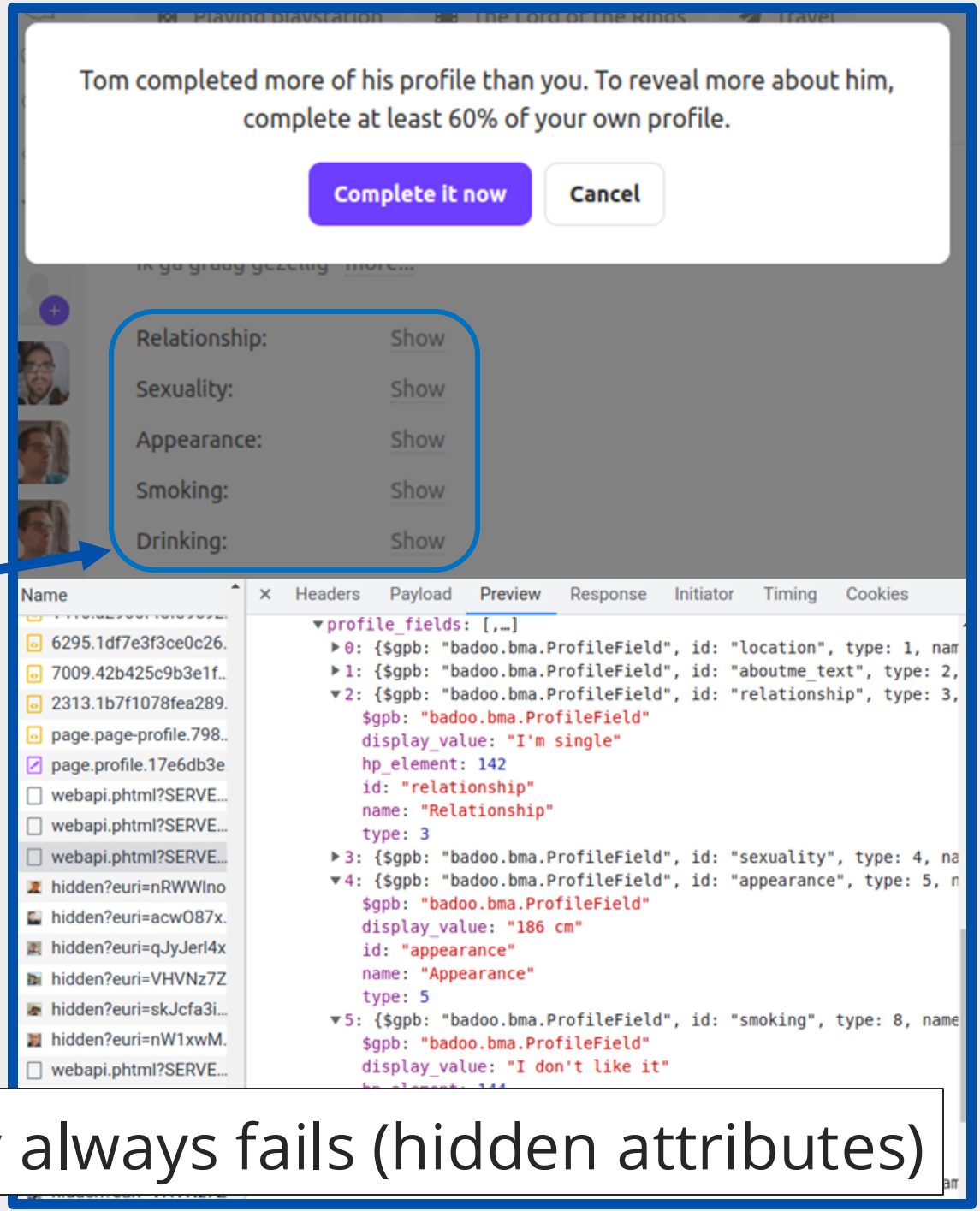


Tinder: leak of **non-binary gender**


```
▼user: {_id: "63a567b59d502c0100626483", badges: [],…}
    badges: []
    bio: "Academic research account, please ignore. We only colle
    birth_date: "1994-01-21T08:21:29.418Z"
    custom_gender: "Gender non-conform"
    gender: -1
    is_traveling: false
    jobs: []
    name: "Stijn"
    online_now: true
  ▶ photos: [{id: "1c6784d8-ee4a-4798-800f-5431b23809c3",…}]
    recently_active: true
    schools: []
  ▶ sexual_orientations: [{id: "ques", name: "Nog twijfelend"}]
    show_gender_on_profile: false
    _id: "63a567b59d502c0100626483"
▶ meta: {status: 200}
```

Sensitive Data Leaks





All apps: **data reciprocity** nearly always fails (hidden attributes)

App Usage Data Leaks

	Tinder	Badoo	POF	MeetMe	Tagged	Grindr	Tantan	Jaumo	LOVOO	happn	Bumble	Hinge	Hily	OkCupid	Meetic
Other has liked you	–	◇	◇	◇	◇	–	◇	◇	–	◇	◇	◇	◇	◇	◇
Other has disliked you	–														
Popularity score	–														
Number of likes/dislikes	–	◈	–	–	–	–	◇	–	–	–	–	–	–	–	–
Relationship type sought	◇	○	◇	◇	○	○	–	○	◇	○	○	○	◇	◇	○
Wanting children	○	◇	○	–	–	–	–	⊙	–	○	○	○	◇	○	○
Filters	–	◇	◇	◇	–	–	◇	◇	–	–	◈				
# profiles per API request															
Card stack	10	20	69	1	20	–	5	10	30	20	10	2			
Grid	–	20	42	30	24	100	–	–	40	–	–	1			
Permanent profile access	◇	◇	◇	◇	◇	◇	◇	◇	◇	◇	◇	◇			
See profiles while paused	◇	–	◇	–	◇	–	–	◇	–	◇	–	◇			

```
129  projection_fields = [360] # projection_fields
130
131  user_id = "zAgEACjE3NjIwMjM0MzQI4UEWZwAAAAAgeiAbCr4VcNwO1ugCQXJoKL
132
133  body = '{"$gpb":"badoo.bma.BadooMessage","body":[{"message_type":4
     "projection":' + str(projection_fields).replace(' ','') + ',"reque
     "request_albums":[{"person_id":"'+user_id+'","album_type":2,"offse
     "client_source":10}}],"message_id":14,"message_type":403,"version"
134
135  r = requests.post("https://am1.bumble.com/mwebapi.phtml?SERVER_GET
136      data=body,
137      headers={
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

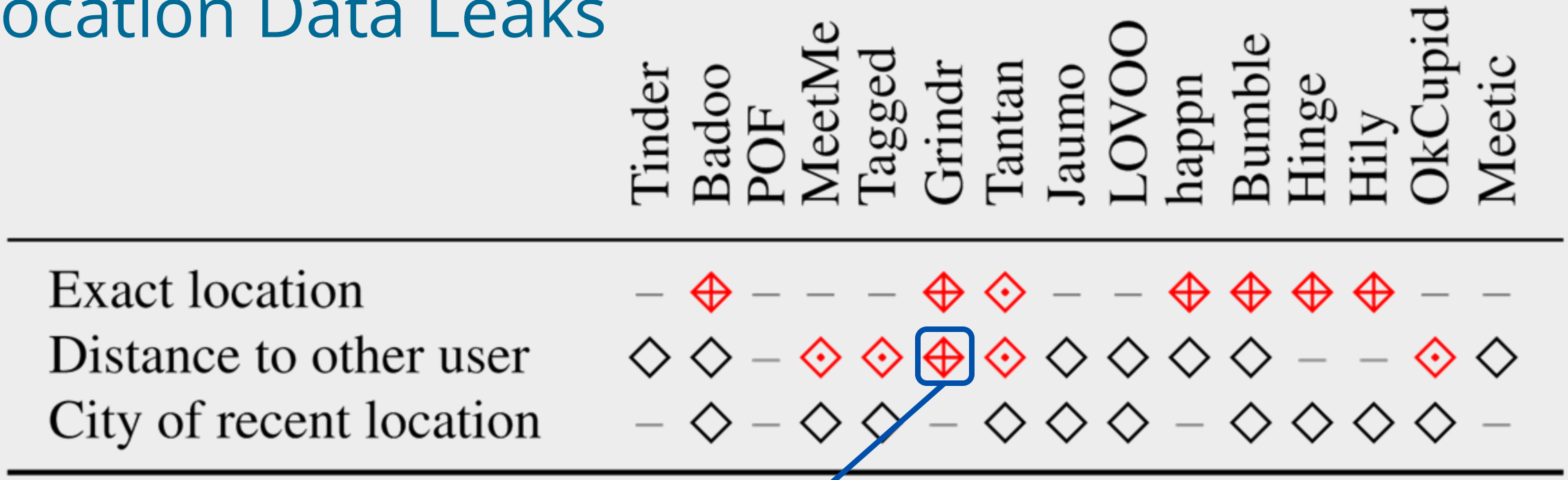
Badoo, Bumble: **exfiltration** leaks of activity, filters

All apps: **data reciprocity** nearly always fails (hidden profiles)

```
            "$gpb": "badoo.bma.MessageBody",
            "message_type": 404,
            "user": {
                "$gpb": "badoo.bma.User",
                "access_level": 10,
                "client_source": 10,
                "projection": [
                    360
                ],
                "user_id": "zAgEACjE3NjIwMjM0MzQI4UEWZwAAAAAgeiAbCr4VcNwO1ug
                "wish": "Wants to date with guys, 27-37"
            }
        }
    ],
```

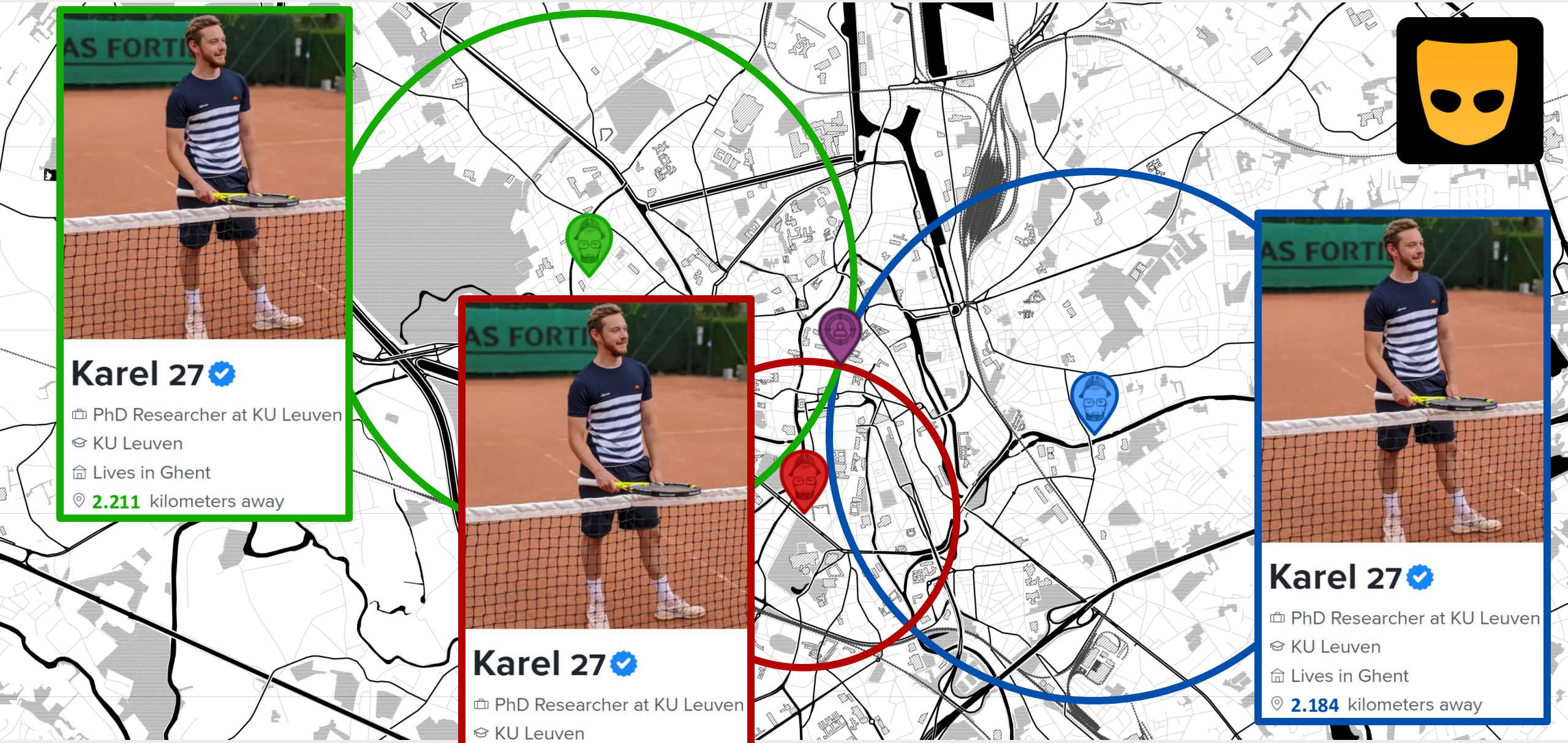
All except OkCupid: fetch **multiple profiles** at once

Location Data Leaks

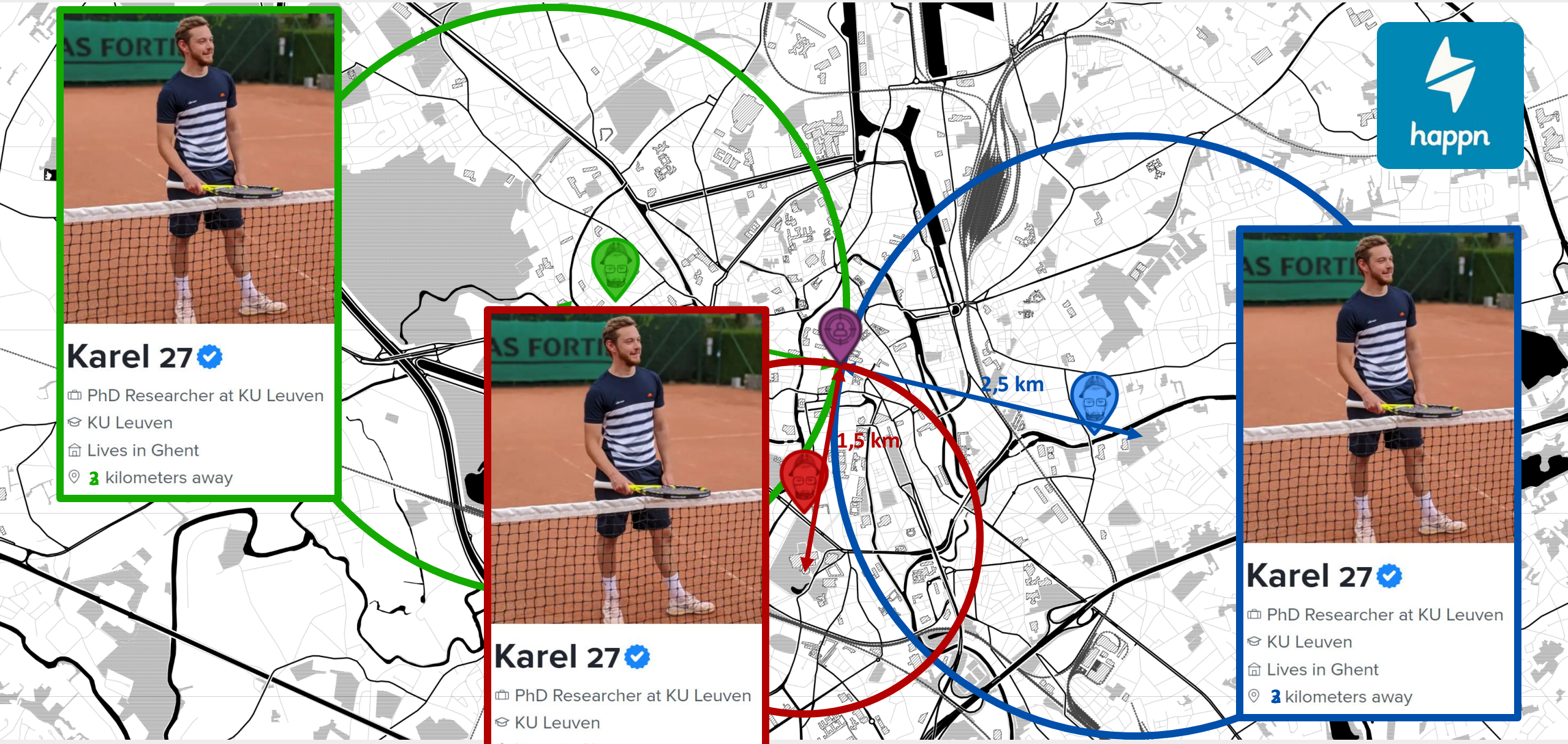



```python
def get_nearby(self, geohash, min_age=None, max_age=None, search_after_profile_id=None, search_after_distance=None):
    url = f"https://grindr.mobi/v8/search?nearbyGeoHash={geohash}&online=false"
    if min_age is not None:
        url += "&ageMinimum=" + str(min_age)
    if max_age is not None:
        url += "&ageMaximum=" + str(max_age)
    if search_after_profile_id is not None:
        url += "&searchAfterProfileId=" + str(search_after_profile_id)
    if search_after_distance is not None:
        url += "&searchAfterDistance=" + str(search_after_distance)
    url += "&photoOnly=false&faceOnly=false&notRecentlyChatted=false&profileTags=&fresh=false&freeFilter=false&insertable=false"

    response = self.session.get(url)

    assert response.status_code == 200

    return response.json()
```

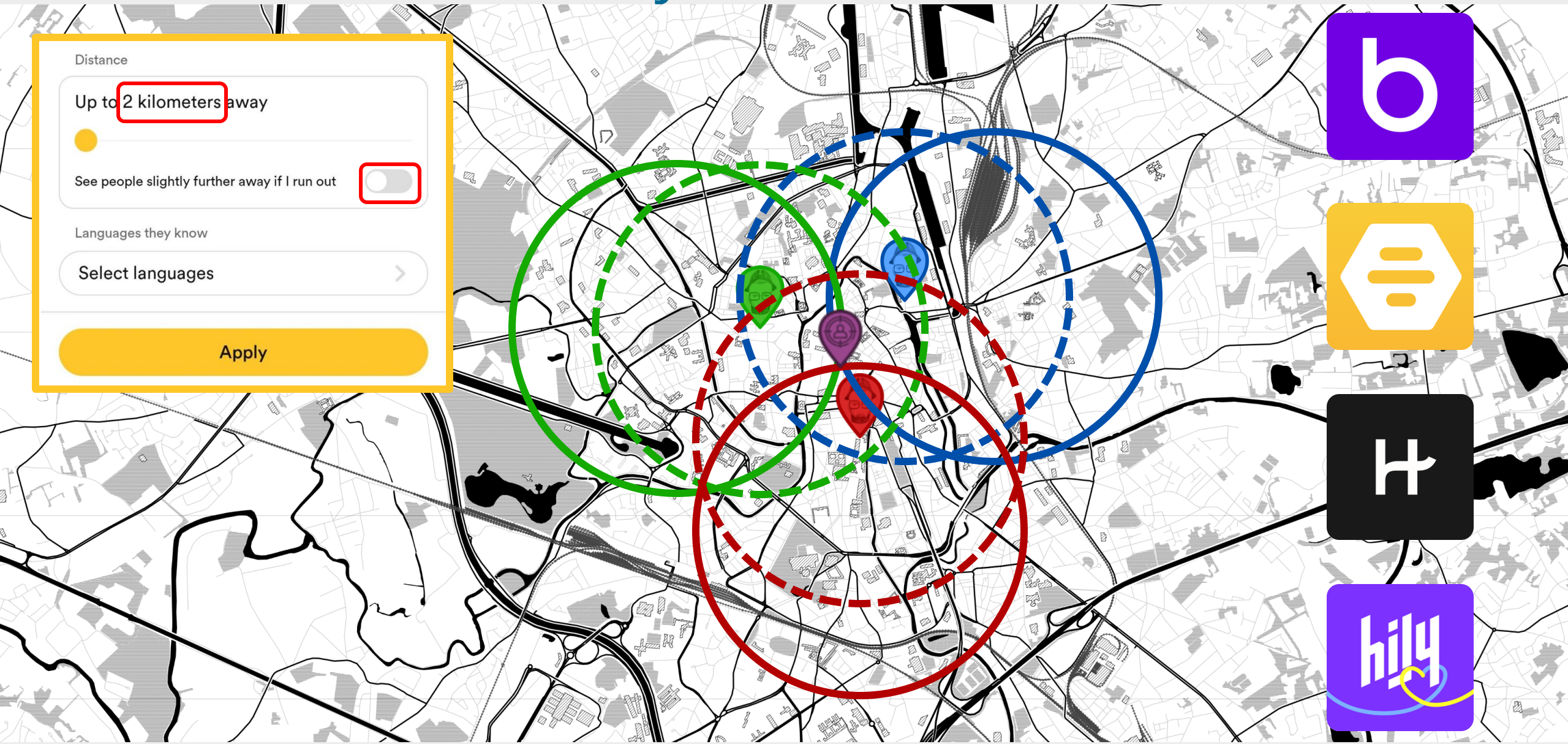
Trilateration: Exact Distance



Trilateration: Rounded Distance



Trilateration: Proximity Oracle



Bulk **account creation** accelerates stealthy stalking

- The adversary requires an **account** to browse profiles

  → This may ***expose*** the adversary to

  - the platform (/law enforcement) → *anonymous*
  - other users → *hidden*

Bulk **account creation** accelerates stealthy stalking

- The adversary requires an **account** to browse profiles

  → This may ***expose*** the adversary to

  - the platform (/law enforcement) → *anonymous*
  - other users → *hidden*

- How **easily** and **stealthily** can adversaries gather data?

Security measures for account creation

(also friction & forced sharing for legitimate users!)

Security of the **account creation** process

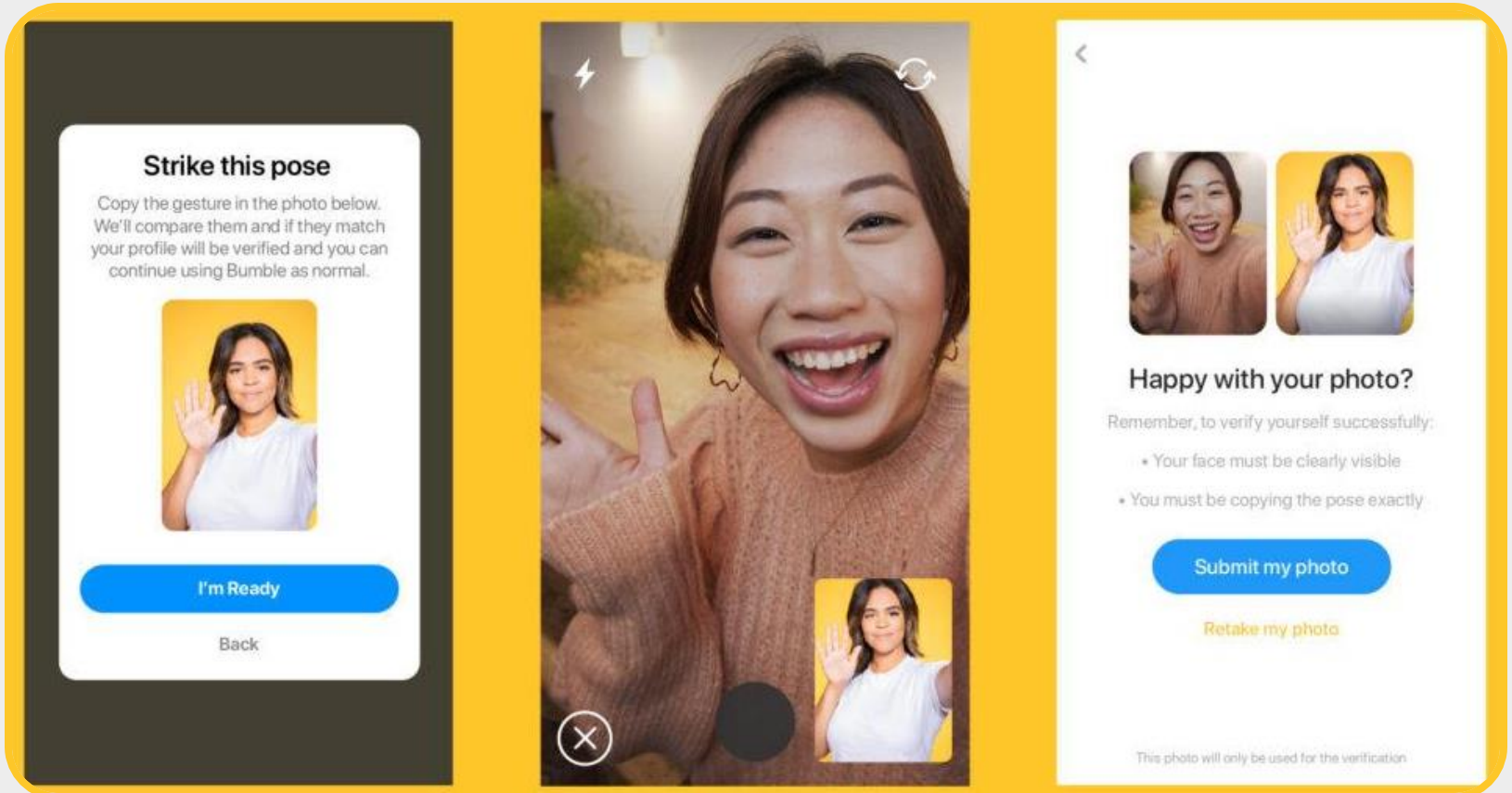
- **Requirements** for account setup
  - Email (11/15) — *Easy to acquire*
  - Valid phone number (8/15) — *Higher barrier, esp. anonymously*
  - Real profile data (8/15) — *Never verified*

- *Stealth*: empty profile (Grindr); hidden profile (Hinge)
- *Anonymity*: only email (MeetMe/Tagged)

Security of the **account creation** process

- Photo (12/15)
- Face photo (11/15)
- Face verification (13/15)

- Only mandatory on Bumble
- Profile badge = trust



Privacy policies of LBD apps fall short

- Legal basis for processing of sensitive data: consent
  - Sensitive data is stated to be optional *(sexual orientation?)*
- Location sharing options are insufficiently clear
  - 12 apps function without location permission
  - Grindr warns about location inference
- Partially private profile may require paid subscription
- **Burden to protect data is shifted to users**
  - 7 apps warn about sharing data with other users

Functionality and *privacy* experience **tension**

Sufficient (self-)disclosure ↔ Maintaining privacy

- *Users **want** data*: filter on desired traits, search more info, increase trust, improve safety feeling
- *Users **provide** data:* more success, protective disclosure; expectation, nudging, defaulting, and pressure to disclose

Sharing data is expected, not concerning, even beneficial

Functionality and *privacy* experience **tension**

Sufficient (self-)disclosure ↔ **Maintaining privacy**

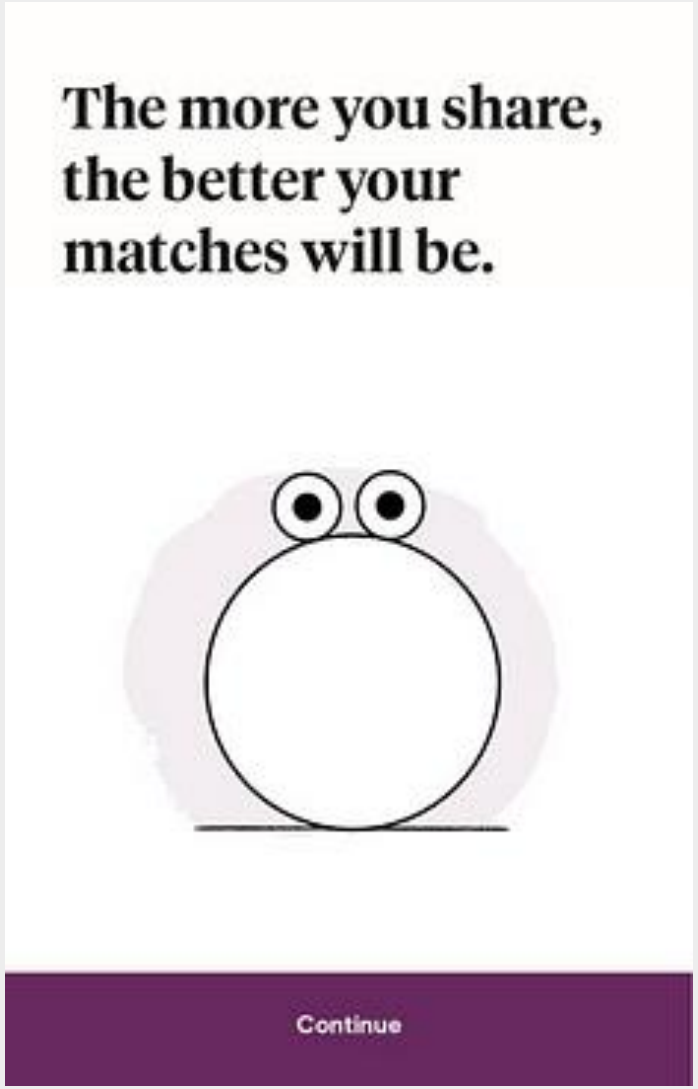
- *Users **care** about social privacy*: limit or falsify disclosure
- *Certain populations are at **higher risk**:*

  women: stalking/harassment; LGBTQ: outing/prosecution

Online dating is a sensitive context with genuine risks

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
  - Only show profile to verified users
- Request location update explicitly
  - Give option to share approximate location



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

- Fix inadvertent API leaks *(OWASP API Security Top 10)*
  - Limit exposure of/by API endpoints
  - Enforce proper access control *(least privilege)*
  - Match UI and API: avoid unnecessary extra data in API responses
- Prevent location inference
  - Account for simple *(trilateration)* and advanced *(stats)* techniques
  - Implement solutions such as spatial cloaking *(rounding coordinates)*
  - Consider user needs: does high accuracy matter?

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

- Prevent mass data gathering *(account creation, stealth)*
  - Requiring phone number, face verification *(deepfakes)*
  - Rate limiting, detecting fake requests *(client-side signatures)* /locations
  - *Just annoying the adversary, and increasing friction for legit users?*
- Avoid having data in the first place *(data minimization)*
  - *Tinder* has fewer sensitive data fields, deploys rounding coordinates

If you do not have data, you cannot leak it

Responsible disclosure

- 12 out of 15 apps **acknowledged** receipt
- 9 engaged in substantial **discussion** & deployed **fixes**
  - All location leaks have been fixed
- *Security vulnerability* vs. *privacy leak*
  - Access control bugs, improper filtering, hidden parameters, …

"As for the data in the API responses, this is not private information"

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*
- Privacy policies fall short – Apps put **burden on users**
  - *Need for **technical audits** of UI and API, compared with privacy policy*

Black Hat Sound Bytes

1. **Think beyond** the typical “hacker”
2. **API hardening** is crucial
3. **Data minimization** reduces leaks

Swipe Left for Identity Theft

An Analysis of User Data Privacy Risks on Location-based Dating Apps

kareldhondt@outlook.com
victorlepochat@gmail.com

KU LEUVEN DistriNet Cyber Security Flanders

Full paper: