# Is your OSM App spying on you?

State of the Map 2019, Heidelberg
Thomas Skowron

Disclaimers ahead

## Disclaimer I

I am not a professional security researcher.
I just know some tools and am curious.

# Disclaimer II

I am not a very privacy oriented person.
I like it when products can be made in a
privacy-preserving manner though.

# Disclaimer III

I am not saying every behaviour I will mention is bad.

*”I love using OpenStreetMap*
*because I don’t want to*
*give my data to X“*

People have expectations

But: We do not control
„the whole stack“

# “I only use openstreetmap.org“

nominatim.openstreetmap.org

graphhopper.com

gravatar.com

routing.openstreetmap.de

tile.openstreetmap.org

piwik.openstreetmap.org

*your OS’ location service*

# Privacy Policies

# Varying degrees of private

*IP addresses stored […] are shortened to two bytes and detailed usage information is retained for 180 days.*

*Every API request is stored. We save the associated information (request body and headers, IP, time) for a maximum of 5 weeks.*

*[…] we collect information that web browsers, mobile devices, and servers typically make available, such as the browser type, IP address, unique device identifiers, language preference, referring site, the date and time of access, operating system, and mobile network information*

Some third-parties don’t even say why they store the data

Some make an effort about their third-party providers

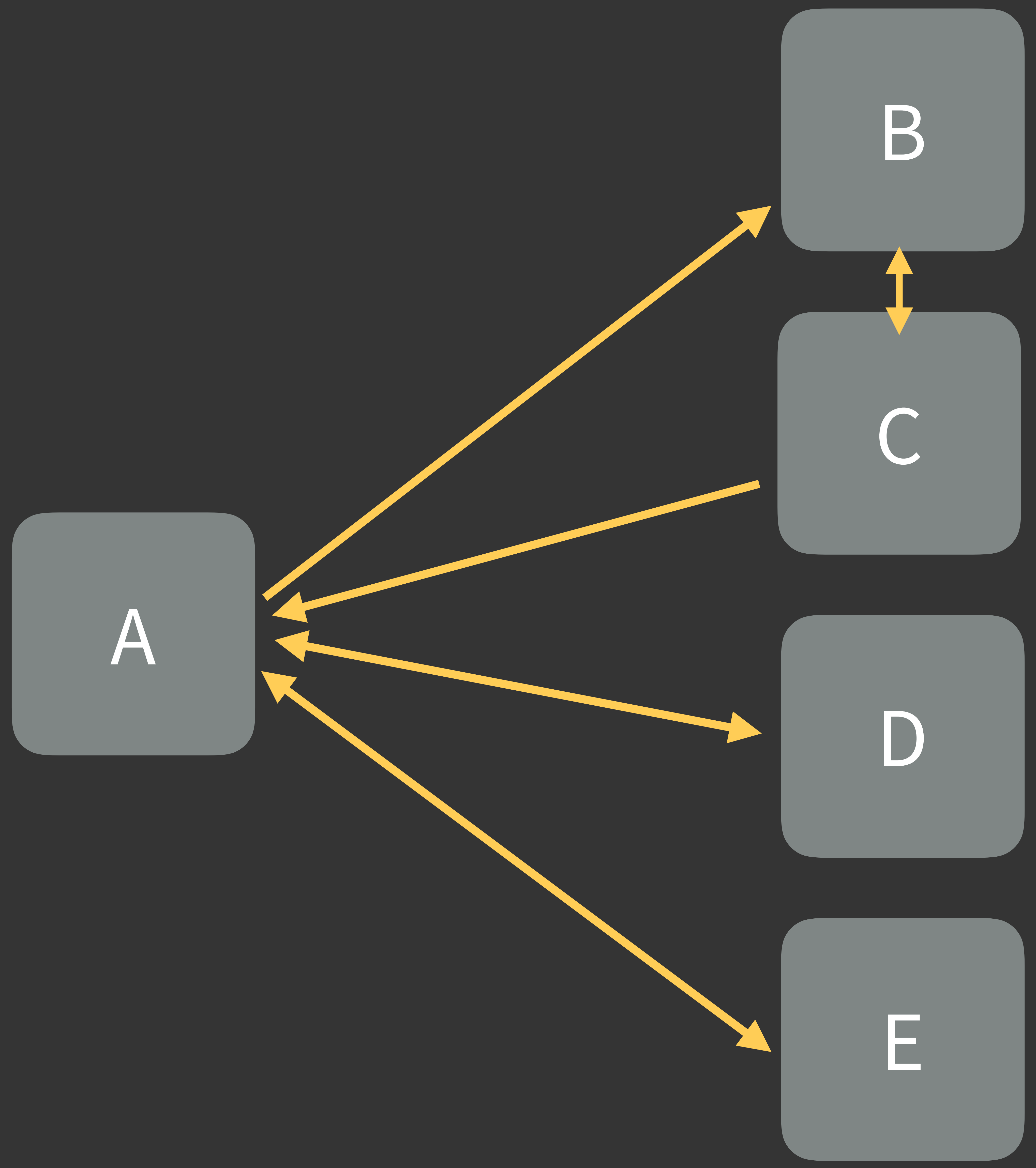
# Risk assessment

# It’s your location data

Your current location

Your usual location(s)

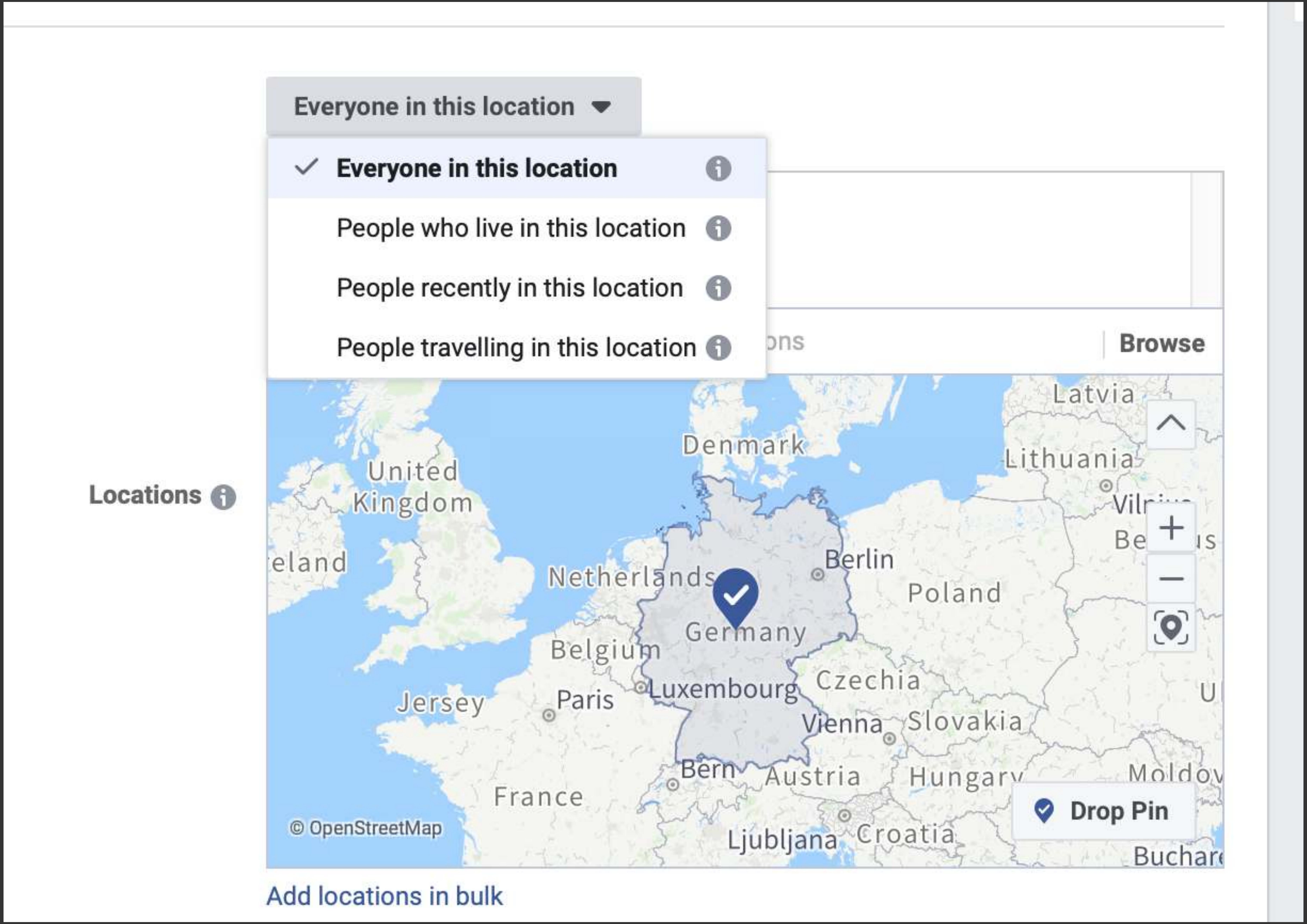
```
> 50.88349/7.06657 to 50.93754/6.96146
> 50.93754/6.96146 to 49.01071/8.38718
> 49.01071/8.38718 to 50.88349/7.06657
> 50.88349/7.06657 to 49.01071/8.38718
> 49.01071/8.38718 to 50.88349/7.06657
> 50.88349/7.06657 to 49.41659/8.67051
> 49.41659/8.67051 to 50.88349/7.06657
> A to B
> B to C
> C to A
> A to D
> D to A
> A to E
> E to A
```



But who will make such an effort?

Clearly not people like operators of OSM infrastructure

But companies that focus on selling ads.
Location based ads.



Locations

Everyone in this location

✓ Everyone in this location

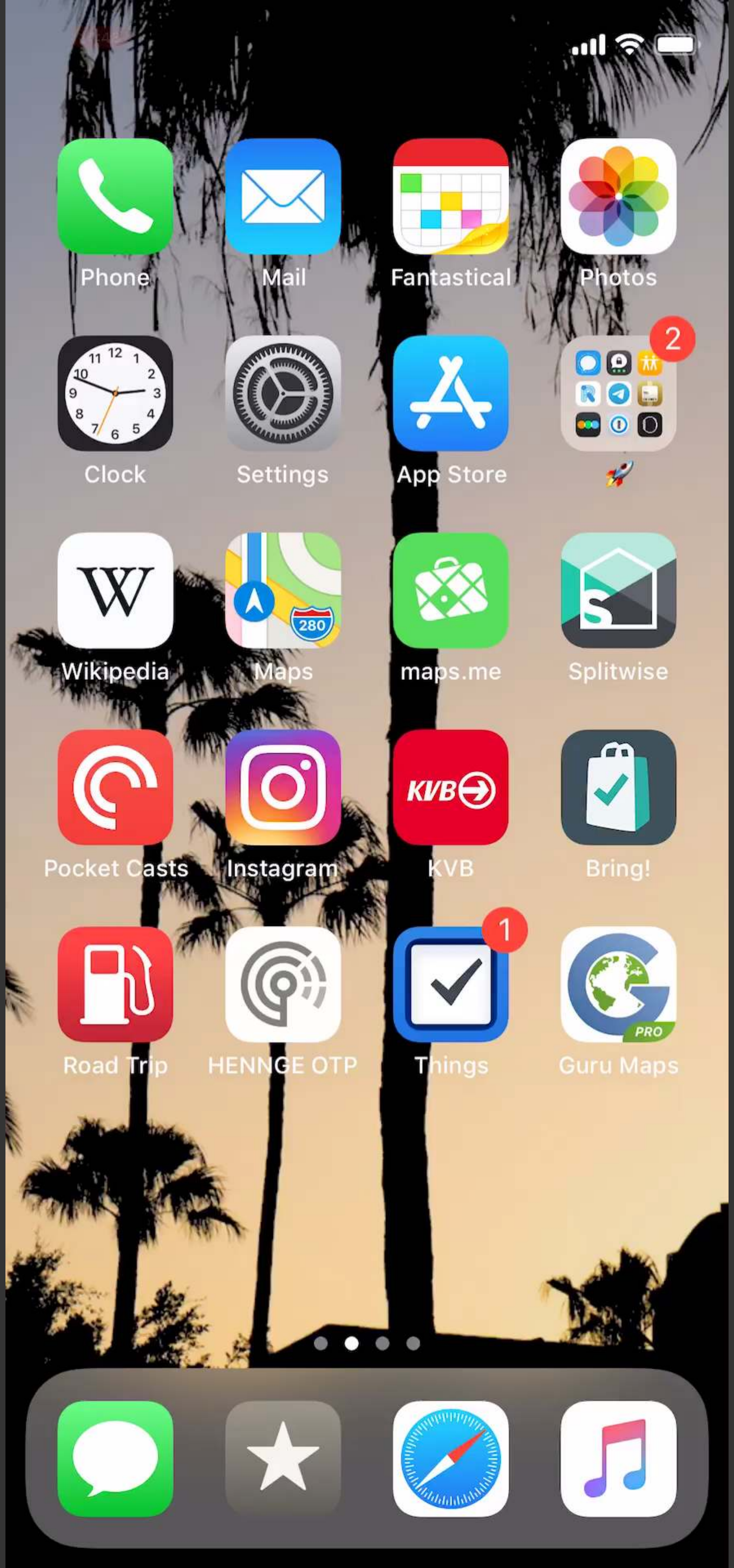
People who live in this location

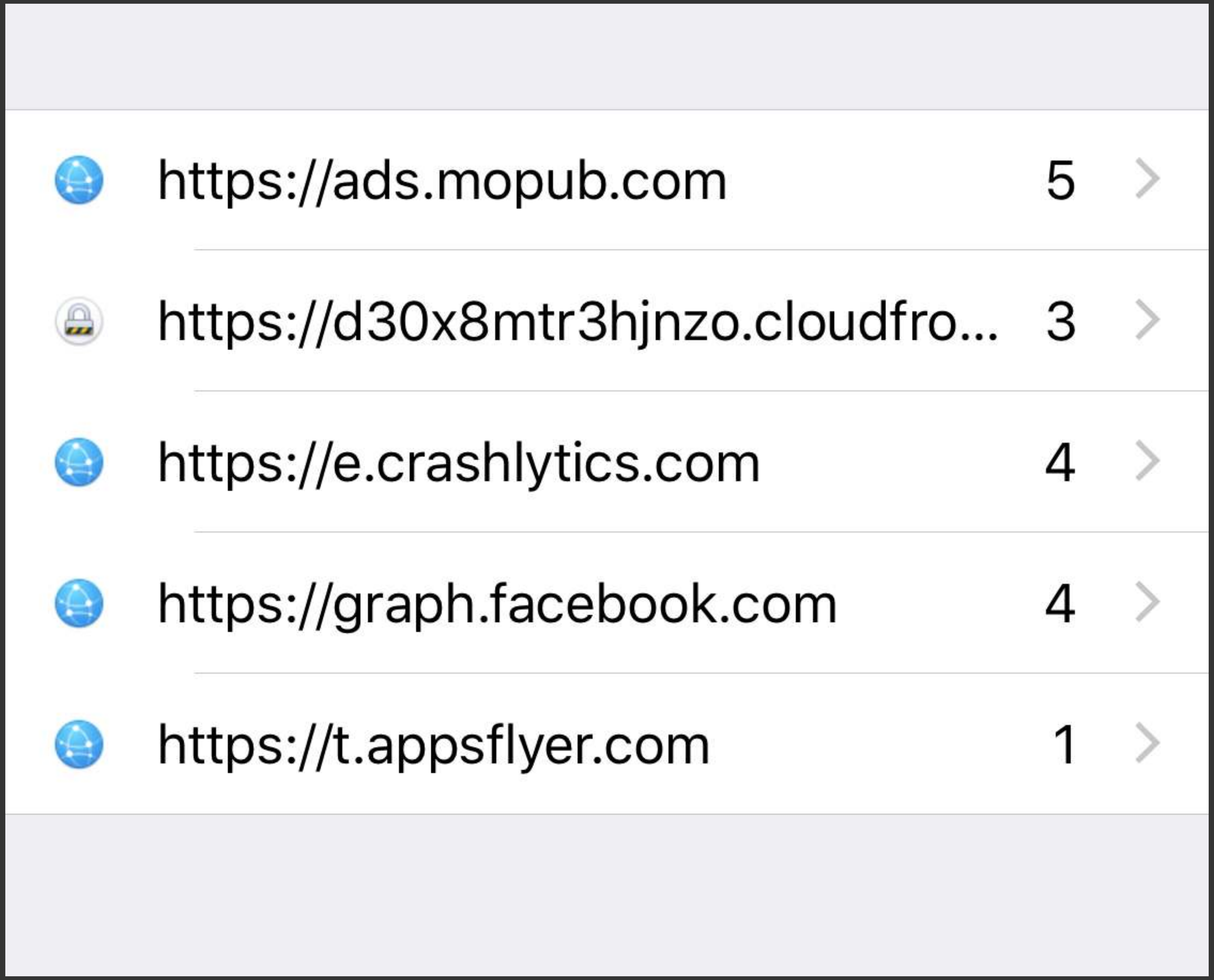
People recently in this location

People travelling in this location

Add locations in bulk

"Ok, but there are 3rd party apps that even work offline"


Phone
Mail
Fantastical
Photos
Clock
Settings
App Store
2
Wikipedia
Maps
280
maps.me
Splitwise
Pocket Casts
Instagram
KVB
Bring!
Road Trip
HENNGE OTP
1
Things
PRO
Guru Maps



| | |
|---|---|
| https://ads.mopub.com | 5 |
| https://d30x8mtr3hjnzo.cloudfro... | 3 |
| https://e.crashlytics.com | 4 |
| https://graph.facebook.com | 4 |
| https://t.appsflyer.com | 1 |

# What is actually transmitted?

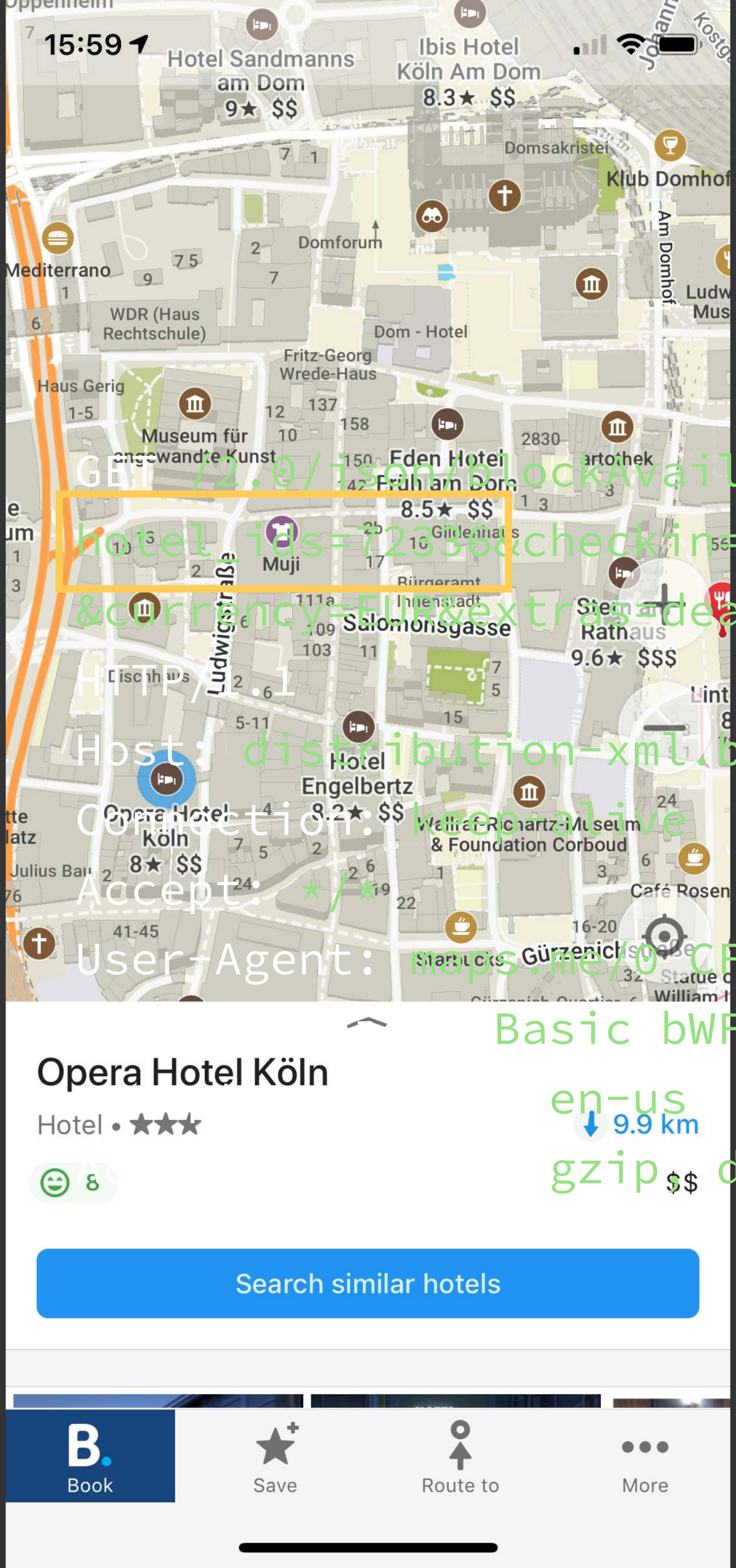
*at the time of writing*

```
ADAPTERS=AN
AFP=c94208
SCREEN_WIDTH=375
ROOTED=1
COCOS2D=0
LOCALE=en_DE
IDFA_FLAG=1
UNITY=0
CLIENT_EVENTS=
MEDIATION_SERVICE=MOPUB_5.0.0
BUNDLE=com.mapswithme.full
DENSITY=3
OS=iOS
COPPA=0
VOLUME=0.2177424430847168
APPBUILD=0
MODEL=iPhone10,6
CORE_AFP=5430e1a8
HEIGHT=-1
MAKE=Apple
SDK=ios
NETWORK_TYPE=1
```

```
PLACEMENT_ID=185237551520383_145032492
5011633
SDK_VERSION=4.28.1
TEMPLATE_ID=200
SDK_CAPABILITY=[3,4,5,7,9,10,12,16,17]
ORIENTATION=0
M_BANNER_KEY=Y29tLm1hcHN3aXRobWUuZnVsb
A==
REQUEST_TIME=1547567978.829753
NUM_ADS_REQUESTED=1
SCREEN_HEIGHT=812
ALLOWS_ARBITRARY_LOADS=1
WIDTH=-1
SESSION_ID=CAC323A7-XXXX-XXXX-9D0E-
D69E5E96E119
IDFA=A0A5A823-XXXX-XXXX-902F-
C67B7872F33F
APPVERS=8.6.0
OSVERS=12.1.2
SESSION_TIME=0.002051115036010742
```

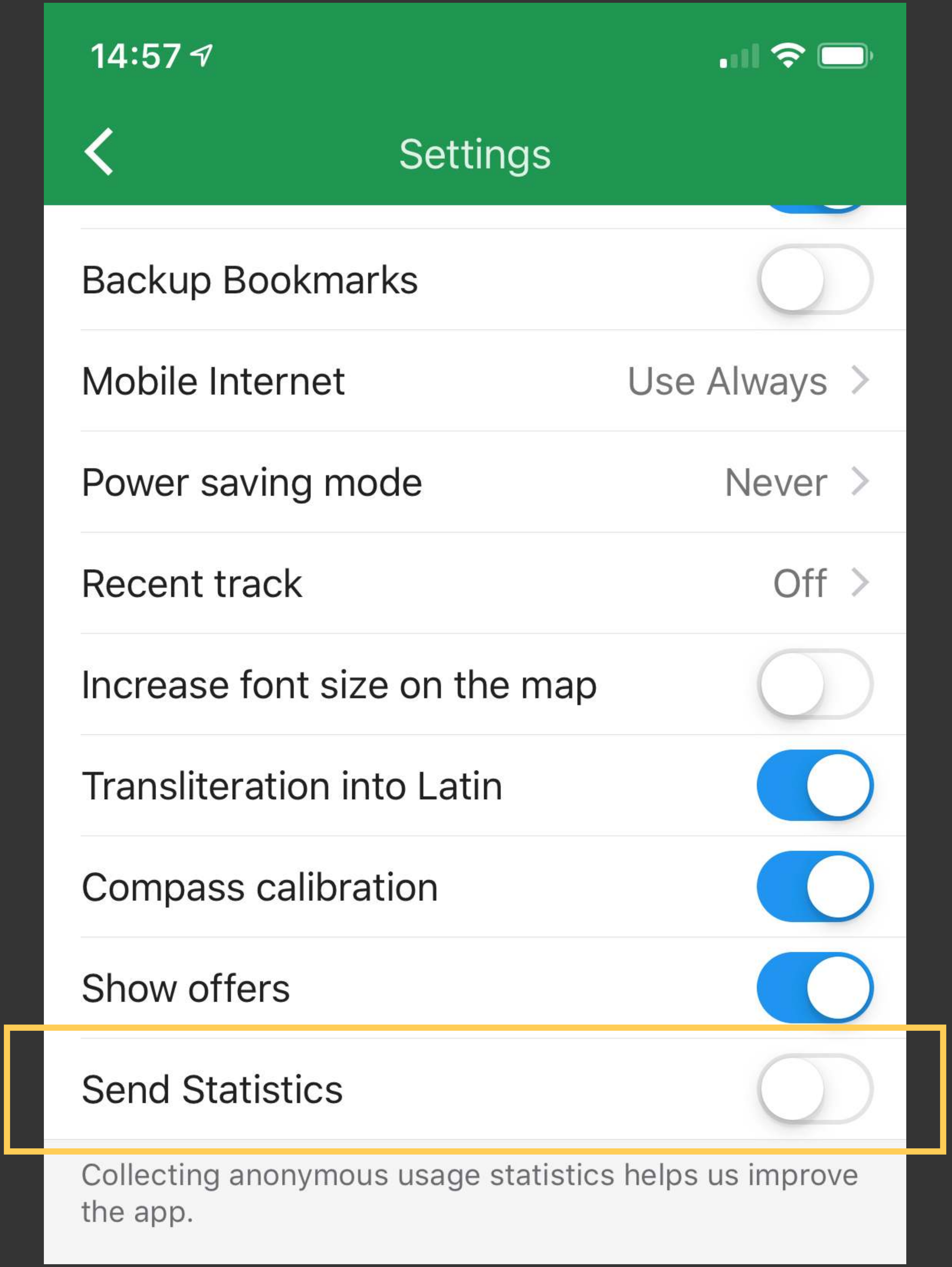
```
{
  "mnc": "02",
  "av": "8.6.0",
  "dn": "iPhone10,6",
  "q": "user_lang:en",
  "ats": "1",
  "gdpr_applies": "1",
  "h": "2436",
  "udid": "mopub:BA6D22D6-22E2-48E3-9C87-042E2D99FAB4",
  "iso": "de",
  "assets": "ctatext,title,iconimage,text",
  "nv": "5.0.0",
  "ct": "2",
  "id": "29c1bc85b46442b5a370552916aa6822",
  "mcc": "262",
  "w": "1125",
  "mr": "1",
  "v": "8",
  "z": "+0100",
  "bundle": "com.mapswithme.full",
  "cn": "Vodafone.de",
  "sc": "3.0",
  "current_consent_status": "potential_whitelist",
  "o": "p"
}
```

but beware what you tap on



```
GET /2.0/json/blockAvailability?
hotel_ids=72336&checkin=2019-09-18&checkout=2019-09-19
&currency=EUR&extras=deal_smart,deal_lastm,photos
HTTP/1.1
Host: distribution-xml.booking.com
Connection: keep-alive
Accept: */*
User-Agent: maps.me/0 CFNetwork/978.0.7 Darwin/18.7.0
        Basic bWFwczE6cmVnNzNydDIzcmU=
          en-us
          gzip, deflate
```

```
GET /ads/1/190621/Germany_North%20Rhine-
Westphalia_Regierungsbezirk%20Koln_Koln.ads HTTP/1.1
Host: localads.maps.me
Accept: */*
Accept-Language: en-us
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: MAPS.ME/iOS/9.3.0
```



14:57

Settings

Backup Bookmarks ○

Mobile Internet Use Always >

Power saving mode Never >

Recent track Off >

Increase font size on the map ○

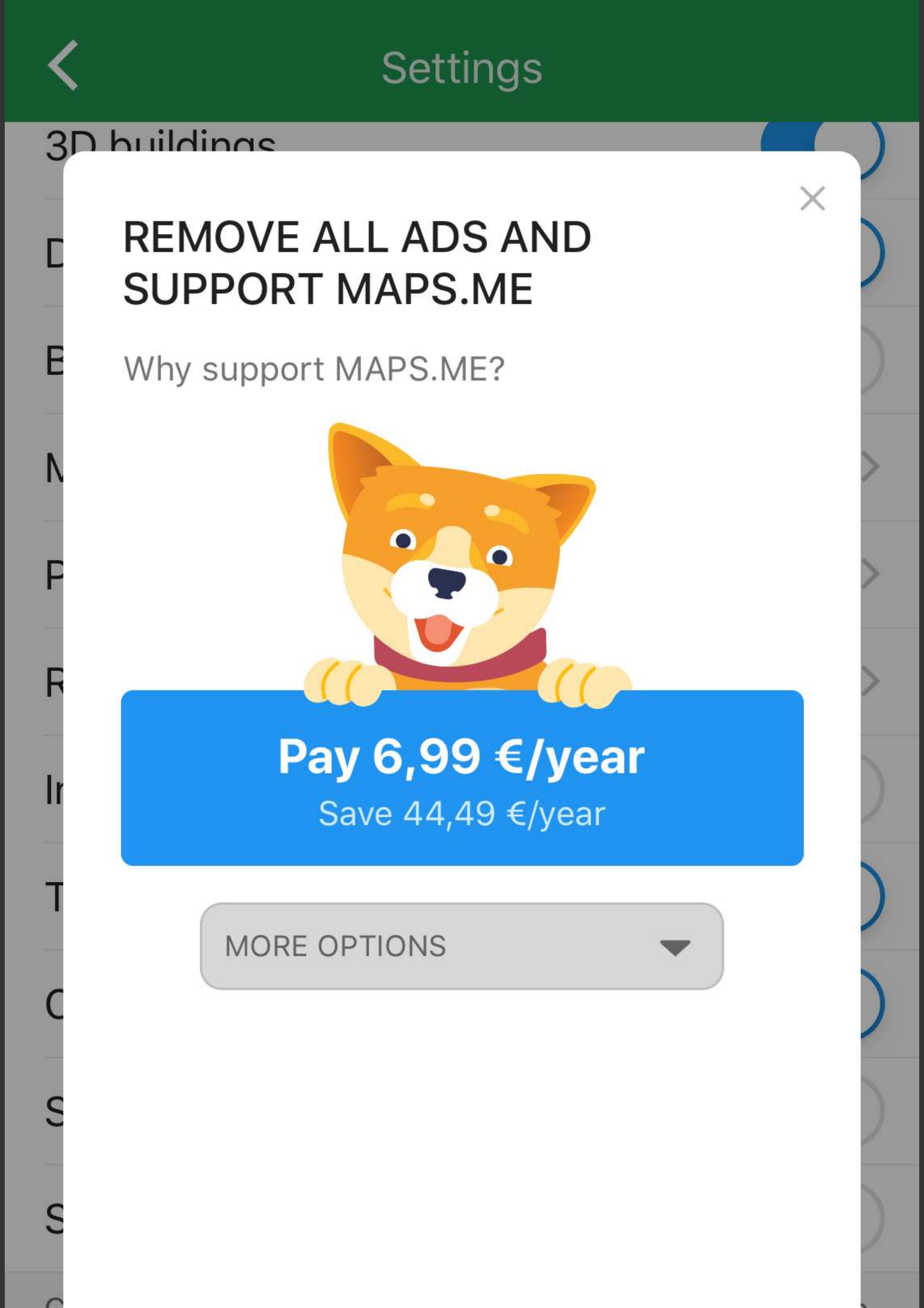
Transliteration into Latin ●

Compass calibration ●

Show offers ●

Send Statistics ○

Collecting anonymous usage statistics helps us improve the app.



Settings

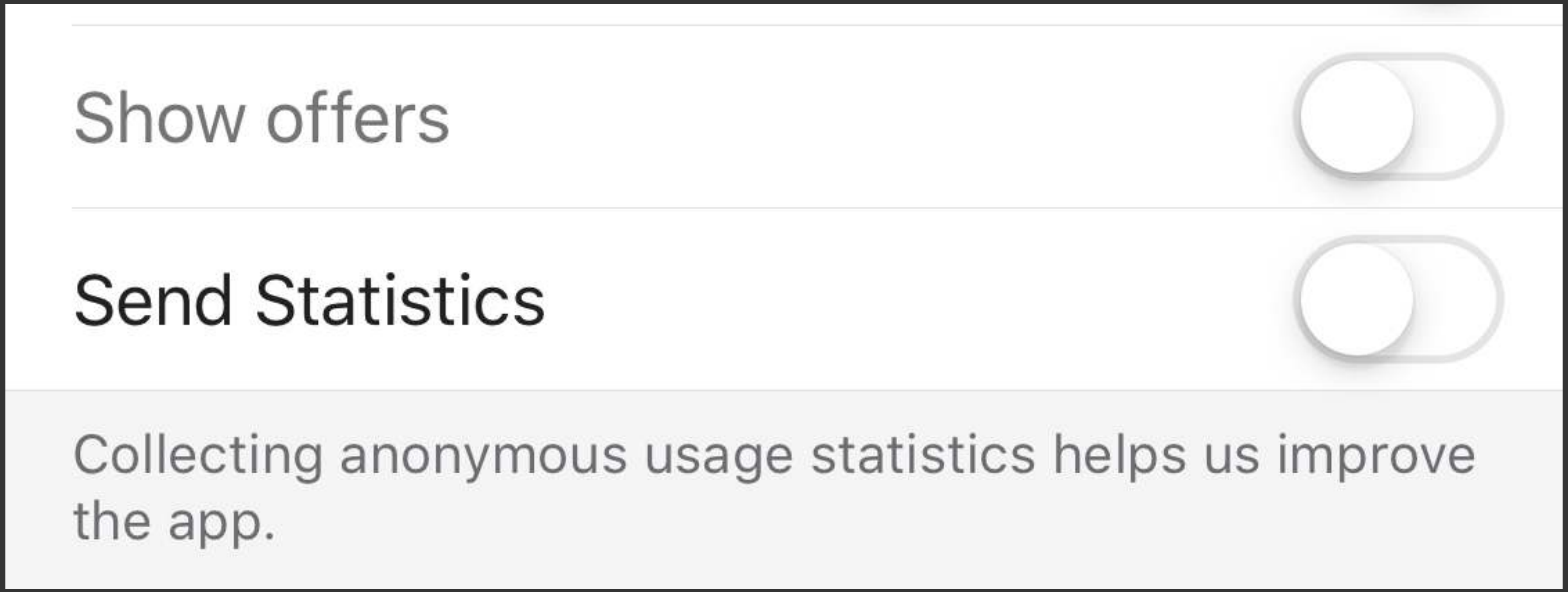
3D buildings

REMOVE ALL ADS AND SUPPORT MAPS.ME

Why support MAPS.ME?

Pay 6,99 €/year

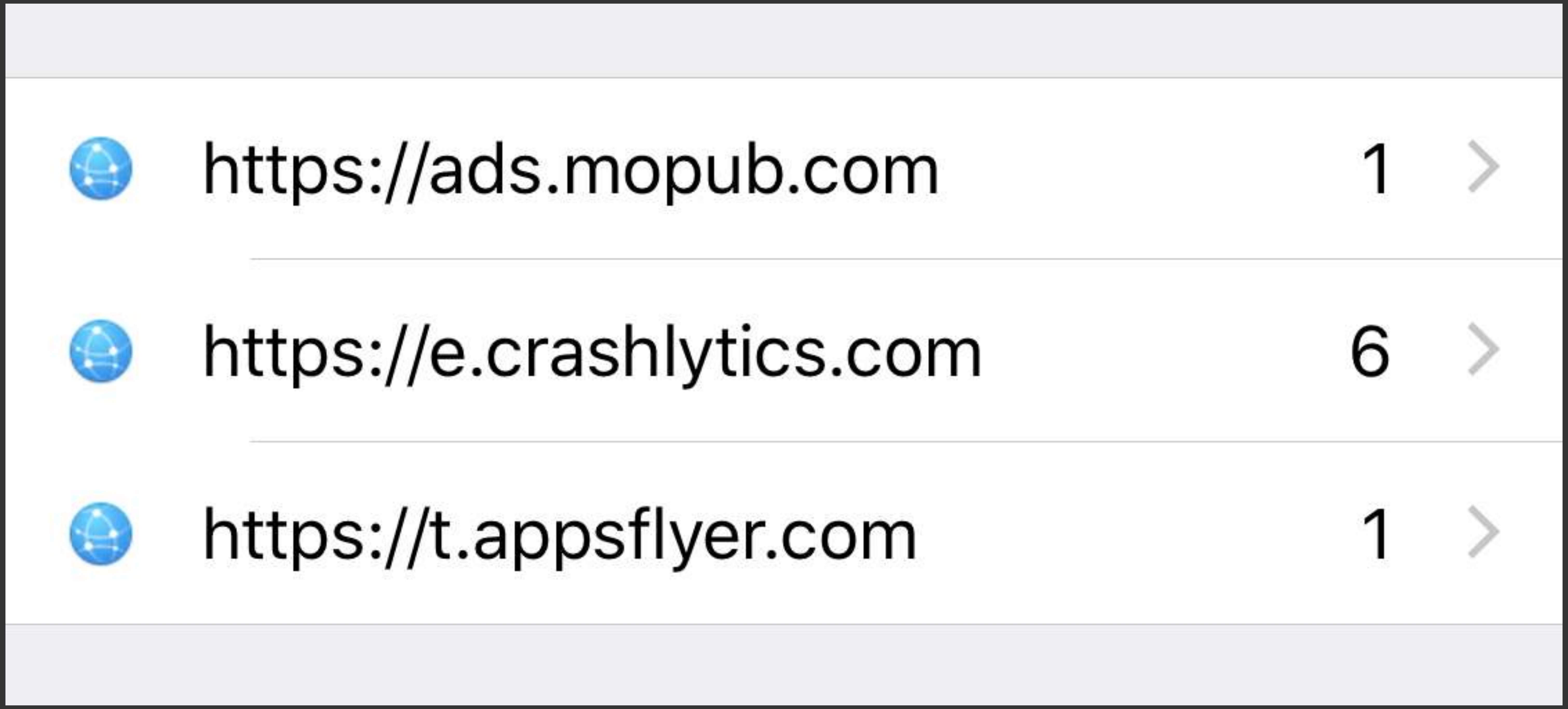
Save 44,49 €/year



Show offers

Send Statistics

Collecting anonymous usage statistics helps us improve the app.

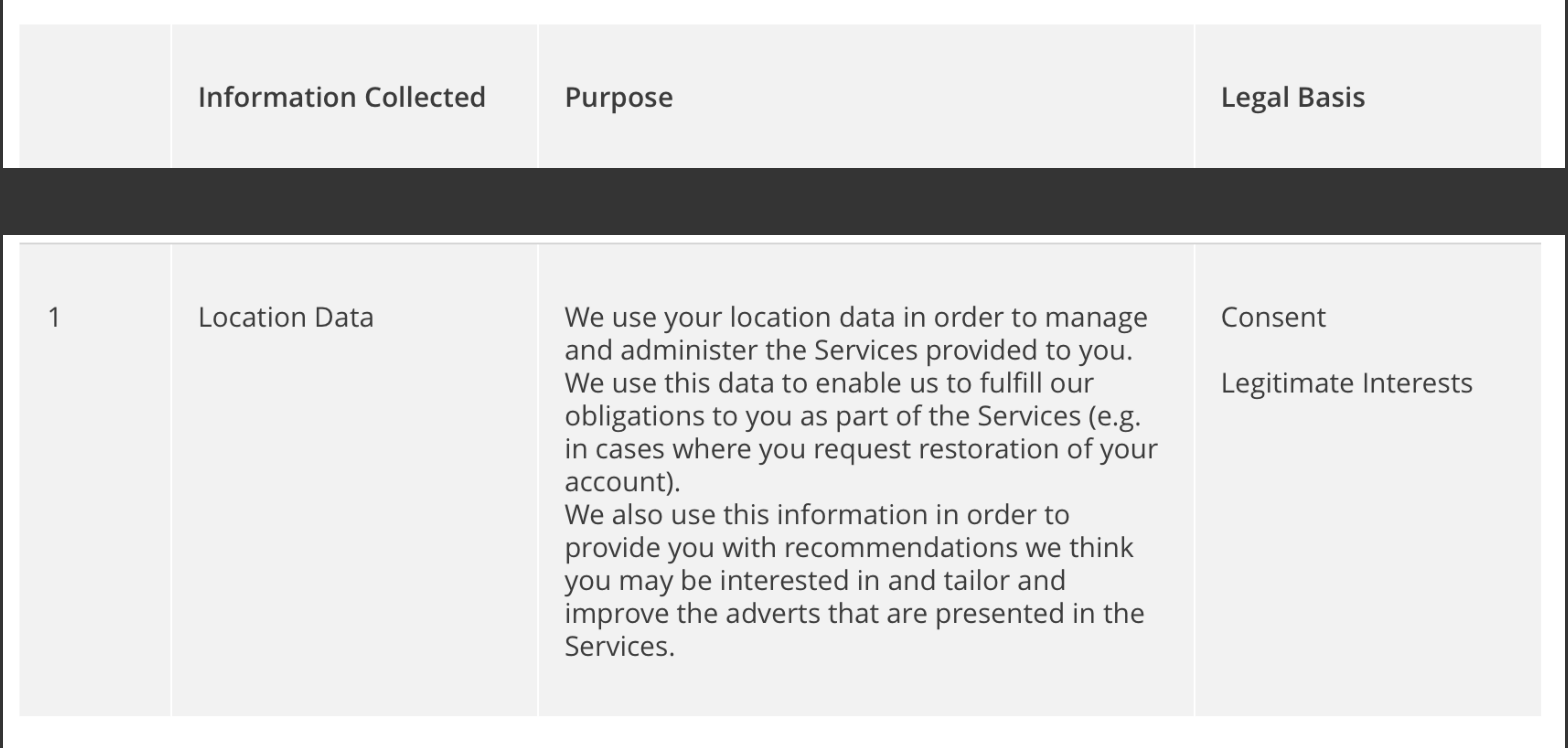


| | |
|---|---|
| https://ads.mopub.com | 1 |
| https://e.crashlytics.com | 6 |
| https://t.appsflyer.com | 1 |

```
{
  "id": "com.mapswithme.full",
  "av": "9.3.0",
  "udid": "mopub:692BE0BE-C9DE-4573-BF8A-E8AED4069996",
  "v": "8",
  "gdpr_applies": "1",
  "nv": "5.0.0",
  "st": "1",
  "current_consent_status": "dnt"
}
```

sent to ads.mopub.com

sent to t.appsflyer.com



| | Information Collected | Purpose | Legal Basis |
|---|---|---|---|
| 1 | Location Data | We use your location data in order to manage and administer the Services provided to you.<br>We use this data to enable us to fulfill our obligations to you as part of the Services (e.g. in cases where you request restoration of your account).<br>We also use this information in order to provide you with recommendations we think you may be interested in and tailor and improve the adverts that are presented in the Services. | Consent<br>Legitimate Interests |

Dear maps.me,

It is nice that you give people the option to opt-out, but it would be nice if it actually worked. Please don’t mess with OSM’s reputation.

Are there apps who are doing better?

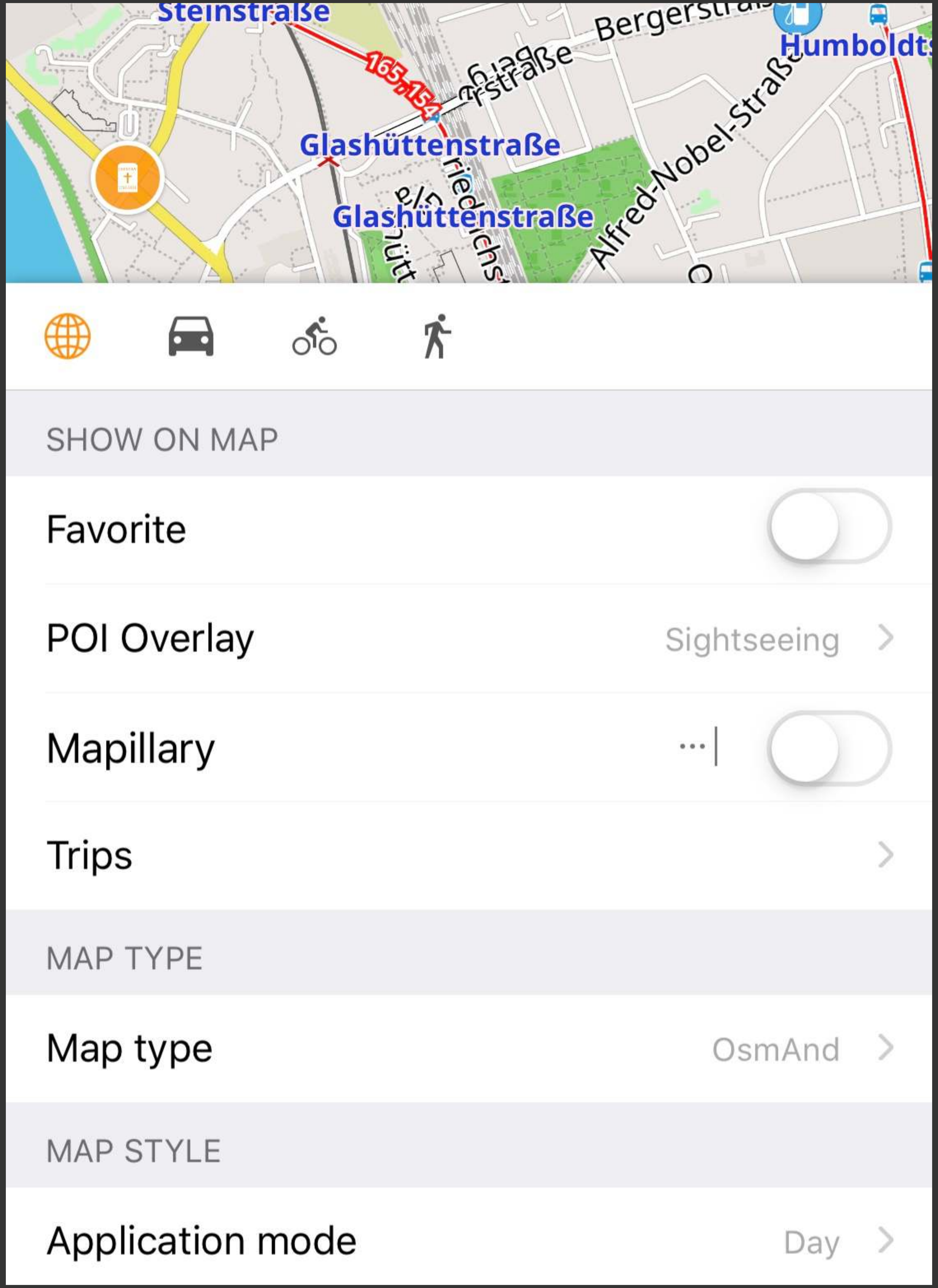
# Let’s look at OSMAnd

*on iOS*

Generally less chatty.

# But if you tap a place,
# it phones home

```
GET /api/cm_place?lat=50.884595&lon=7.058571 HTTP/1.1
```



SHOW ON MAP

Favorite ○

POI Overlay Sightseeing >

Mapillary ··· ○

Trips >

MAP TYPE

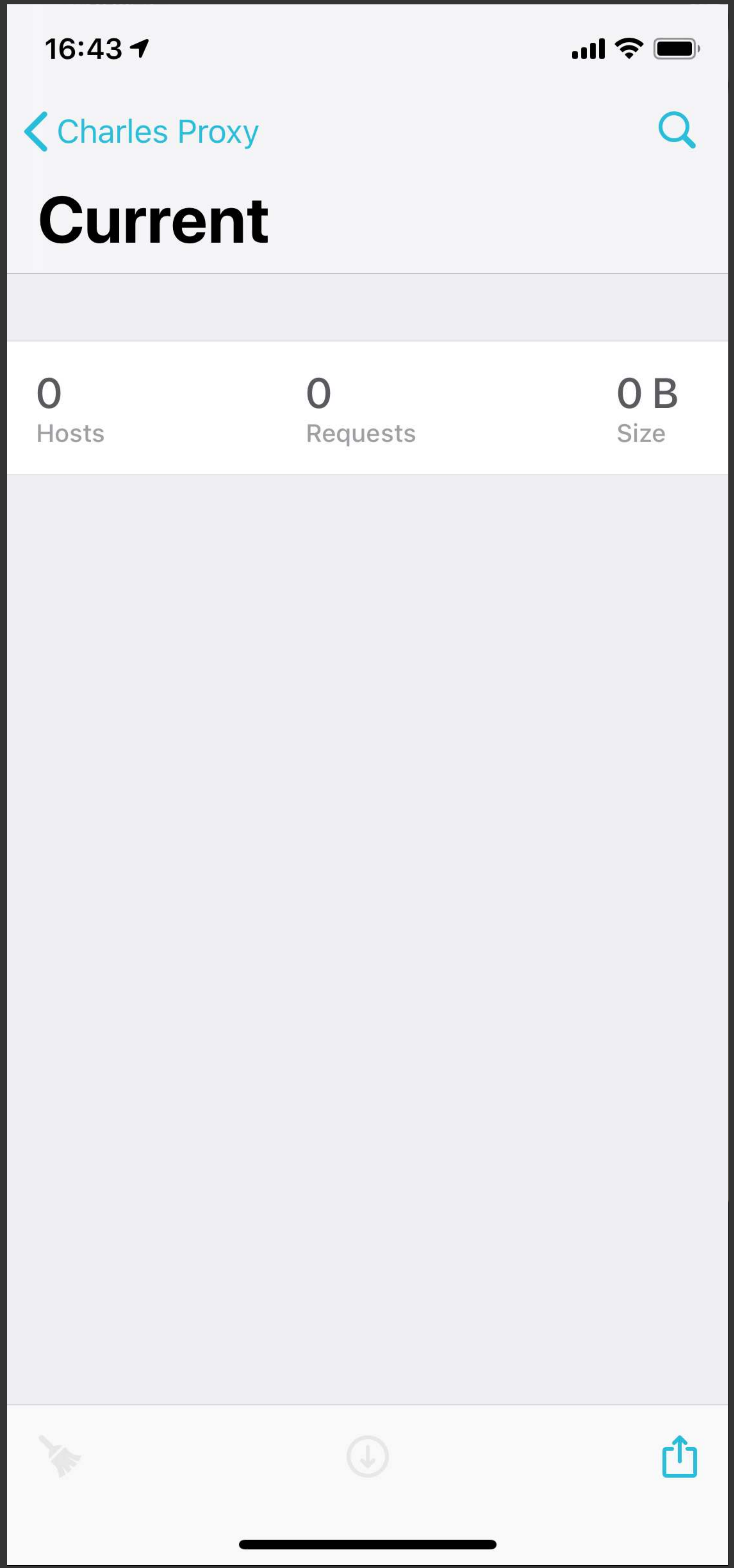
Map type OsmAnd >

MAP STYLE

Application mode Day >

# Positive Example

# Guru Maps



| 0 | 0 | 0 B |
|---|---|---|
| Hosts | Requests | Size |

# What do we learn?

1. Not every app that is OSM based is a private app

2. Not even open source software is guaranteed to be private

# 3. `@Developers`, please respect the need for privacy

Ask users for consent.
Don’t blindly assume it.

Use system APIs to check for system-wide privacy settings

e.g. `ASIdentifierManager.isAdvertisingTrackingEnabled`

Don’t include 3rd party frameworks blindly

# Is your OSM App spying on you?

State of the Map 2019, Heidelberg

Thomas Skowron
https://skowron.eu