Ready or not, here I come!

Rick Ramgattie | Associate Security Analyst

./bio

- Rick Ramgattie
  - Coding
  - Reading
  - Reverse Engineering
  - Happy to be back in Puerto Rico
  - Associate Security Analyst @ Independent Security Evaluators

./work

- Where:
  - Baltimore, MD
- What: Security Assessments
  - Web
  - Mobile
  - Infrastructure
- How:
  - Whitebox, Blackbox, other stuff

What's this talk about

- Using dating apps to track and locate people.
  - **Trilateration**.
- How geolocation obfuscation can be circumvented.
  - **Colluded Trilateration**.
- Defenses

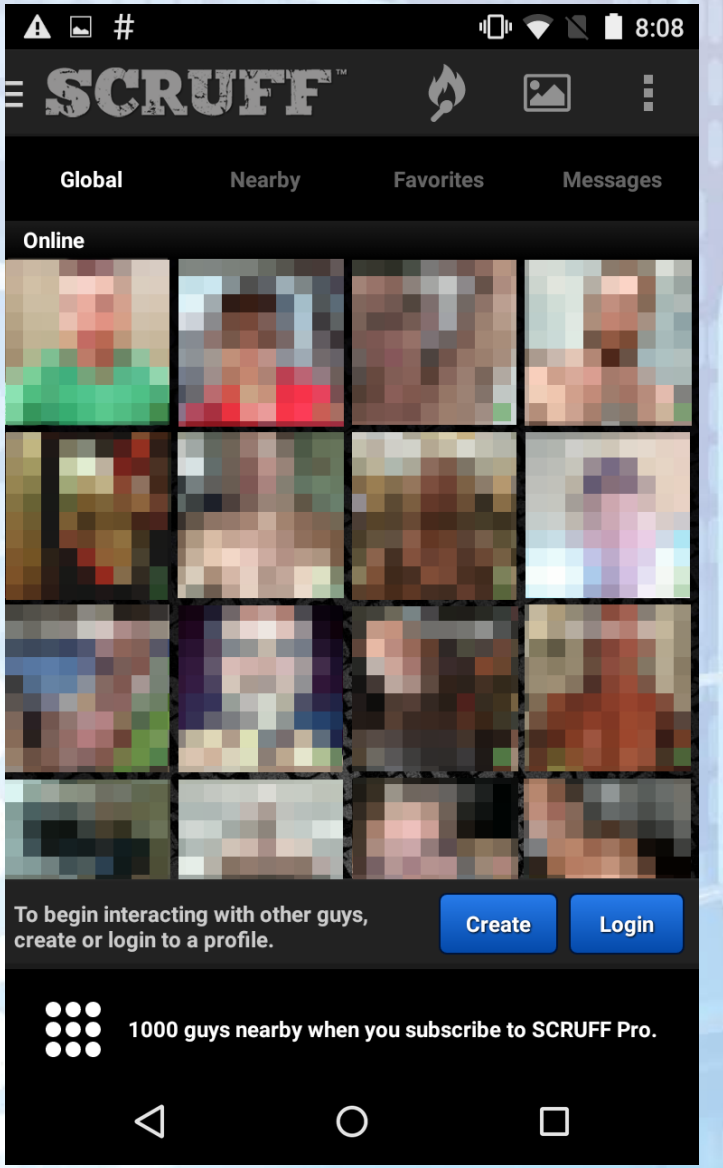
Why is it important?

- Black mail
- Legal evidence
  - Divorce Lawsuits
- Stalking
- Deaths
  - Orlando Shooting

Scruff

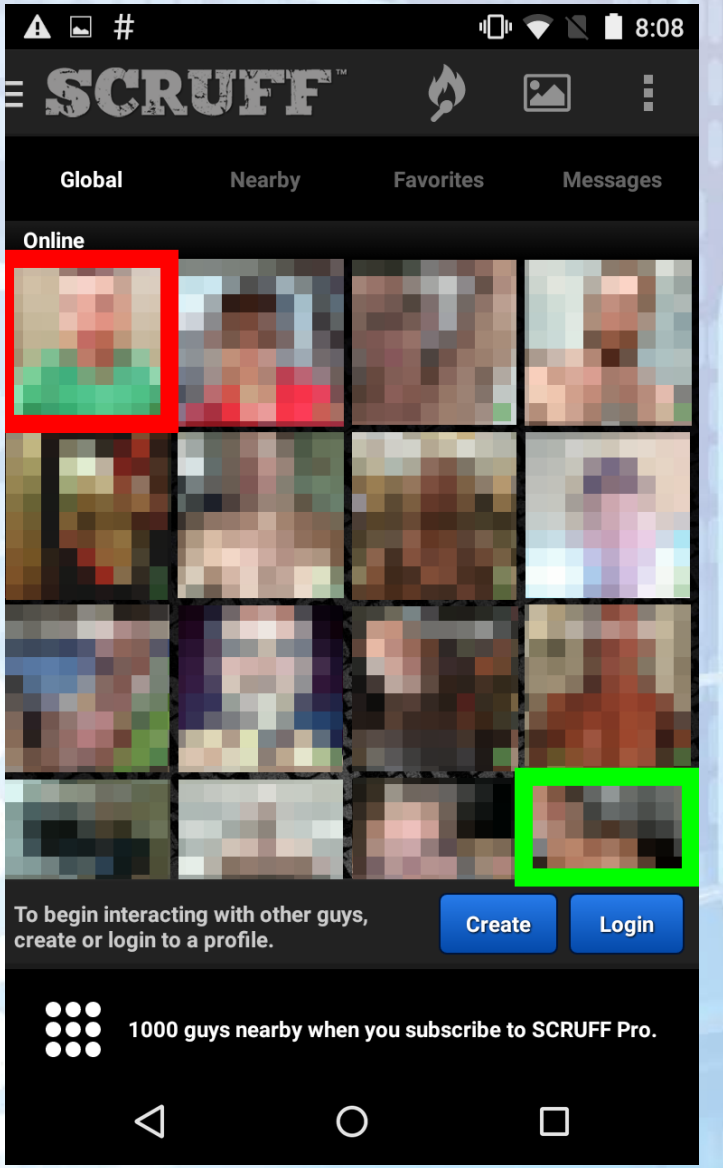
independent security evaluators

Scruff: Home Interface



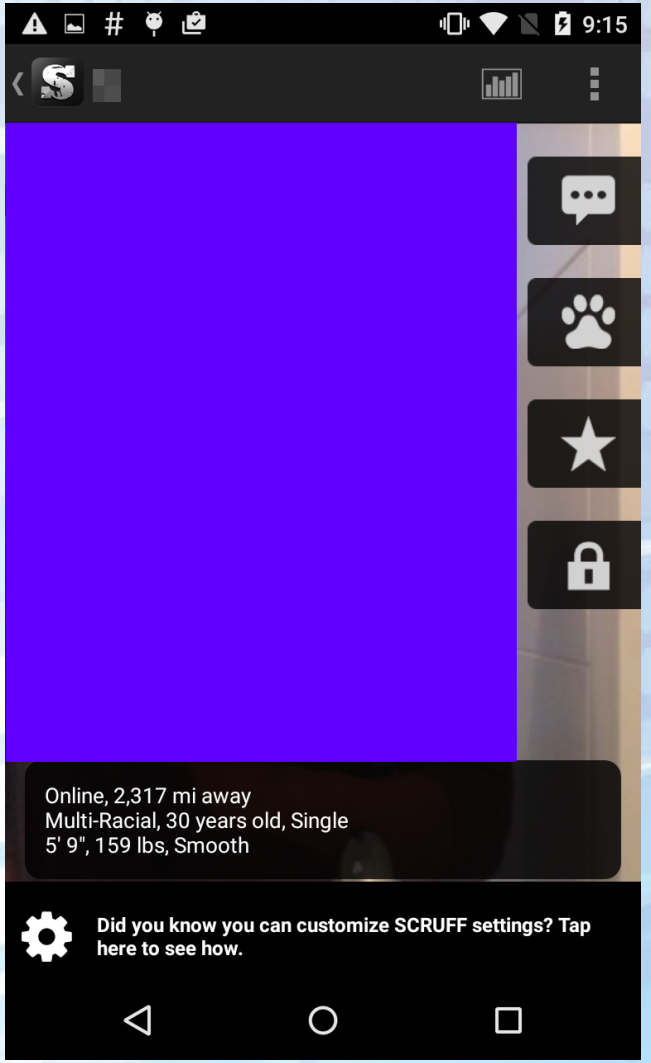
independent security evaluators

Scruff: Home Interface



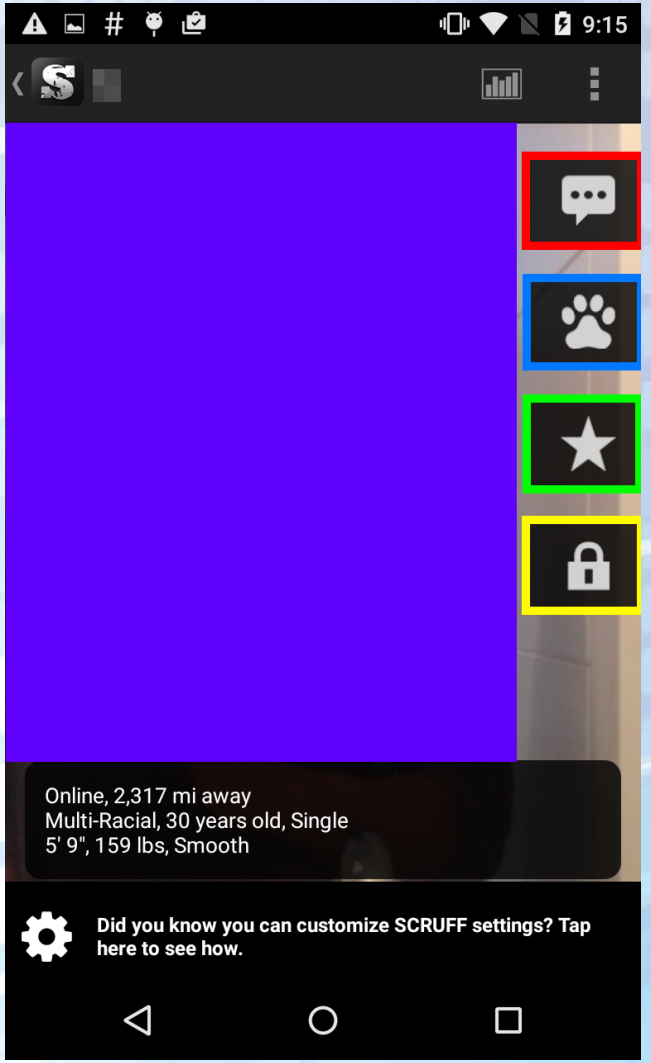
independent security evaluators

Scruff: User Profile



independent security evaluators

Scruff: User Profile



independent security evaluators

How do Scruff users identify with the server?

device_id

1f05bab60c0c6fb6040d47d33dd09cdb

Provide Scruff with your location:

Method: POST

URL: https://api.scruffapp.com/app/location

latitude: *18.4695102*

longitude: *-66.1257145*

device_id: *36c2c12b4cc1ed98fb3cbdc48dfbc06b*

device_type: *3*

client_version: *5.0115*

independent security evaluators

Users Near You:

Method: GET

URL: https://api.scruffapp.com/app/location

latitude: *18.4695102*

longitude: *-66.1257145*

offset: *0*

request_id: *d5f87755c7ec5213e2d1f1455f15aeae*

client_version: *5.0115*

query_sort_type: *3*

independent security evaluators

Users Near You:

https://api.scruffapp.com/app/location?client_version=5.0115&device_type=3&latitude=18.4695102&longitude=-66.1257145&offset=0&query_sort_type=0&request_id=d5f87755c7ec5213e2d1f1455f15aeae

independent security evaluators

Users Near You:

```
def get_request_id():
    return ''.join([random.choice('0123456789abcdef') for x in range(32)])
```

Users Near You:

{
u'album_images': 5,
u'dst': 940.7932633736375,
u'has_image': 7,
u'id': 328313123,
u'lat': 0,
u'logged_in': True,
u'lon': 0,
u'name': u’Naminton',
u'online': True,
u'recent': True,
u'updated_at': u'Tue, 06 Sep 2016 23:54:09 GMT’
}

independent security evaluators

Users Near You:

Method: GET
URL: https://api.scruffapp.com/app/location
latitude: *18.4695102*
longitude: *-66.1257145*
offset: *0*
request_id: *d5f87755c7ec5213e2d1f1455f15aeae*
client_version: *5.0115*
query_sort_type: *3*

[…{
u'album_images': 5,
u'dst': 940.7932633736375,
u'has_image': 7,
u'id': 328313123,
u'lat': 0,
u'logged_in': True,
u'lon': 0,
u'name': u'Naminton',
u'online': True,
u'recent': True,
u'updated_at': u'Tue, 06 Sep 2016 23:54:09 GMT'
}, …]

Get user Profile Info:

Method: GET

URL: https://api.scruffapp.com/app/profile

latitude: *18.4695102*

longitude: *-66.1257145*

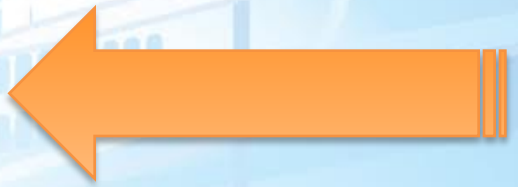
device_type: *3*

client_version: *5.0115*

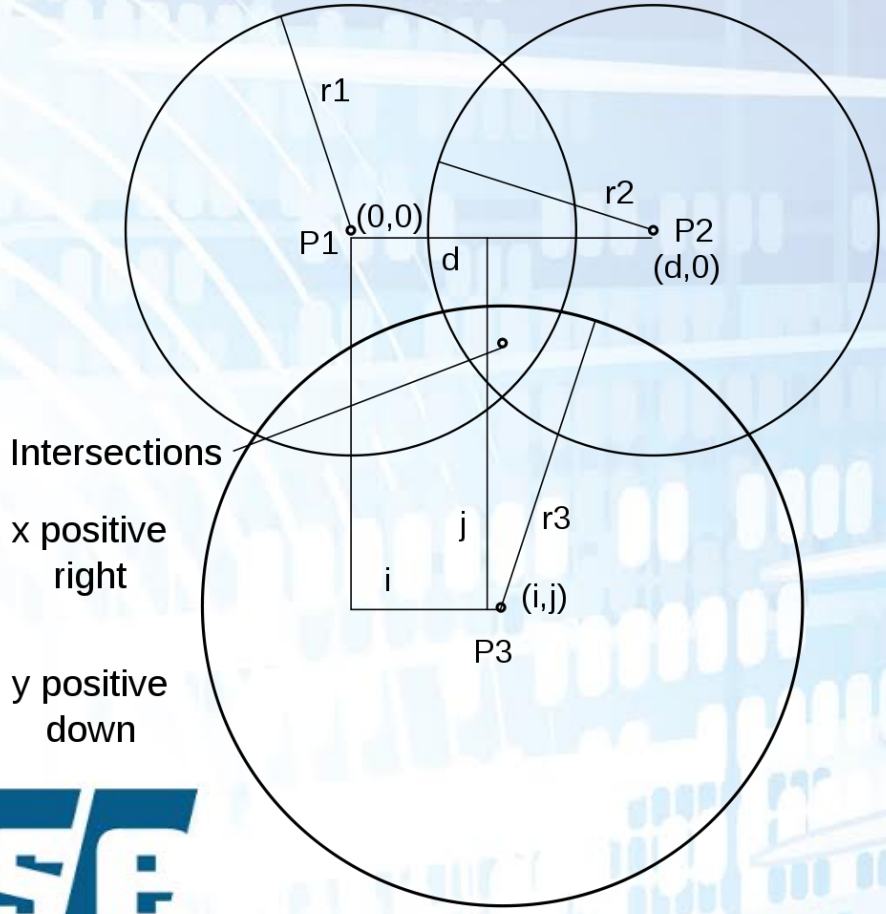
target: *328313123*

Get user Profile Info:

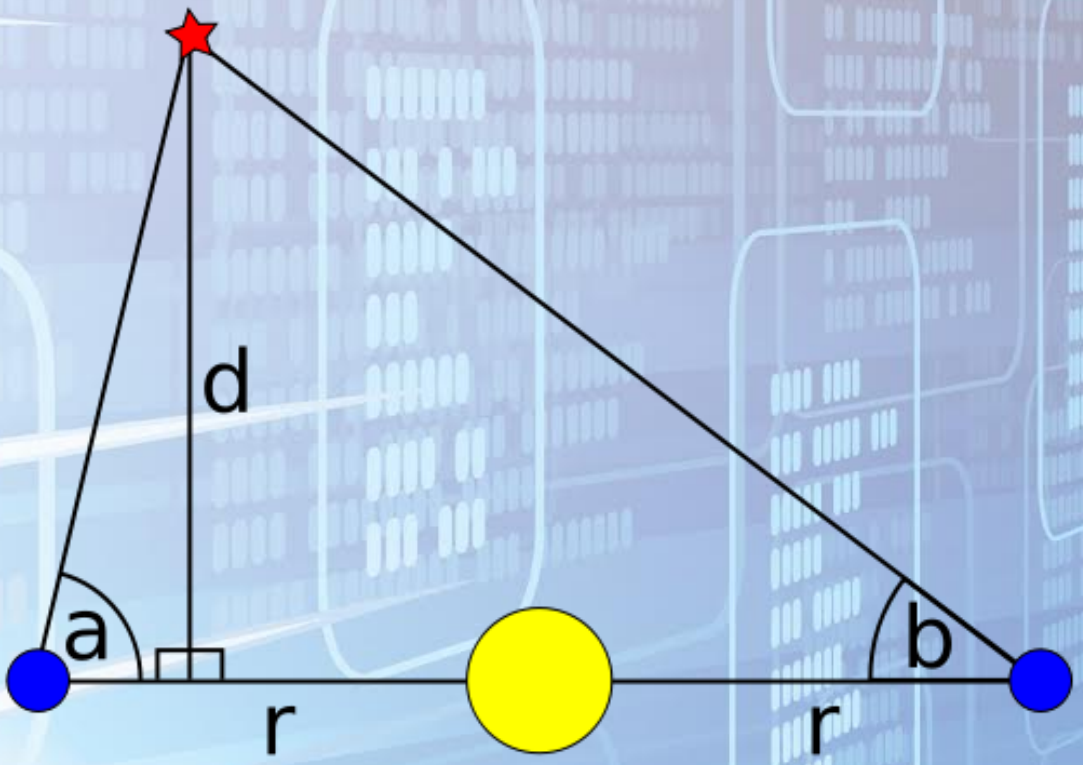
u'about': *None*,
u'birthday': *u'Thu, 22 Aug 1985 00:00:00 GMT'*,
u'checkin_count': *0*,
u'city': *None*,
u'community': [],
u'country': *None*,
u'deleted': *False*,
u'dst': *3767.7204467100823*,
u'ethnicity': *None*,
u'ethnicity_enum': *None*,
u'face_pic': *False*,
u'facebook_url': *None*,
u'featured_at': *None*,
u'flag_count': *0*,
u'flag_reset_count': *0*,
u'fun': *None*,
u'height': *None*,
u'hide_distance': *False*,
u'hide_global': *False*,
u'hiv_status': *None*,
u'id': *110059343*,
u'ideal': *None*,
u'last_login': **u'***Tue, 06 Sep 2016 13:42:36 GMT***'**,
u'lat': *0*,
u'logged_in': *True*,
u'lon': *0*,
u'looking_for': *None*,
u'name': **u'***Kindandstronglikethebear***'**,
u'online': *False*,
u'recent': *False*,
u'relationship_interests': [],
u'relationship_status': *None*,
u'rsvp_count': *0*,
u'sex_preferences': [],
u'sex_safety_practices': [],
u'updated_at': **u'***Tue, 06 Sep 2016 13:42:36 GMT***'**,
u'user_type': *None*,
u'version': *0*,
u'weight': *None*



Trilateration



Triangulation

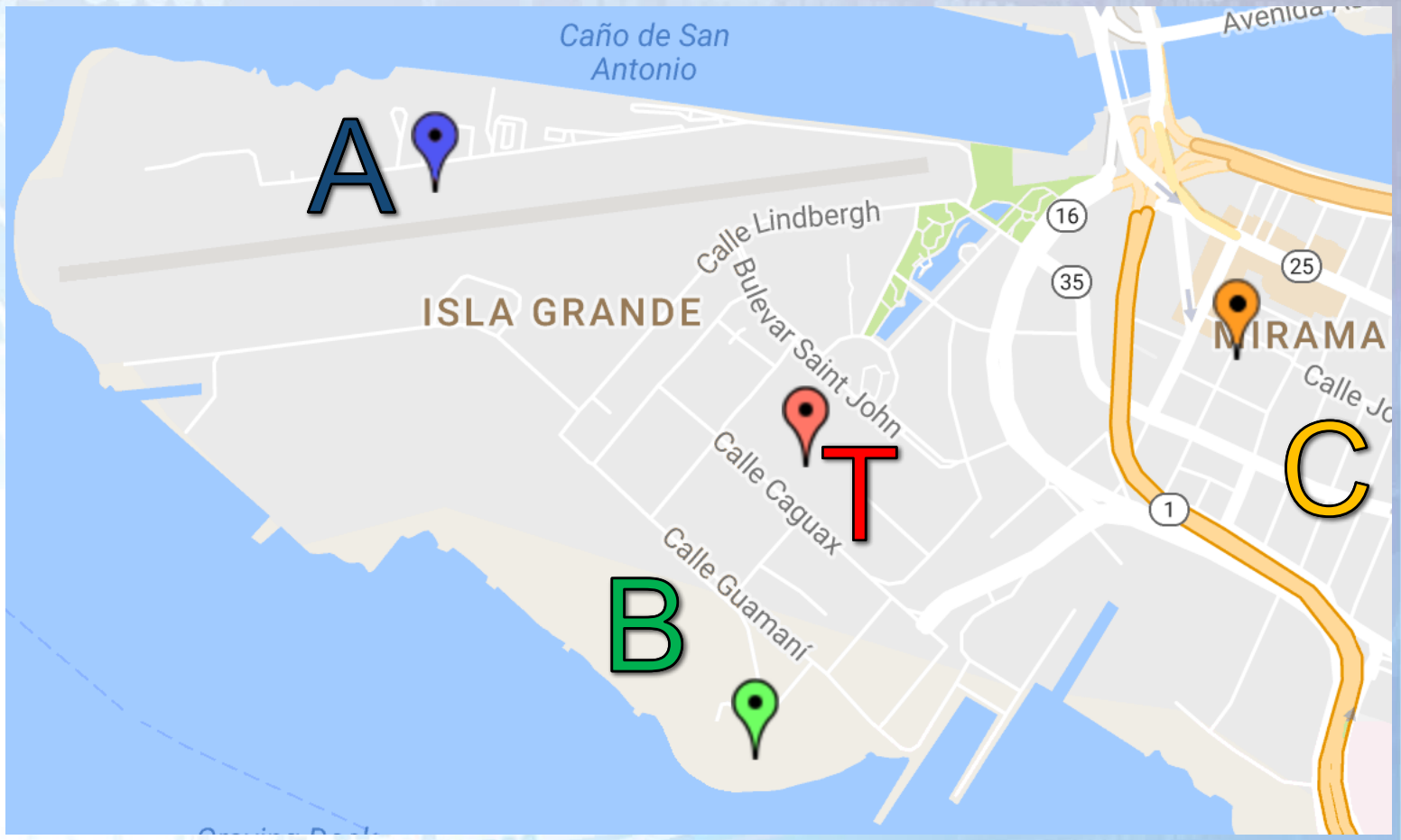


independent security evaluators

Trilateration: Illustrated

independent security evaluators

Trilateration: Illustrated

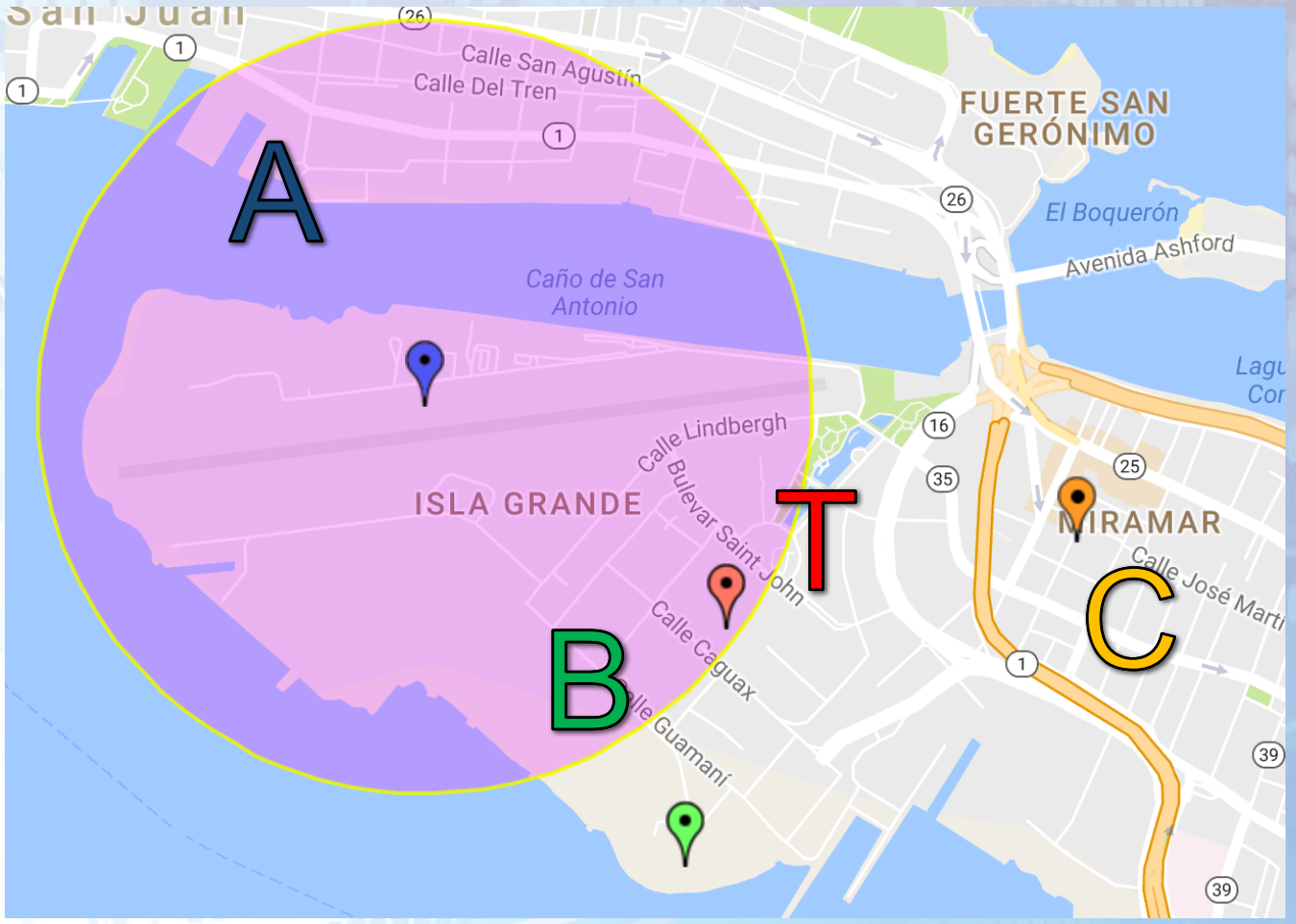


independent security evaluators

Trilateration: Illustrated

independent security evaluators

Trilateration: Illustrated



independent security evaluators

Calculating the Circle:

$$\varphi 2 = \text{asin}(\sin \varphi 1 \cdot \cos \delta + \cos \varphi 1 \cdot \sin \delta \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \text{atan2}(\sin \theta \cdot \sin \delta \cdot \cos \varphi_1, \cos \delta - \sin \varphi_1 \cdot \sin \varphi_2)$$

Ref: http://www.movable-type.co.uk/scripts/latlong.html

Calculating the Circle:

$$\varphi_2 = \text{asin}(\sin \varphi_1 \cdot \cos \delta + \cos \varphi_1 \cdot \sin \delta \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \text{atan2}(\sin \theta \cdot \sin \delta \cdot \cos \varphi_1, \cos \delta - \sin \varphi_1 \cdot \sin \varphi_2)$$

Legend:

φ = *Latitude*

λ = *Longitude*

δ = *Distance*

θ = *Bearing*

Ref: http://www.movable-type.co.uk/scripts/latlong.html

Calculating the Circle:

$$\varphi_2 = \operatorname{asin}(\sin \varphi_1 \cdot \cos \delta + \cos \varphi_1 \cdot \sin \delta \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \operatorname{atan2}(\sin \theta \cdot \sin \delta \cdot \cos \phi_1, \cos \delta - \sin \phi_1 \cdot \sin \phi_2)$$

Legend:

φ = *Latitude*

λ = *Longitude*

δ = *Distance*

θ = *Bearing*

Ref: http://www.movable-type.co.uk/scripts/latlong.html

Calculating the Circle:

$$\varphi_2 = \text{asin}(\sin \varphi_1 \cdot \cos \delta + \cos \varphi_1 \cdot \sin \delta \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \text{atan2}(\sin \theta \cdot \sin \delta \cdot \cos \varphi_1, \cos \delta - \sin \varphi_1 \cdot \sin \varphi_2)$$

Legend:

φ = *Latitude*

λ = *Longitude*

δ = *Distance*

θ = *Bearing*

Ref: http://www.movable-type.co.uk/scripts/latlong.html

Calculating the Circle:

$$\varphi_2 = \operatorname{asin}(\sin \varphi_1 \cdot \cos \delta + \cos \varphi_1 \cdot \sin \delta \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \operatorname{atan2}(\sin \theta \cdot \sin \delta \cdot \cos \varphi_1, \cos \delta - \sin \varphi_1 \cdot \sin \varphi_2)$$

Legend:

$\boldsymbol{\varphi}$ = *Latitude*

$\boldsymbol{\lambda}$ = *Longitude*

$\boldsymbol{\delta}$ = *Distance*

$\boldsymbol{\theta}$ = *Bearing*

Calculating the Circle:

$$\varphi_2 = \text{asin}(\sin \varphi_1 \cdot \cos \boldsymbol{\delta} + \cos \varphi_1 \cdot \sin \boldsymbol{\delta} \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \text{atan2}(\sin \theta \cdot \sin \boldsymbol{\delta} \cdot \cos \varphi_1, \cos \boldsymbol{\delta} - \sin \varphi_1 \cdot \sin \varphi_2)$$

Legend:

$\boldsymbol{\varphi}$ = *Latitude*

$\boldsymbol{\lambda}$ = *Longitude*

$\boldsymbol{\delta}$ = *Distance*

$\boldsymbol{\theta}$ = *Bearing*

Calculating the Circle:

$$\varphi_2 = \text{asin}(\sin \varphi_1 \cdot \cos \delta + \cos \varphi_1 \cdot \sin \delta \cdot \cos \theta)$$

$$\lambda_2 = \lambda_1 + \text{atan2}(\sin \theta \cdot \sin \delta \cdot \cos \varphi_1, \cos \delta - \sin \varphi_1 \cdot \sin \varphi_2)$$

Legend:

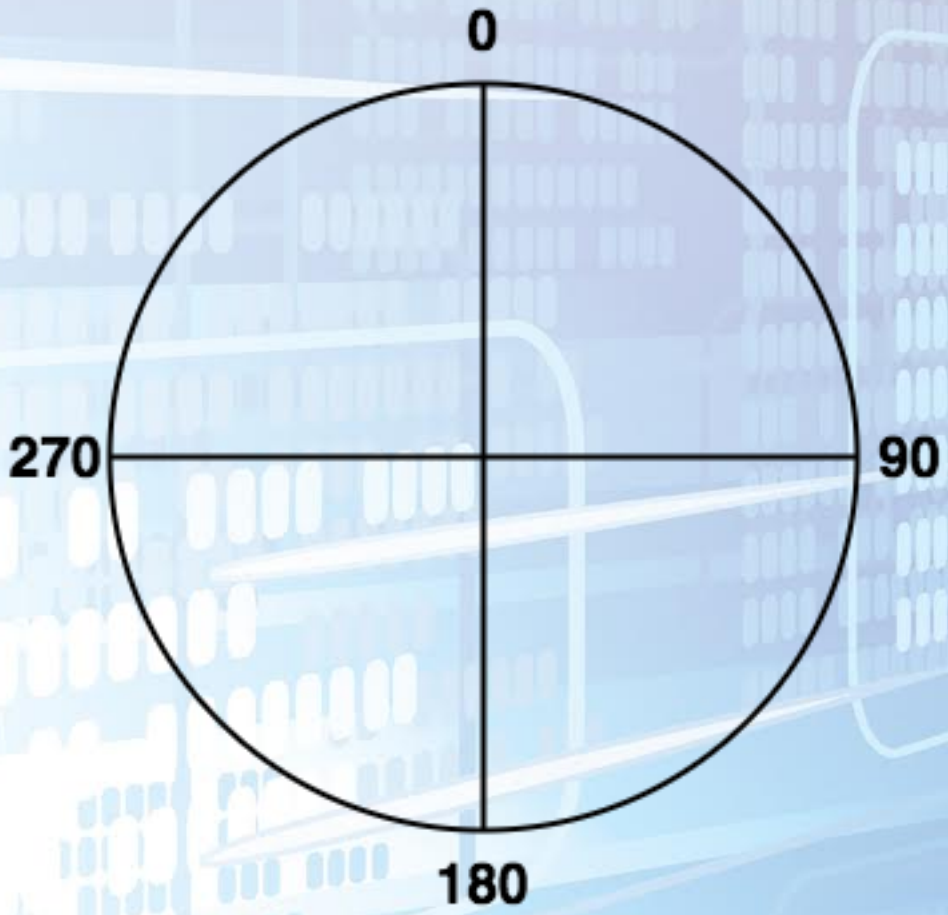
φ = *Latitude*

λ = *Longitude*

δ = *Distance*

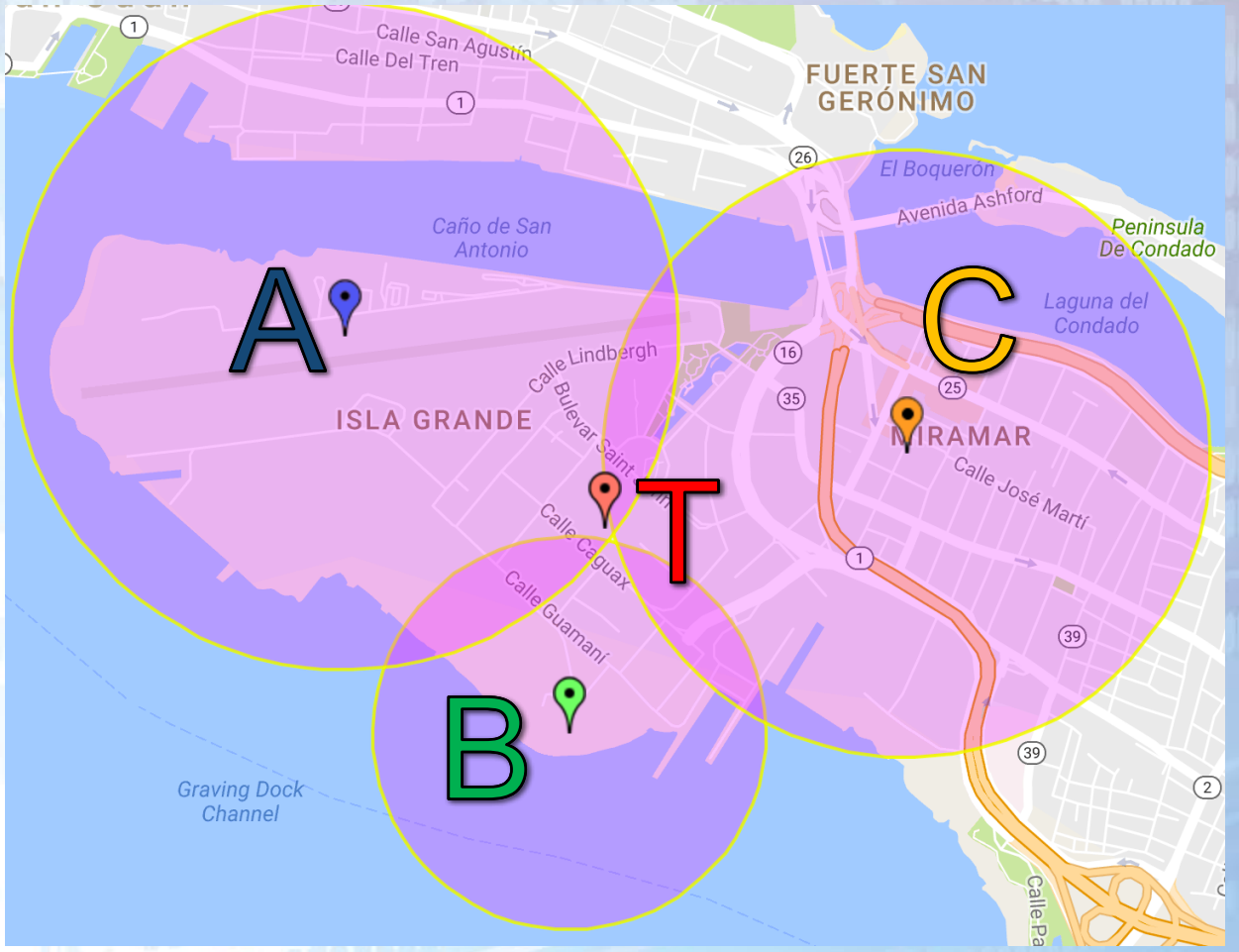
θ = *Bearing*

Bearing?



independent security evaluators

Trilateration: Illustrated



independent security evaluators

EXAMPLE TIME!

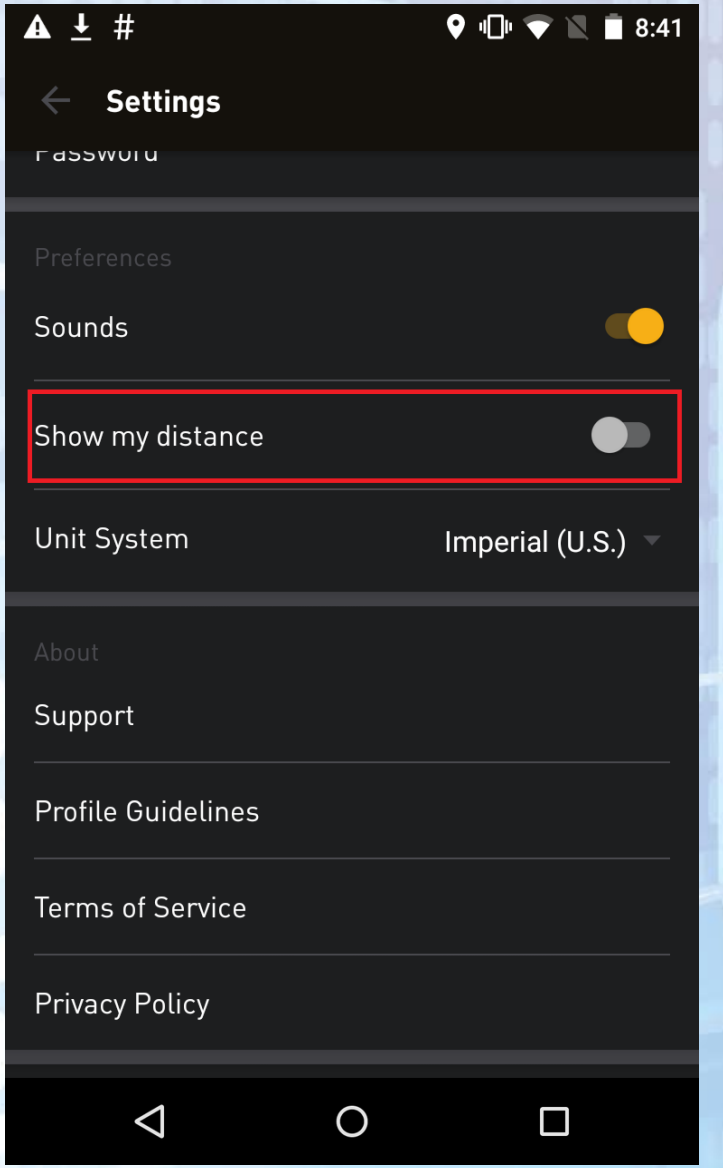
How do you fix this?

1. Allow users to opt-out of displaying their distance.

Grindr

independent security evaluators

Grindr: Settings



independent security evaluators

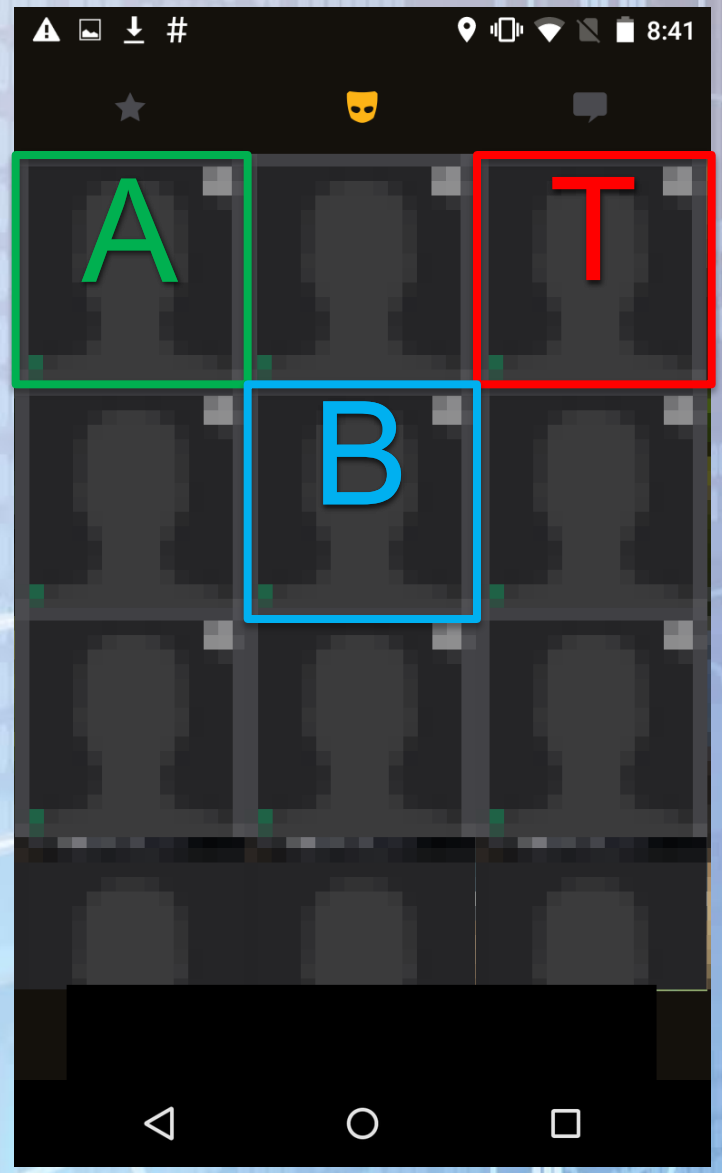
Grindr Home Screen

- Grindr Home Screen:
  - Sorts users based on their proximity to the user.

independent security evaluators

Grindr: Home Screen

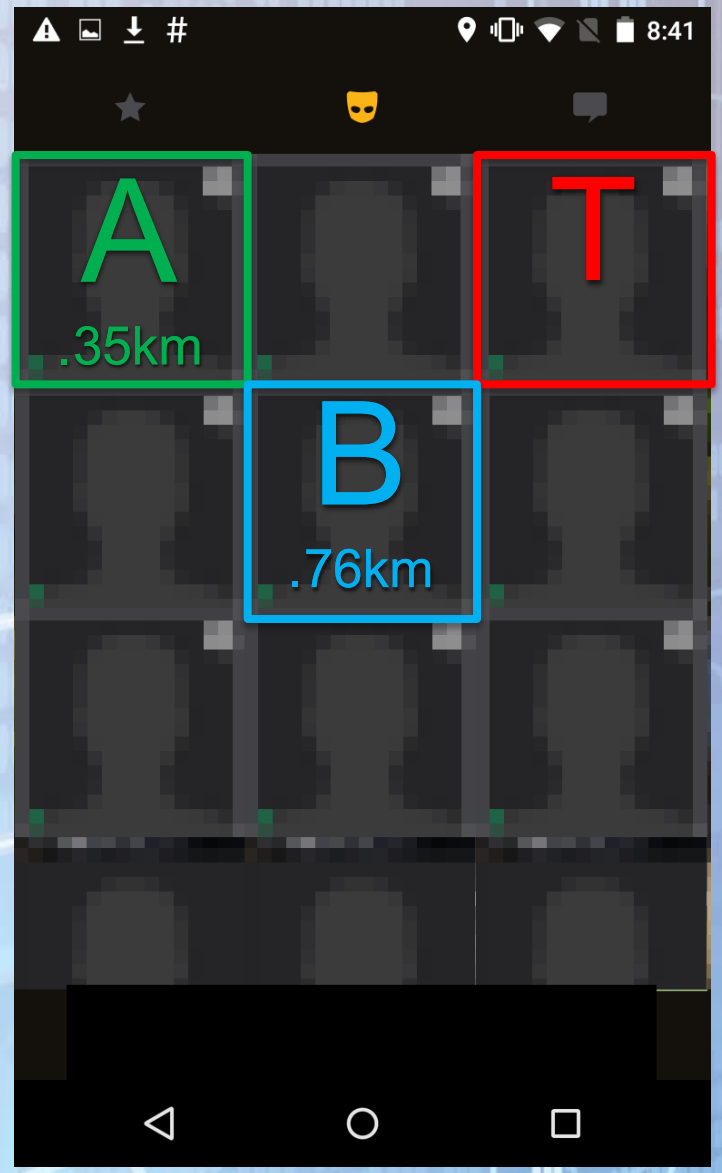
- Grindr Home Screen:
  - Sorts users based on their proximity to the user.
  - Suppose that we control users on either side of the user.



independent security evaluators

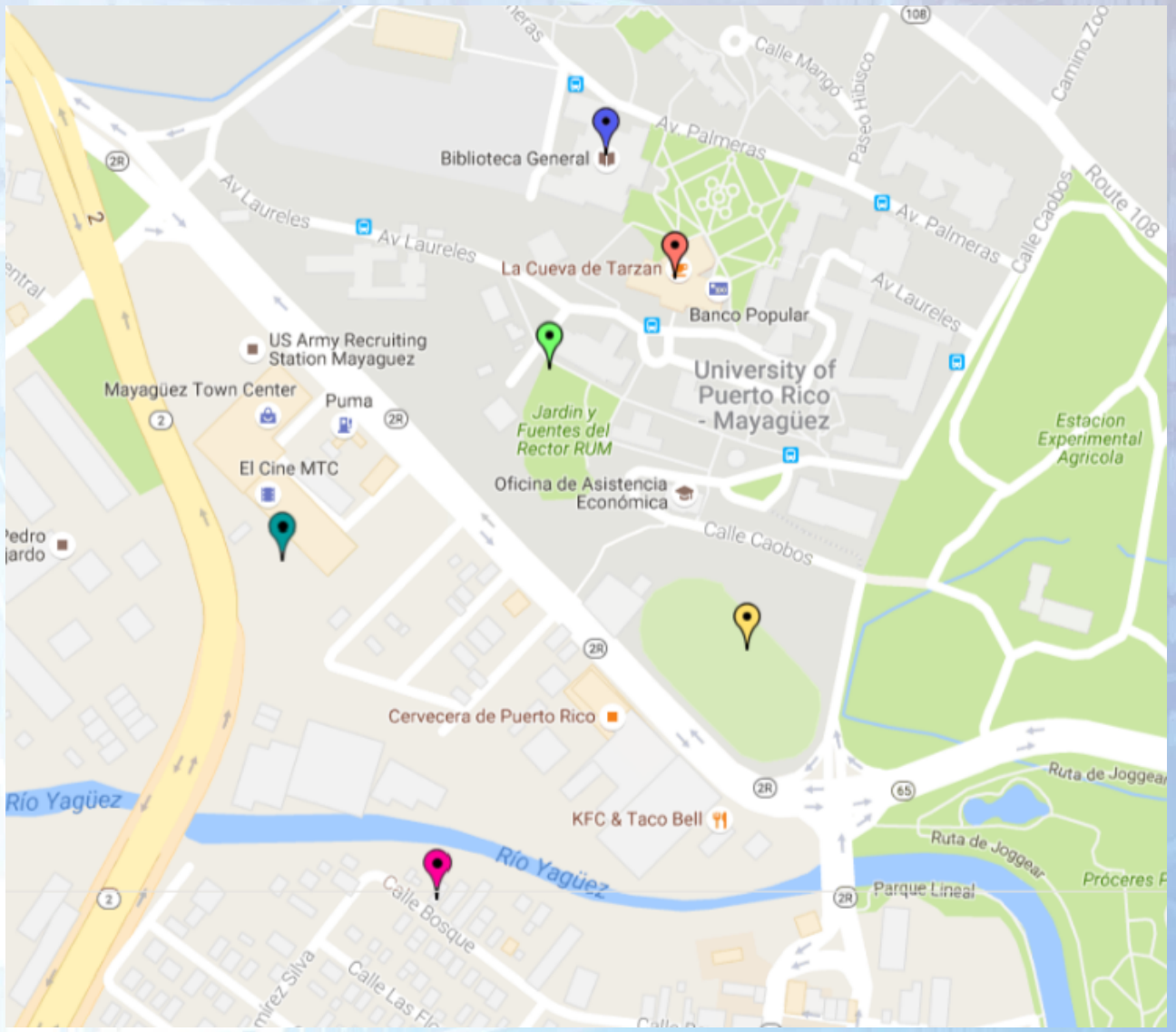
Grindr: Home Screen

- Grindr Home Screen:
  - Sorts users based on their proximity to the user.
  - Suppose that we control users on either side of the user.
  - And, we know the distance between our main user account and our controlled accounts.



independent security evaluators

Colluded Trilateration:



independent security evaluators

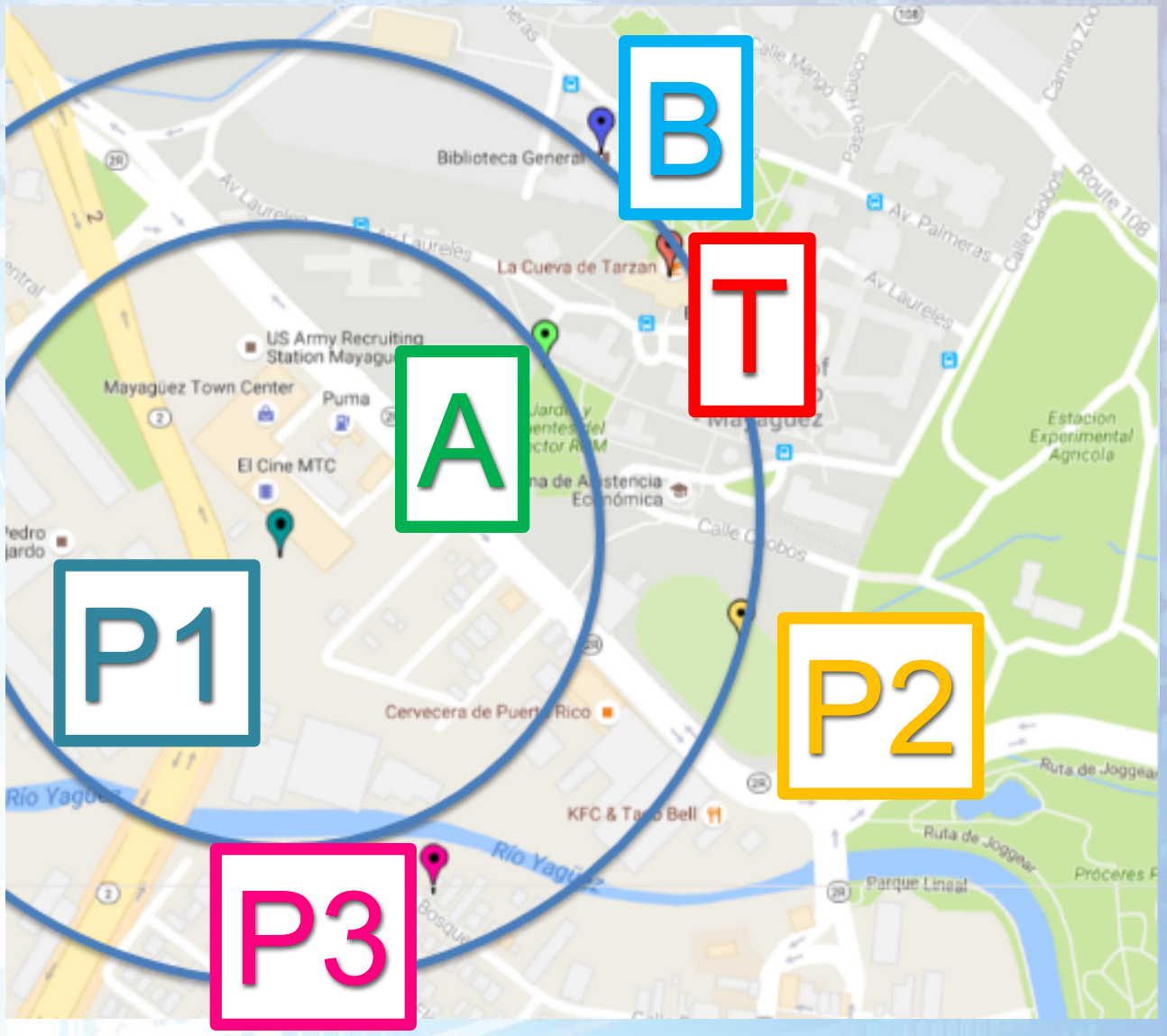
Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Colluded Trilateration:

independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

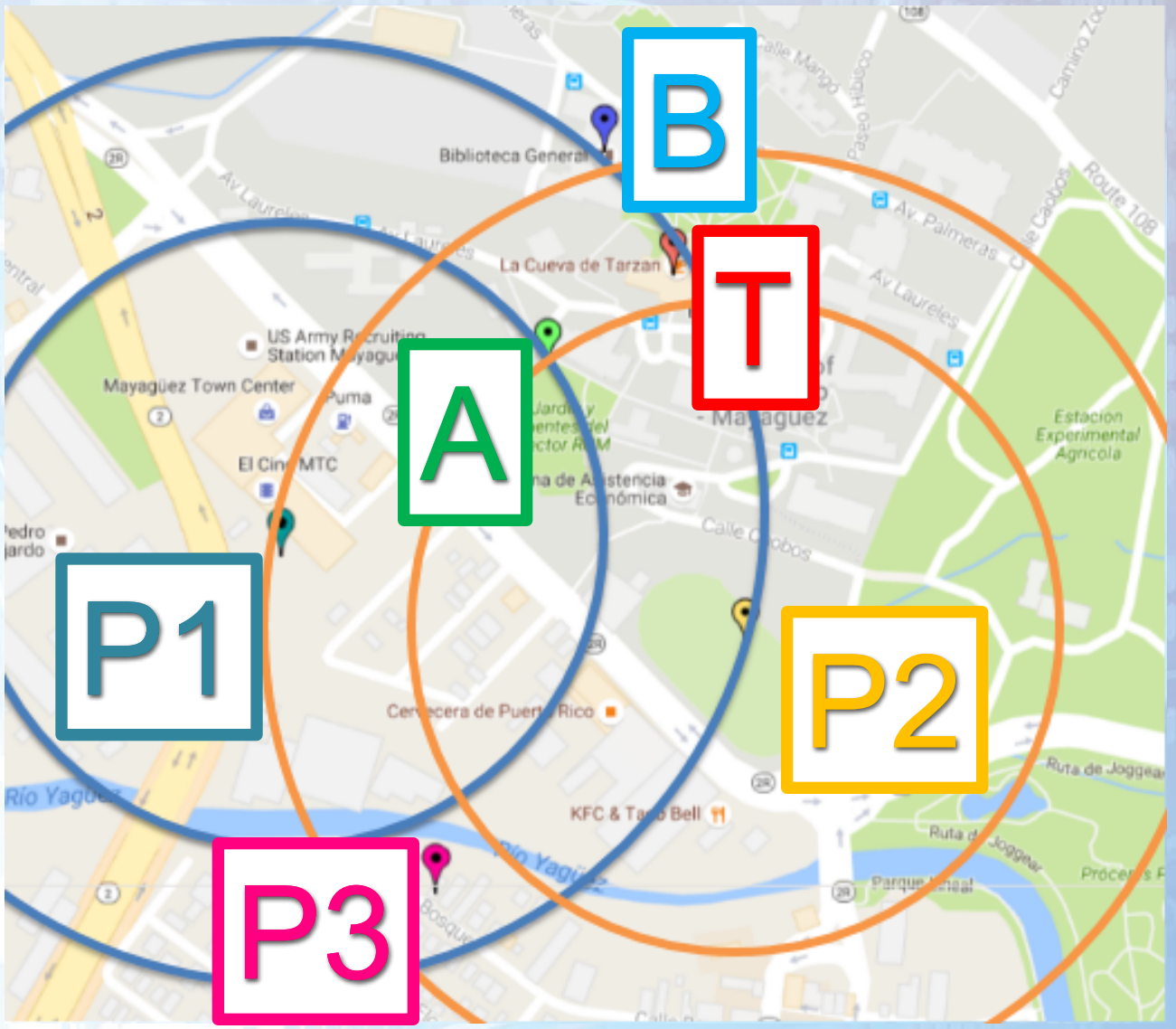
Colluded Trilateration:



independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

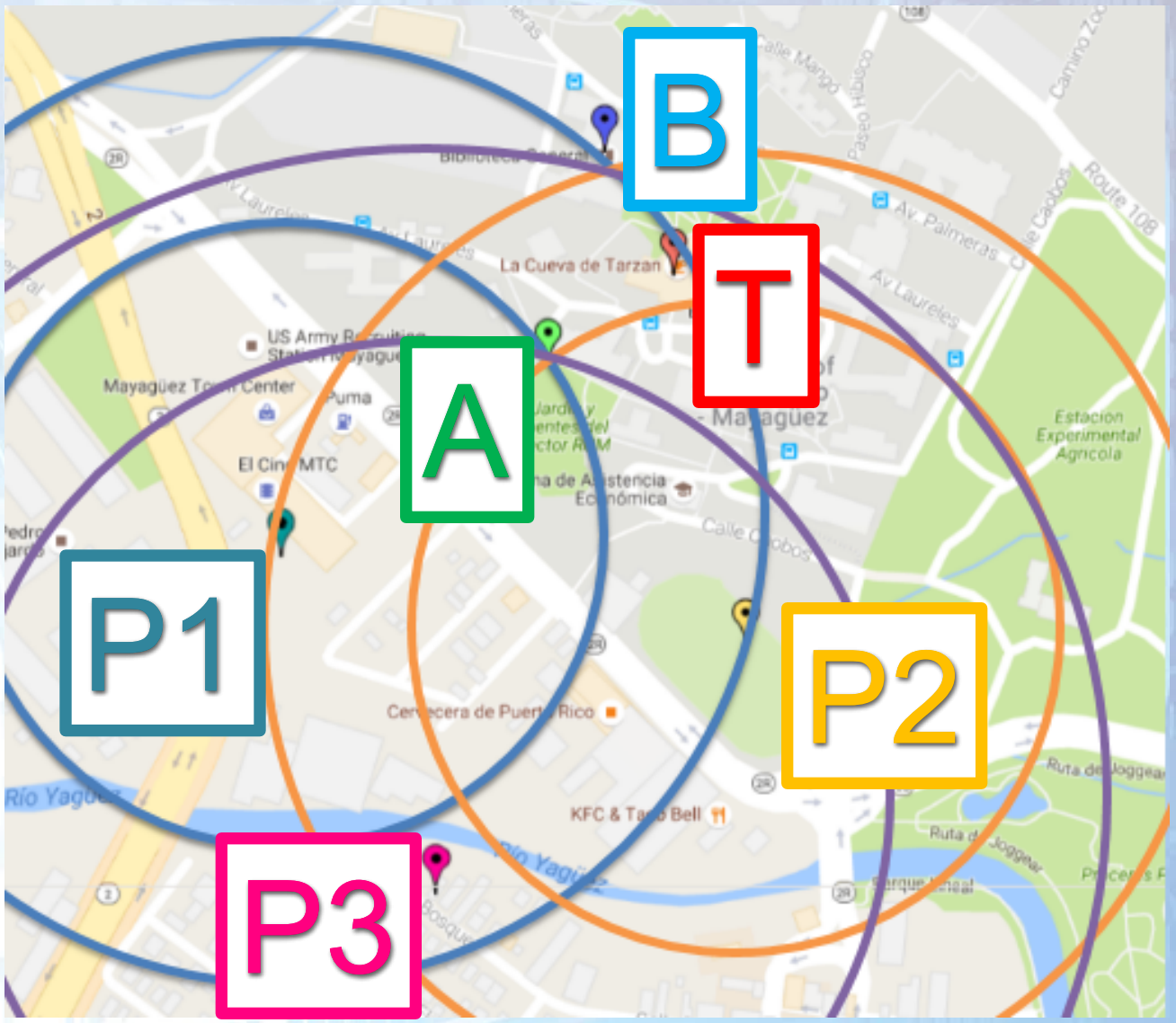
Colluded Trilateration:



independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Colluded Trilateration:



independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

How do you fix this?

1. ~~Allow users to opt-out of displaying their distance.~~
2. Prevent large distance changes.

Grindr: Ban Users

BANNED!

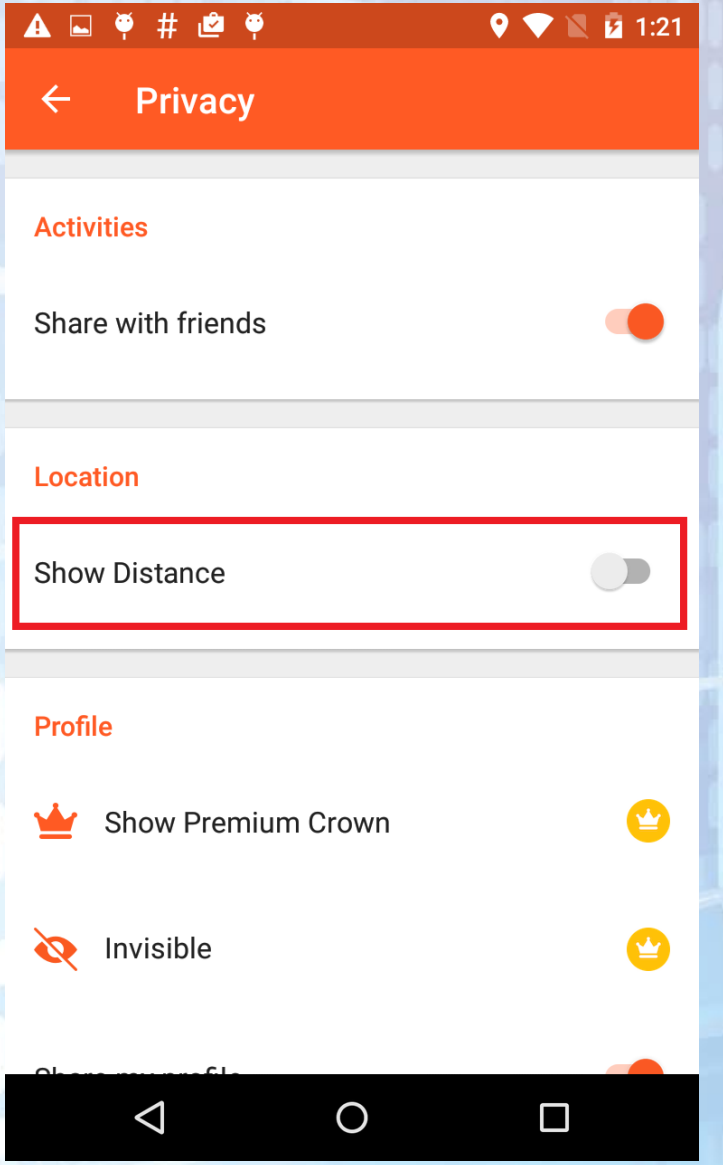
How do you fix this?

1. ~~Allow users to opt-out of displaying their distance.~~
2. ~~Prevent large changes in distance.~~
3. Obfuscate the user's distance

Hornet

independent security evaluators

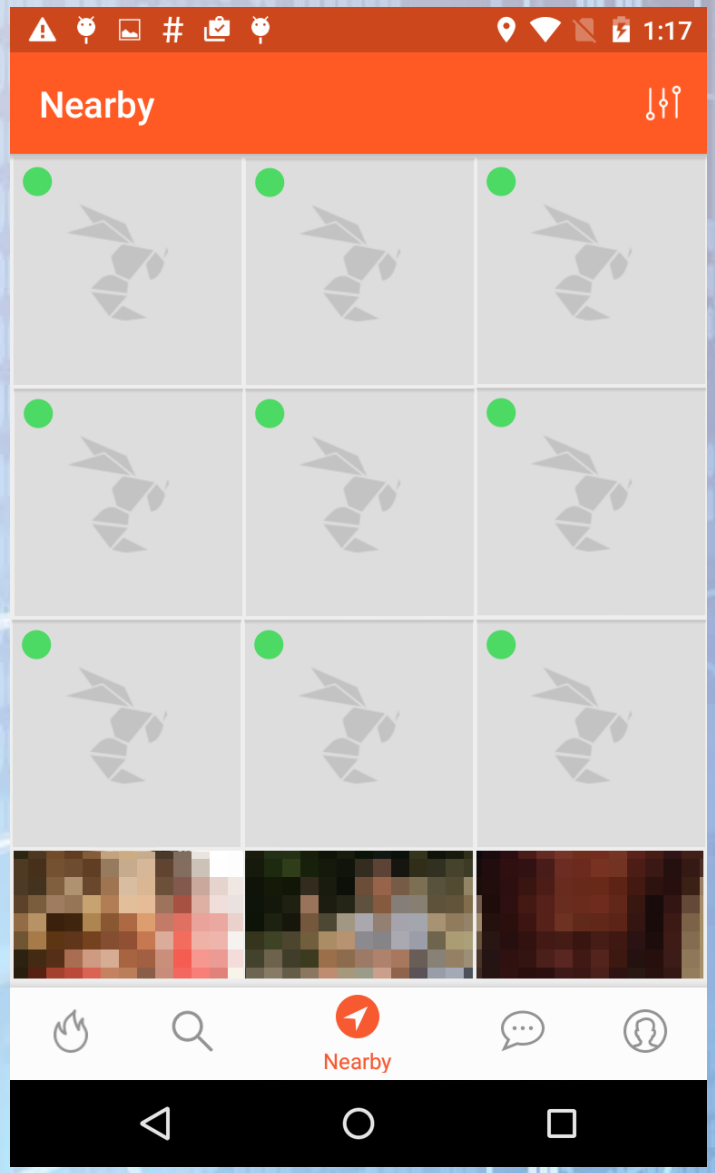
Hornet: Settings



independent security evaluators

Hornet: Home Screen

- Hornet Home Screen:
  - Sorts users based on their proximity to the user.

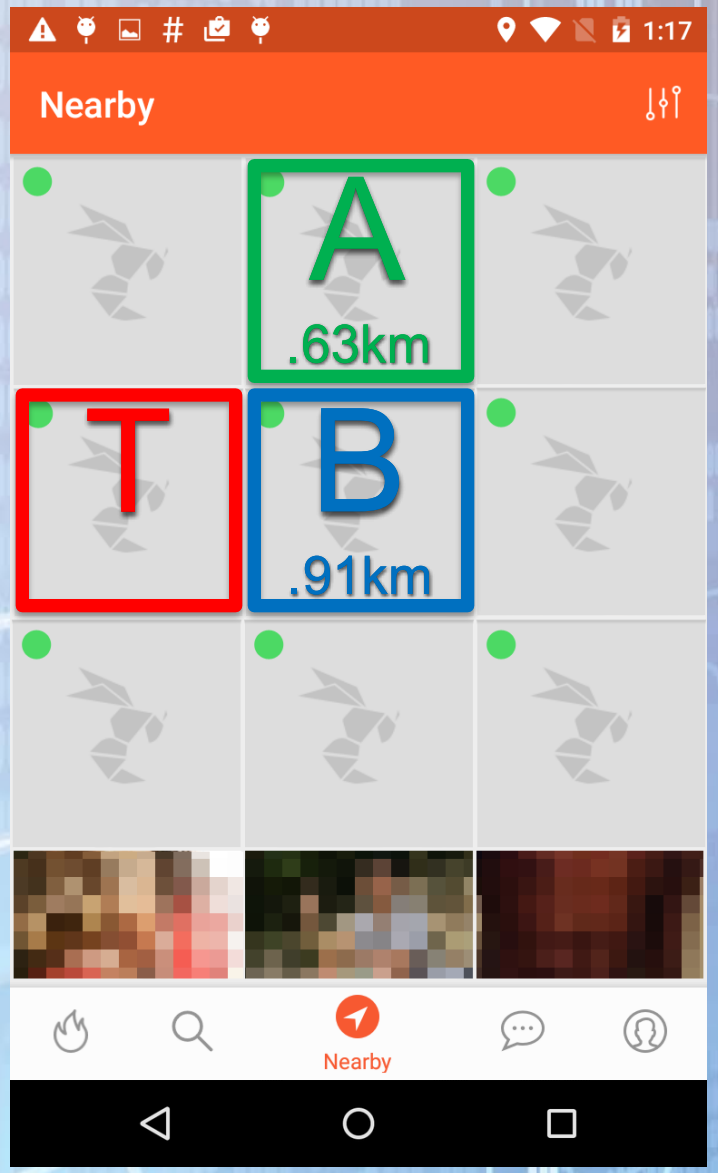


independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Hornet: Home Screen

- Hornet Home Screen:
  - Sorts users based on their proximity to the user.

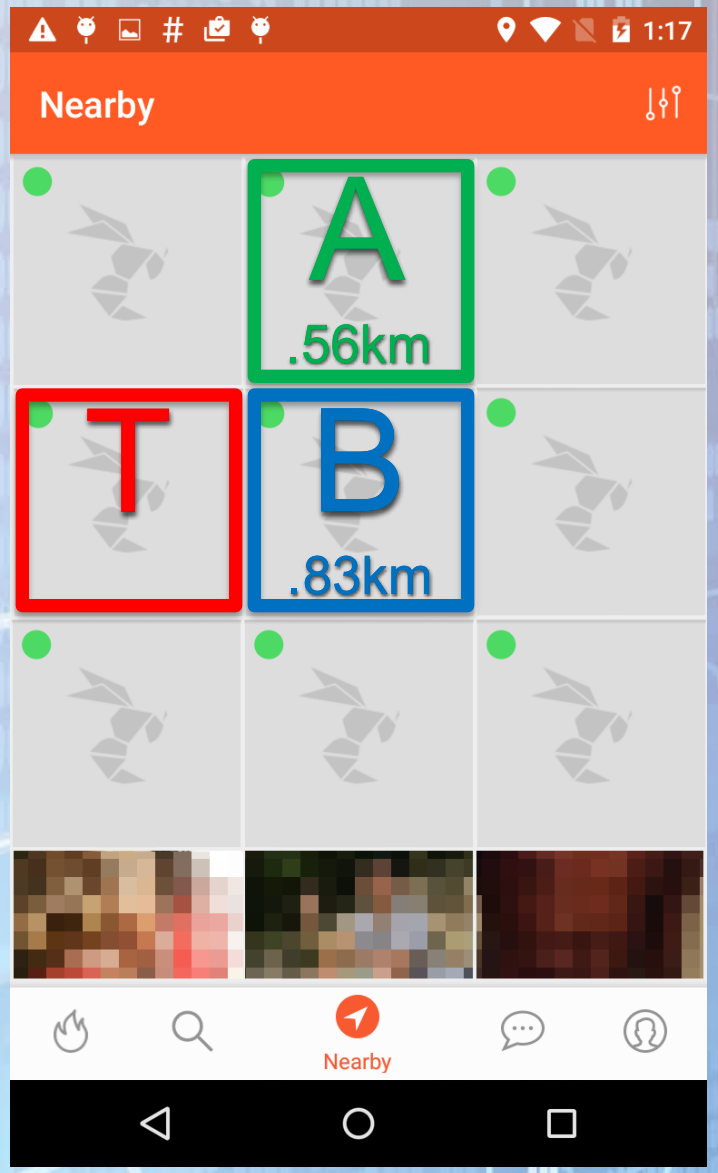


independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Hornet: Home Screen

- Hornet Home Screen:
  - Sorts users based on their proximity to the user.

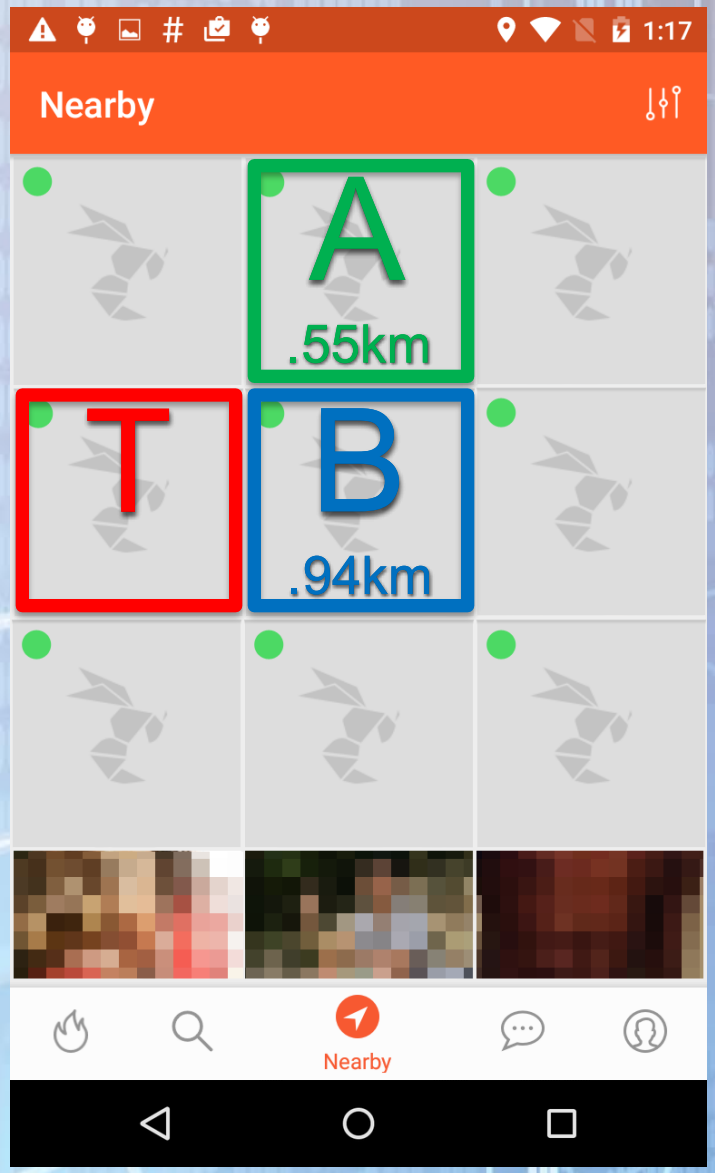


independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Hornet: Home Screen

- Hornet Home Screen:
  - Sorts users based on their proximity to the user.
  - Obfuscates the User's location by randomly adding distance to the users actual location.

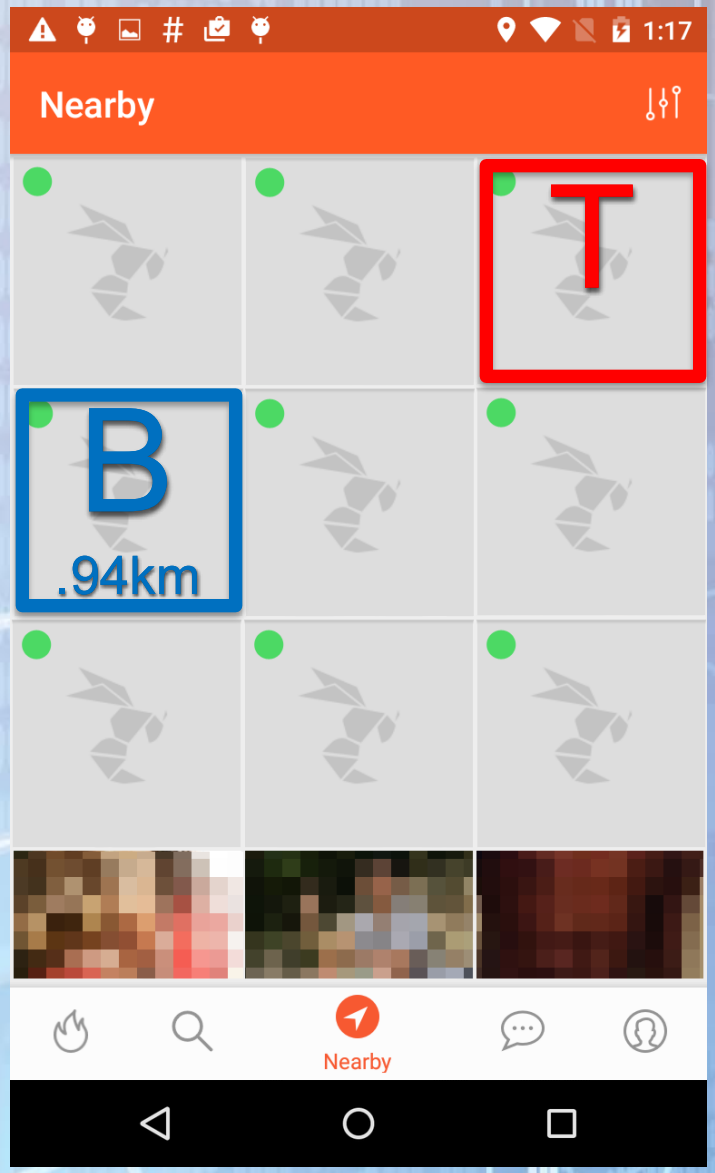


independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Hornet: Home Screen

- Hornet Home Screen:
  - Sorts users based on their proximity to the user.
  - Obfuscates the User's location by randomly adding distance to the users actual location.
  - Prevents Colluded Trilateration by randomly dropping users from the "near users" list. *(Or does it?)*

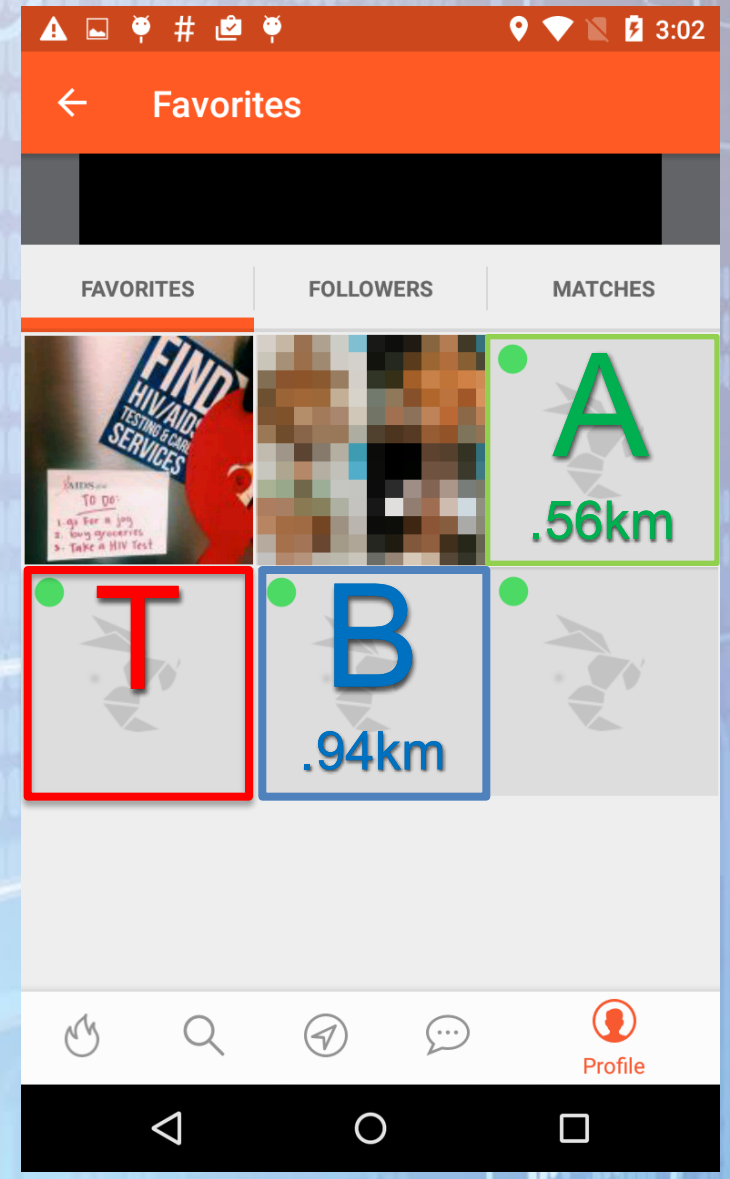


independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

Hornet: Favorites

- Hornet Favorites Screen:
  - List users you have favorited.
  - Does not remove users after issuing multiple queries.
  - Still obfuscates the user's distance by adding a random value.



independent security evaluators

Your Neighbors Are My Spies: Location and other Privacy Concerns in GLBT-focused Location-based Dating Applications (Asano, Hoang, Yoshikawa)

How do you fix this?

1. ~~Allow users to opt-out of displaying their distance.~~
2. ~~Prevent large changes in distance~~
3. ~~Obfuscate the user's distance~~
4. Only show city

How do you fix this?

1. ~~Allow users to opt-out of displaying their distance.~~
2. ~~Prevent large changes in distance~~
3. ~~Obfuscate the user's distance~~
4. ~~Only show city~~
5. Defense in-depth. (Layers of security)

How do you fix this?

1. ~~Allow users to opt-out of displaying their distance.~~
2. ~~Prevent large changes in distance~~
3. ~~Obfuscate the user's distance~~
4. ~~Only show city~~
5. ~~Defense in-depth. (Layers of security)~~
6. Disable location services for all users.

FIN