# ReCon

## Revealing and Controlling PII Leaks from Mobile Devices

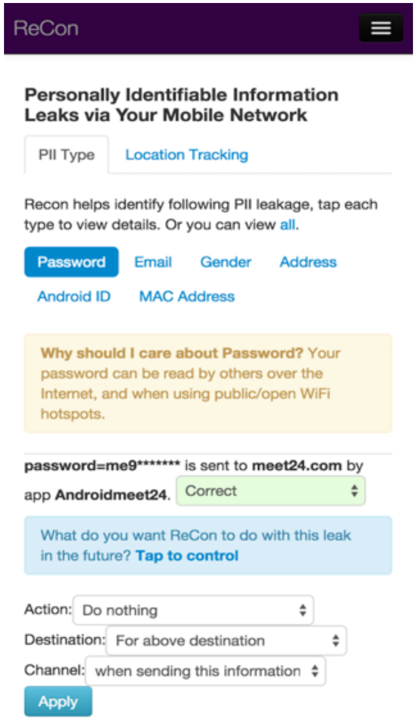
Lead PI: David Choffnes

Lead Student: Jingjing Ren

Team: Ashwin Rao, Martina Lindorfer,
Christophe Leung, Christo Wilson, Arnaud Legout

# What does your phone leak about you?

# What does your phone leak about you?



**Personally Identifiable Information Leaks via Your Mobile Network**

Recon helps identify following PII leakage, tap each type to view details. Or you can view all.

**Why should I care about Password?** Your password can be read by others over the Internet, and when using public/open WiFi hotspots.

**password=me9********* is sent to **meet24.com** by app **Androidmeet24**. Correct

What do you want ReCon to do with this leak in the future? **Tap to control**

Action: Do nothing

Destination: For above destination

Channel: when sending this information

# What does your phone leak about you?

+Z
+Y
+X
ITG-3200
MIC
N
S

Network Trace Analysis

Machine Learning

CrowdSourcing

# Key Results: User study

IRB-approved user study (382 users as of November)

- 220 iOS, 197 Android devices
- 20/26 responses: system useful & behavior change
- PII found: 27,009 cases (12,318 confirmed)

Some details

- ***199 cases of credential leaks***, 168 verified
- Average leaks: iOS > Android ☹
- Unexpected, suspicious leaks
  - Recipe/cooking app tracks location
  - Video/Game/News app leaks gender

# Data Available

Anonymized leaks

- What type of PII
- Which app sent it
- Who received it
- HTTP or HTTPS

Controlled study

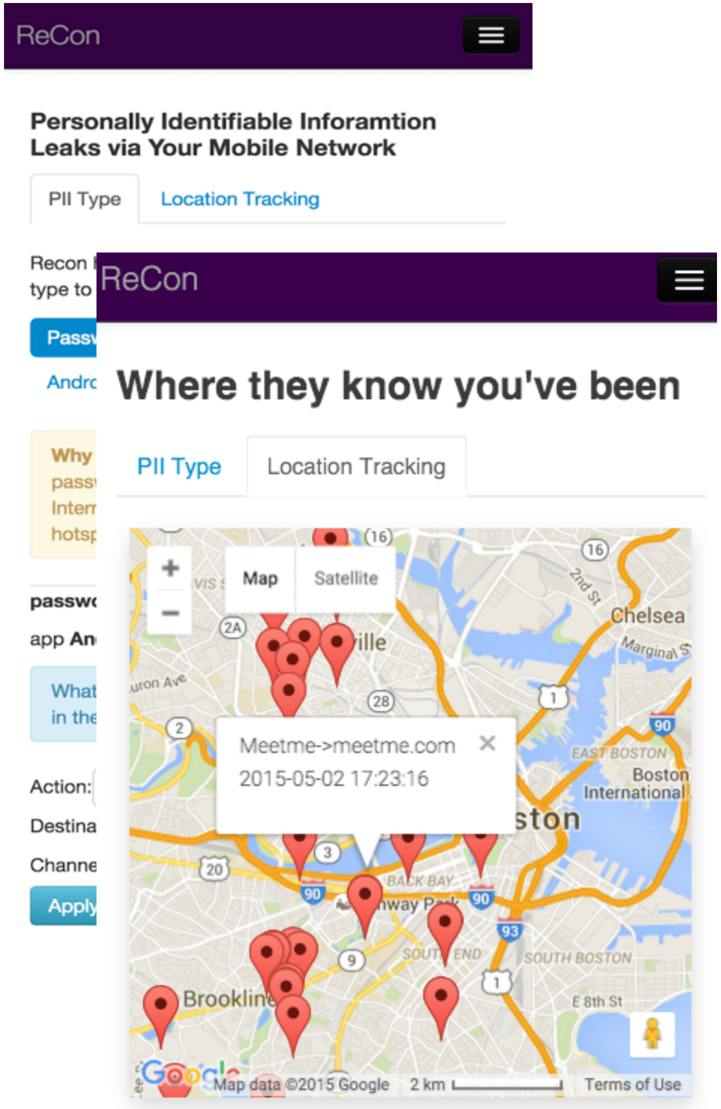
- All PII types/values for apps and some web sites as well

All of this over time

# Hack ideas (1)

Make our ReCon UIs better

- Better dashboard
- New forms of visualizations
- New services using add-on apps



ReCon

Personally Identifiable Inforamtion Leaks via Your Mobile Network

PII Type | Location Tracking

Recon i
type to

Passw

Andro

Why
pass
Interr
hotsp

passwo

app An

What
in the

Action:

Destina

Channe

Apply

ReCon

Where they know you've been

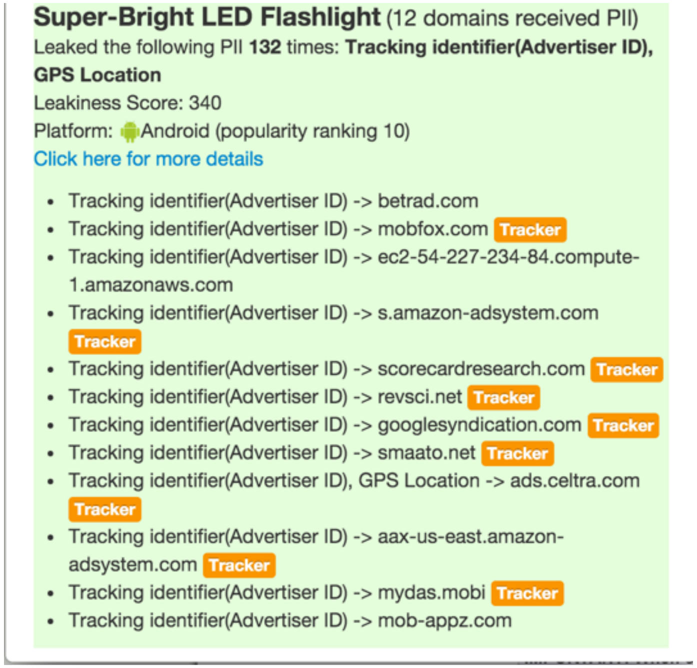
PII Type | Location Tracking

Meetme->meetme.com
2015-05-02 17:23:16

# Hack ideas (2)

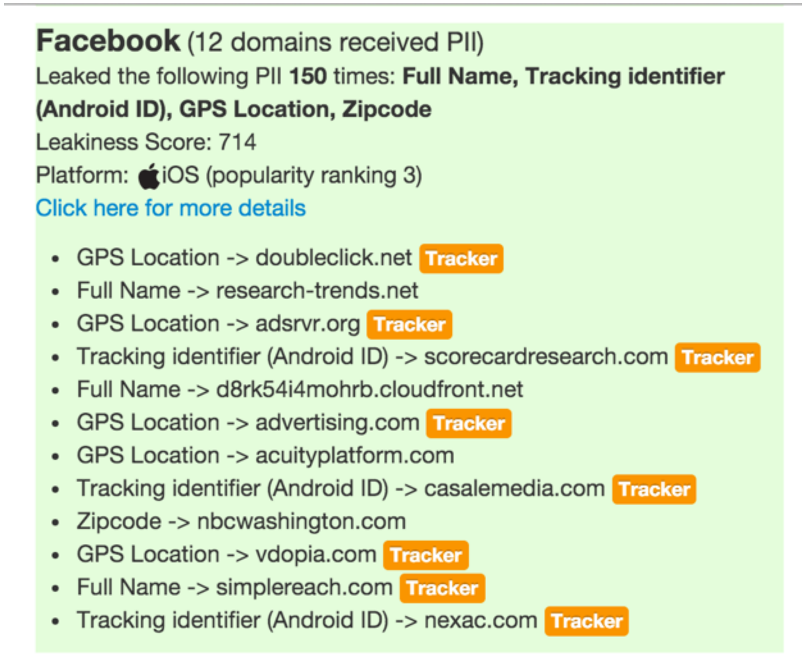
Make our online reports better

- App report is a bit clunky
- Better ways to map user-agent (and other traffic) to app
- Visualize leaks over time



**Super-Bright LED Flashlight** (12 domains received PII)
Leaked the following PII **132** times: **Tracking identifier(Advertiser ID), GPS Location**
Leakiness Score: 340
Platform: Android (popularity ranking 10)
Click here for more details

- Tracking identifier(Advertiser ID) -> betrad.com
- Tracking identifier(Advertiser ID) -> mobfox.com Tracker
- Tracking identifier(Advertiser ID) -> ec2-54-227-234-84.compute-1.amazonaws.com
- Tracking identifier(Advertiser ID) -> s.amazon-adsystem.com Tracker
- Tracking identifier(Advertiser ID) -> scorecardresearch.com Tracker
- Tracking identifier(Advertiser ID) -> revsci.net Tracker
- Tracking identifier(Advertiser ID) -> googlesyndication.com Tracker
- Tracking identifier(Advertiser ID) -> smaato.net Tracker
- Tracking identifier(Advertiser ID), GPS Location -> ads.celtra.com Tracker
- Tracking identifier(Advertiser ID) -> aax-us-east.amazon-adsystem.com Tracker
- Tracking identifier(Advertiser ID) -> mydas.mobi Tracker
- Tracking identifier(Advertiser ID) -> mob-appz.com



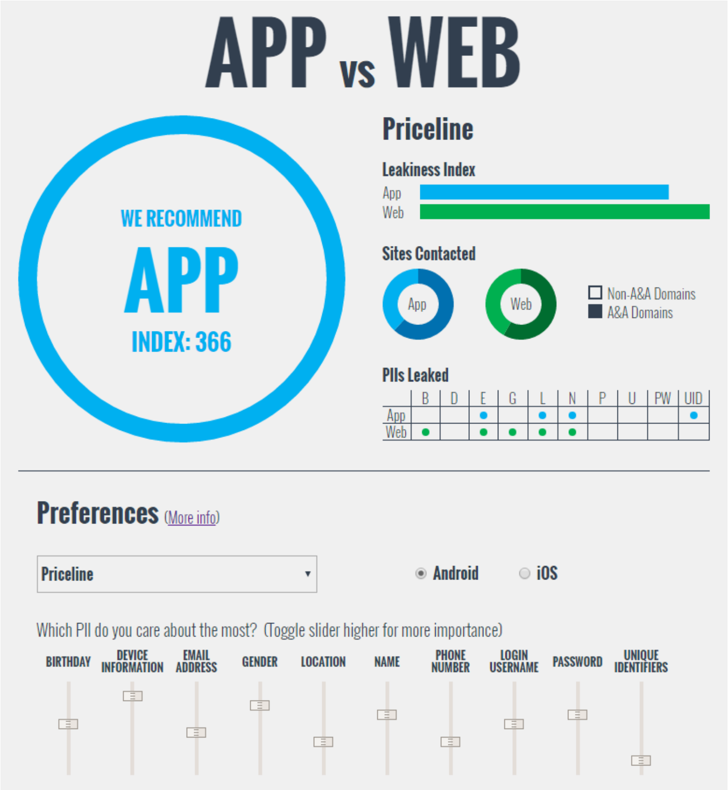
**Facebook** (12 domains received PII)
Leaked the following PII **150** times: **Full Name, Tracking identifier (Android ID), GPS Location, Zipcode**
Leakiness Score: 714
Platform: iOS (popularity ranking 3)
Click here for more details

- GPS Location -> doubleclick.net Tracker
- Full Name -> research-trends.net
- GPS Location -> adsrvr.org Tracker
- Tracking identifier (Android ID) -> scorecardresearch.com Tracker
- Full Name -> d8rk54i4mohrb.cloudfront.net
- GPS Location -> advertising.com Tracker
- GPS Location -> acuityplatform.com
- Tracking identifier (Android ID) -> casalemedia.com Tracker
- Zipcode -> nbcwashington.com
- GPS Location -> vdopia.com Tracker
- Full Name -> simplereach.com Tracker
- Tracking identifier (Android ID) -> nexac.com Tracker

# Hack ideas (3)

Improve our App vs Web visualization

- More information encoded into the page
- Include more user customization



APP vs WEB

WE RECOMMEND

APP

INDEX: 366

Priceline

Leakiness Index

Sites Contacted

PIIs Leaked

| | B | D | E | G | L | N | P | U | PW | UID |
|---|---|---|---|---|---|---|---|---|---|---|
| App | | | ● | | ● | ● | | | | ● |
| Web | ● | | ● | ● | ● | ● | | | | |

Preferences (More info)

Priceline ▾

● Android ○ iOS

Which PII do you care about the most? (Toggle slider higher for more importance)

# We’re here to help

Jingjing Ren

(lead ReCon developer)

Christophe Leung
(App vs Web)