

The Long-Standing Privacy Debate: Mobile Websites Vs Mobile Apps

Panagiotis Papadopoulos

Elias P. Papadopoulos, Michalis Diamantaris, Thanasis Petsas,
Sotiris Ioannidis, Evangelos P. Markatos



Every online service provides a website + an app

Apple's App Store Is Growing by 1,000+ Apps a Day

Number of new apps submitted to Apple's App Store per month



@StatistaCharts Source: pocketgamer.biz

statista

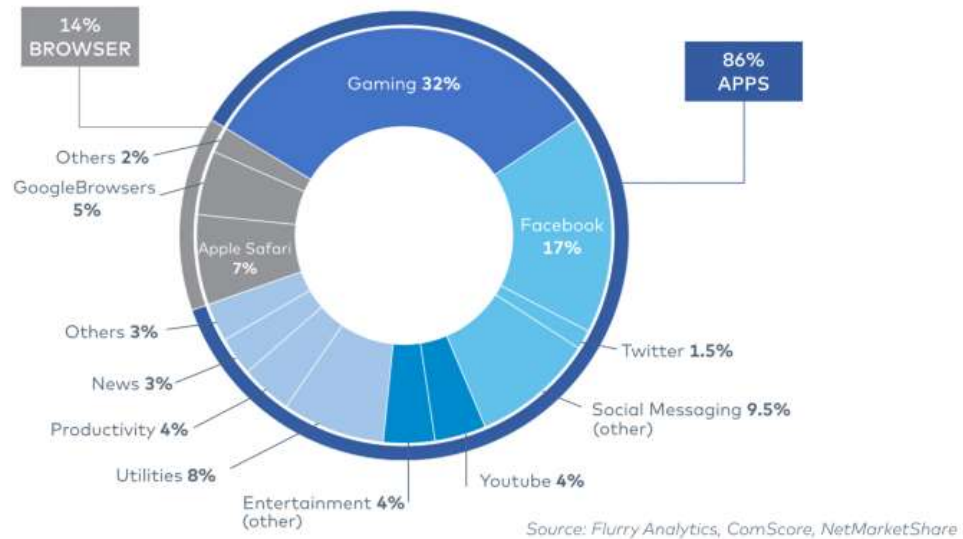
proliferation of mobile devices
+
developer tools



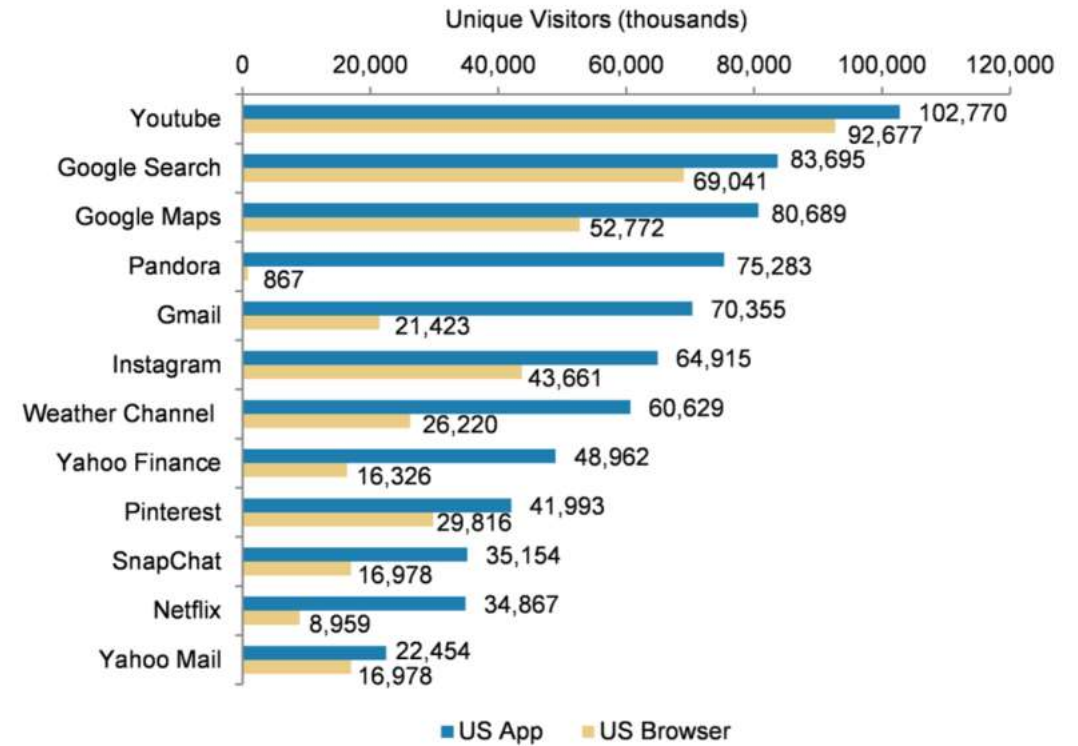
Mobile App Development Boom

The Long-standing debate: Web Vs App

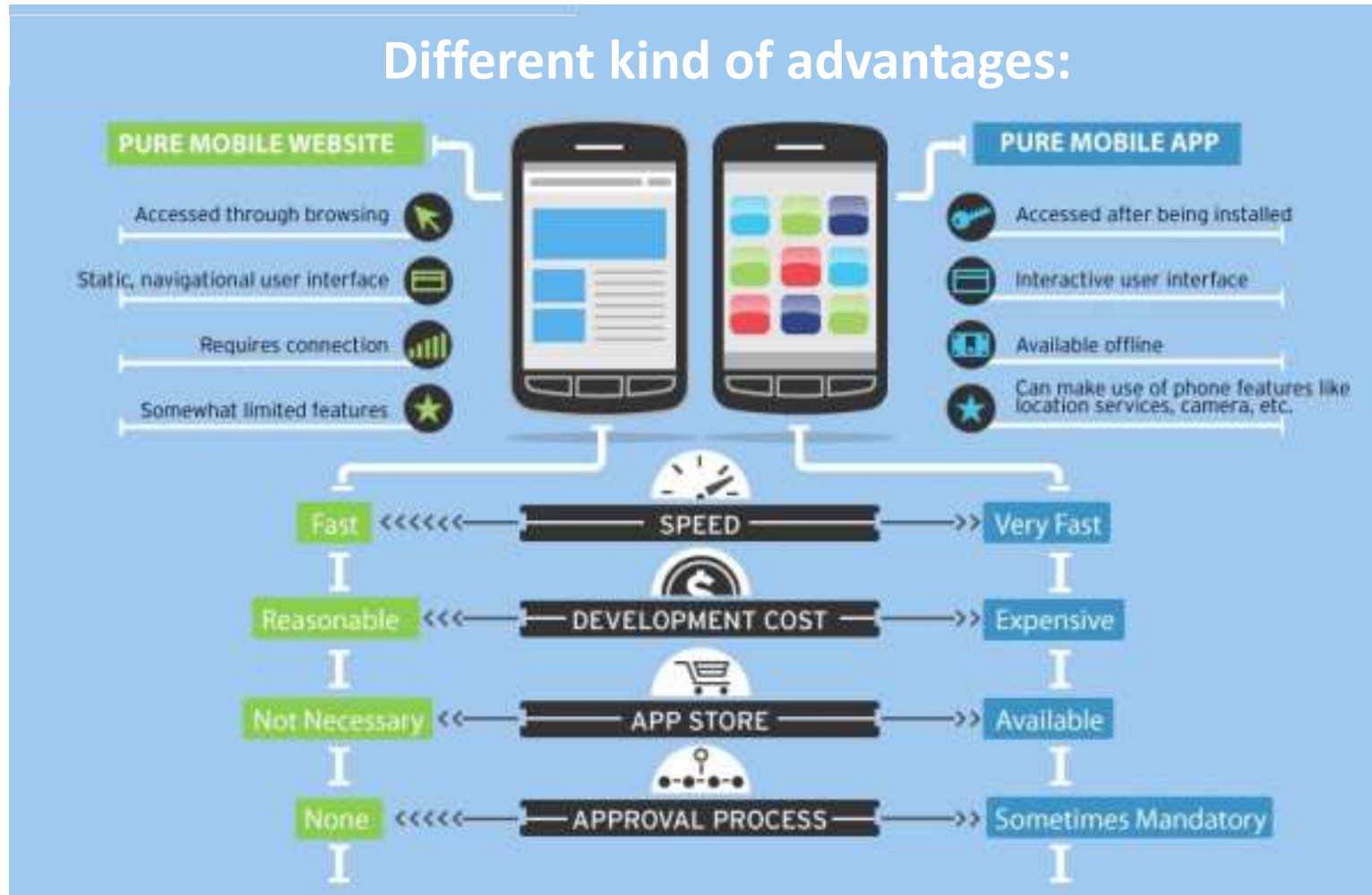
Time Spent on iOS and Android Connected Devices



- We spent more time in mobile apps
- Mobile web tends to draw more unique visitors



The Long-standing debate: Web Vs App





what about the user's privacy?

Privacy Analysis


A service may leak:

- personal data
 - (e.g. birth-date, email addresses, gender, etc.)
- device-specific information
 - can be used as identifiers
 - allow a tracker to follow **cookielessly** users in the network
 - link **web** with **app** sessions
 - correlate **anonymous** (such as TOR) sessions with **eponymous** ones.

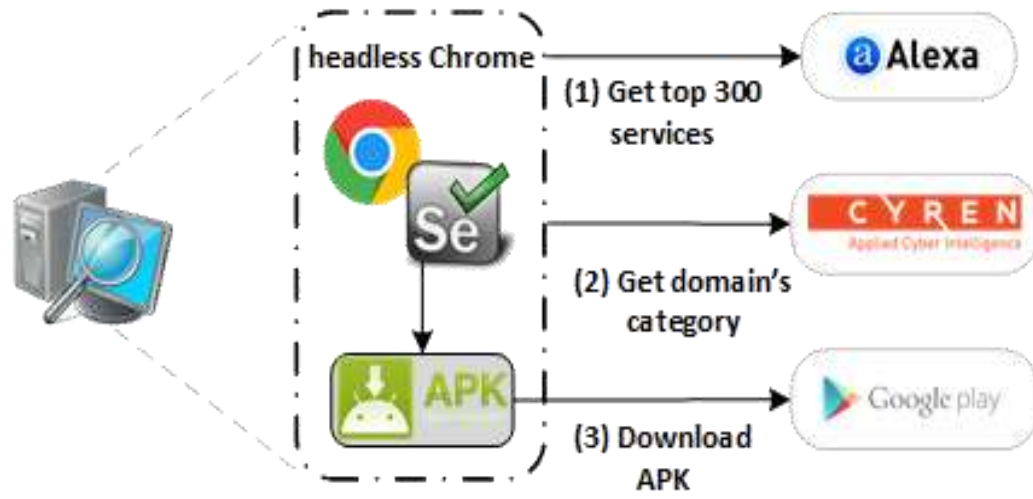
In this study...

- ✓ apps or web facilitates the most privacy leaks?
- ✓ broad definition of privacy

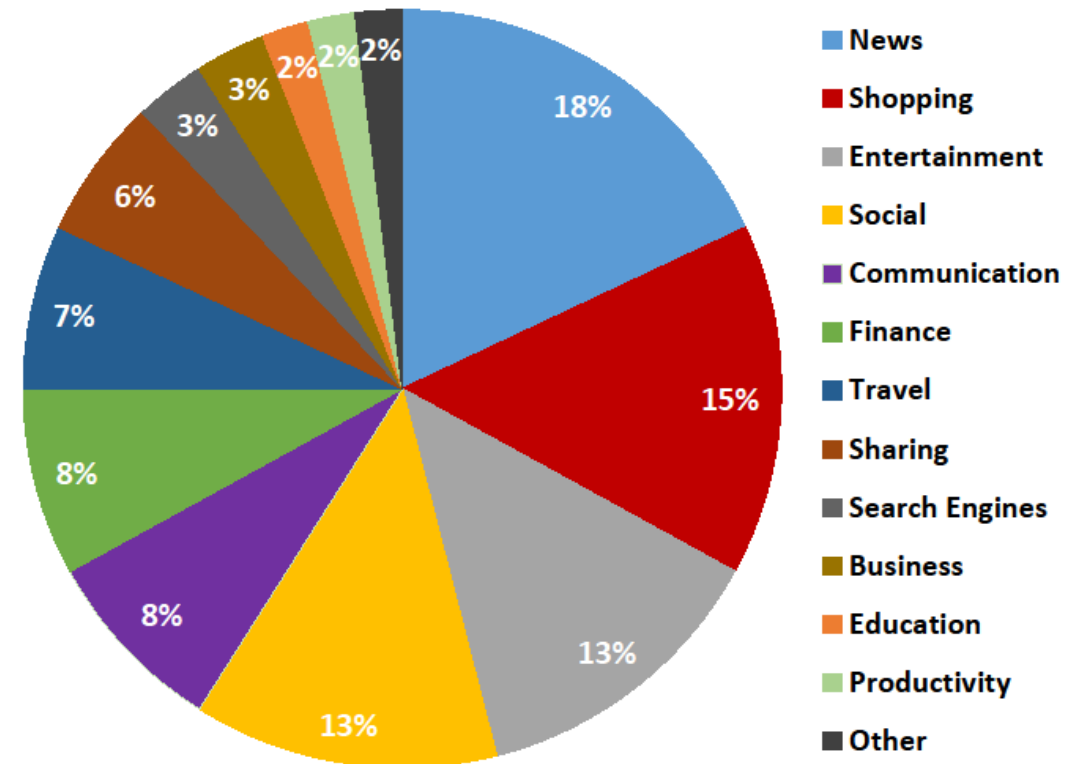
To achieve that:

- dataset of 116 top Alexa services:  mobile app
+
website
- head-to-head comparison regarding privacy leaks
- *antiTrackDroid*: anti-tracking mechanism for mobile devices.

Our dataset

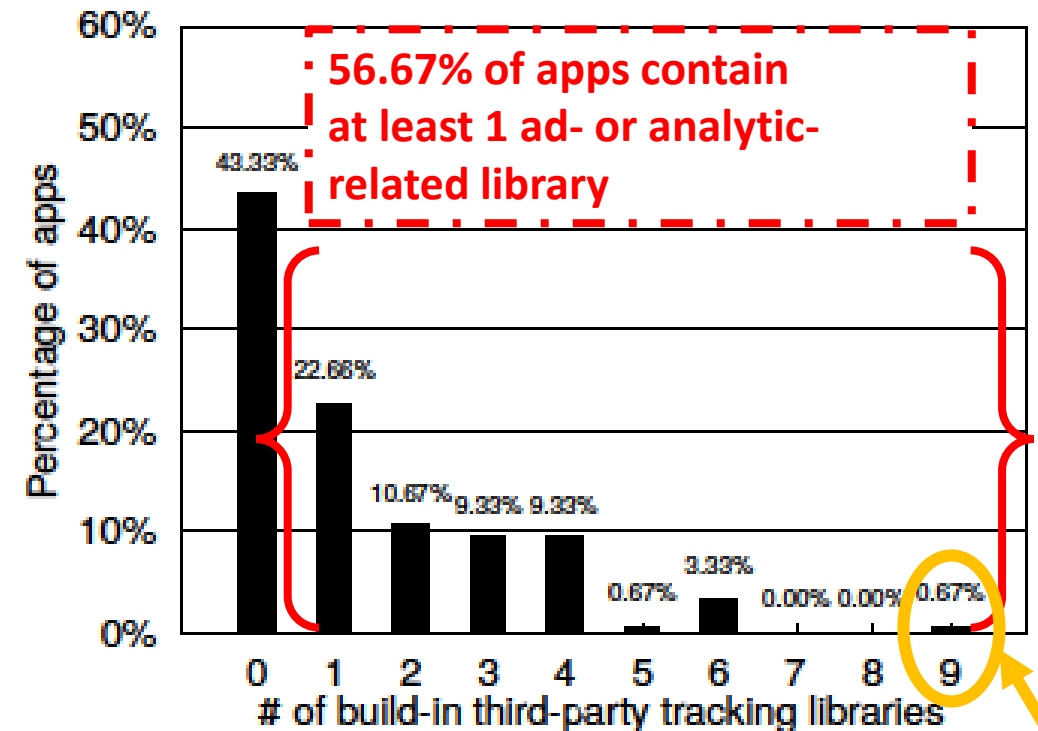


biggest chunks regard News Shopping and Entertainment-related services



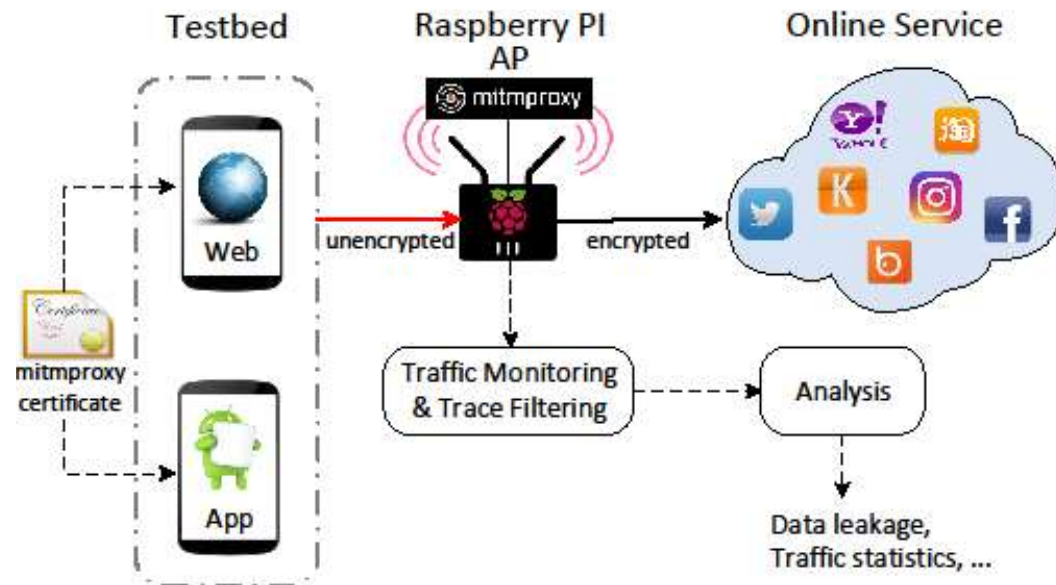
In-app libraries

- free apps embed a third party in-app library.
- Some of them used for analytics- and ad- related purposes
- Inherit all of the app's permissions (access to the phone & SMS, access to contacts list, access to device characteristics, etc.)



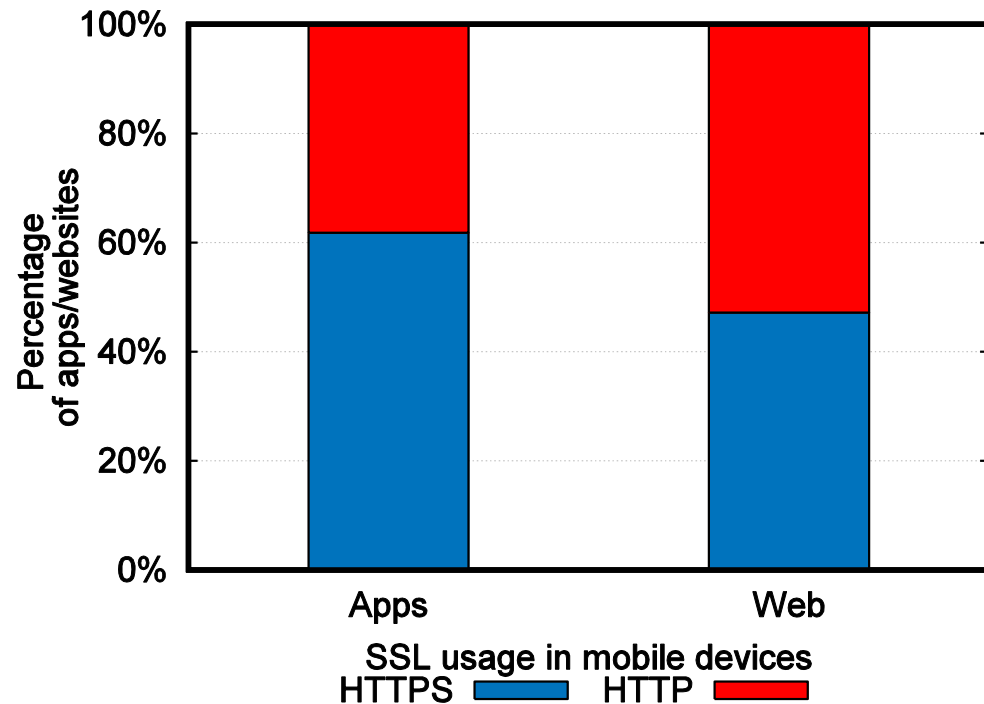
1 app uses 9 of such in-app libraries!!!

Monitoring Outgoing Traffic



- NEXUS 6 smartphone running Android 6.0.1
- Capture traffic: raspberry PI 2 -> SSL-capable monitoring proxy
- Run each service for 20 mins:
 - through web (Firefox mobile browser)
 - through app
- Filter possible leaked identifiers (pattern matching)

Privacy Leak Analysis - Encrypted sessions



- SSL in apps -> 62% of total app-traffic
- SSL in web -> 47% of total web-traffic

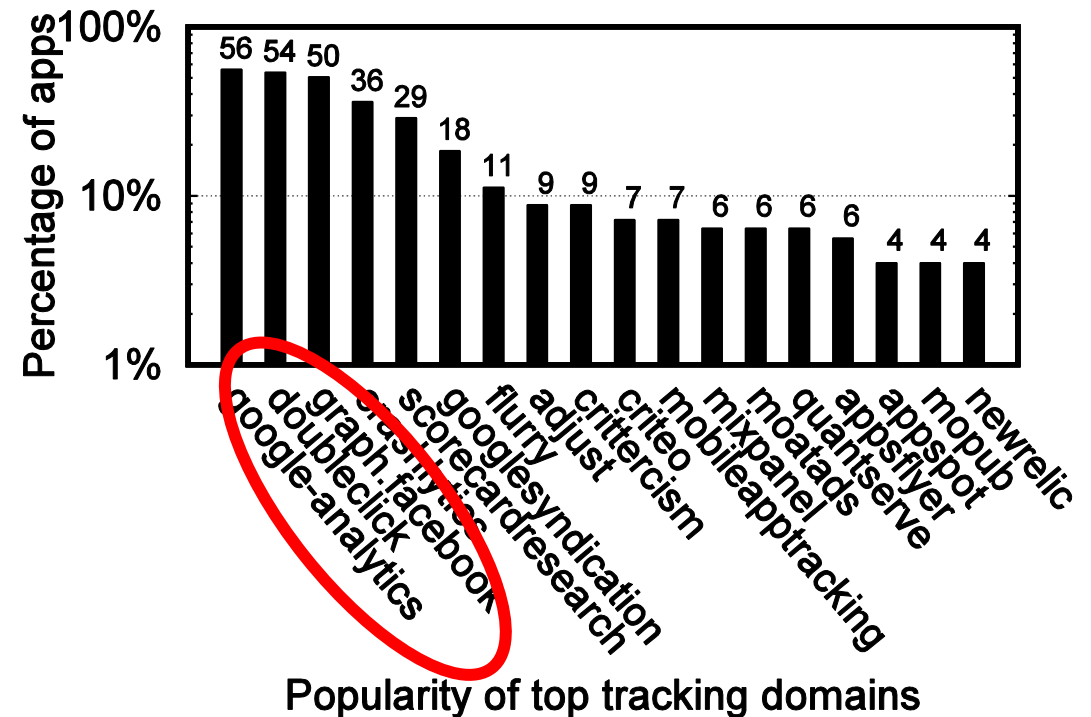
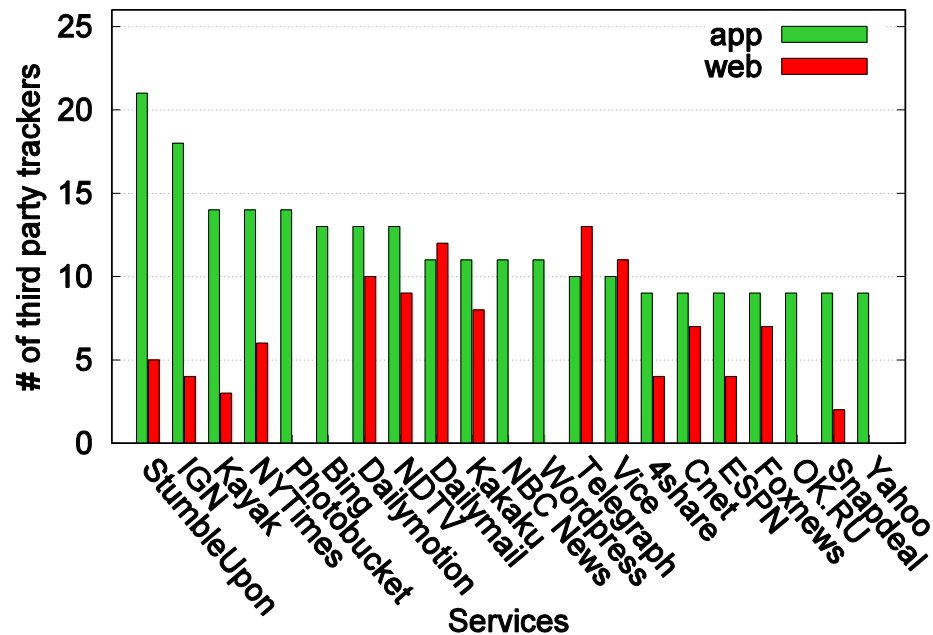
In addition:

- ✓ only 18.97% of apps use exclusively HTTPS
- ✓ 78.45% a susceptible mixture of both HTTP and HTTPS.

Privacy Leak Analysis – Type of leaks

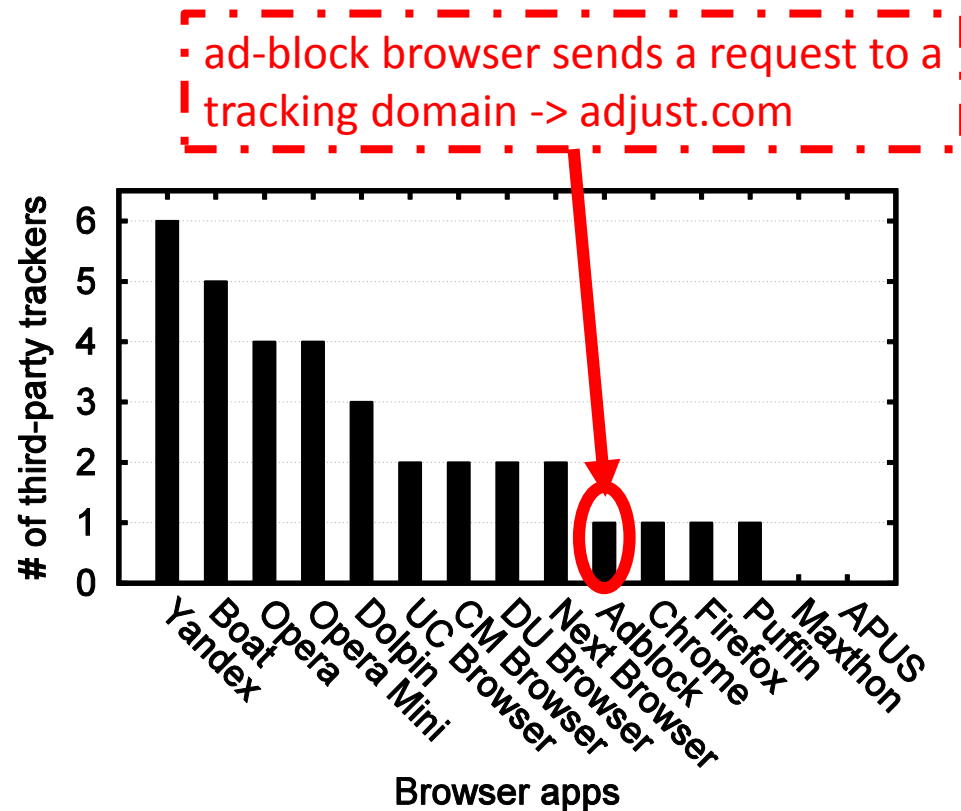
- 57.76% of the apps leak the **Android ID** identifier (not accessible from websites)
- 3.45% of the apps leak the **list of installed apps** (not accessible from websites)
 - 1 received a response with an approximation of **the user's gender, age range**, a list of **possible interests** and a number of recommended brand names
- 4.31% of the apps leak **nearby WiFi APs**
 - current geolocation and possible interpersonal relations of people in the same location at the same time
 - 1 app leaked the entire list of known APs (-> previous locations the user has visited)
- 85.34% of mobile websites leak **GPS coordinates** (Vs. 66.38% of apps)

Privacy Leak Analysis - Diffusion of privacy leaks



- apps leak information to an **average of 11.7** trackers (-> websites to an **average of 5** trackers.)
- **94% of apps** leak data to 1 or more trackers, (-> **69% in websites**).

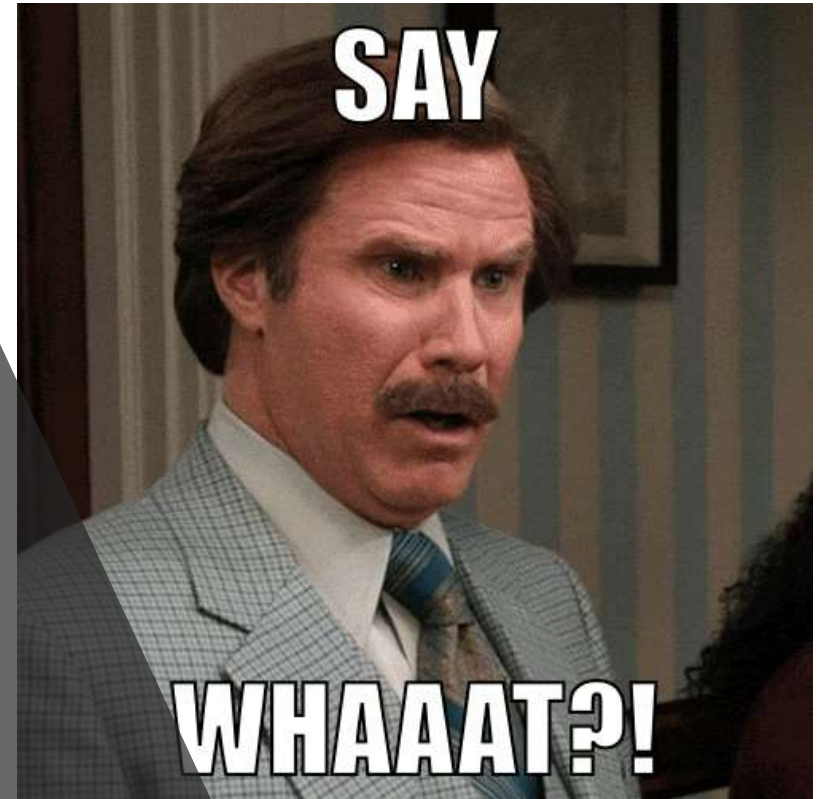
Mobile browsers leak too...



- websites are being accessed through mobile browsers
- mobile browsers are apps, too
 - ✓ install 15 popular mobile browsers
 - ✓ fetch google.com
 - ✓ monitor traffic

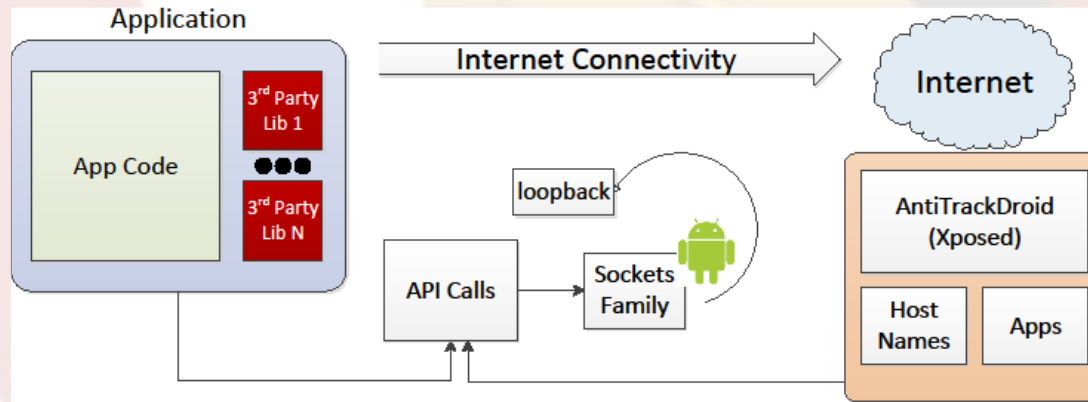
So, if you care about
your privacy:

Don't use mobile apps...

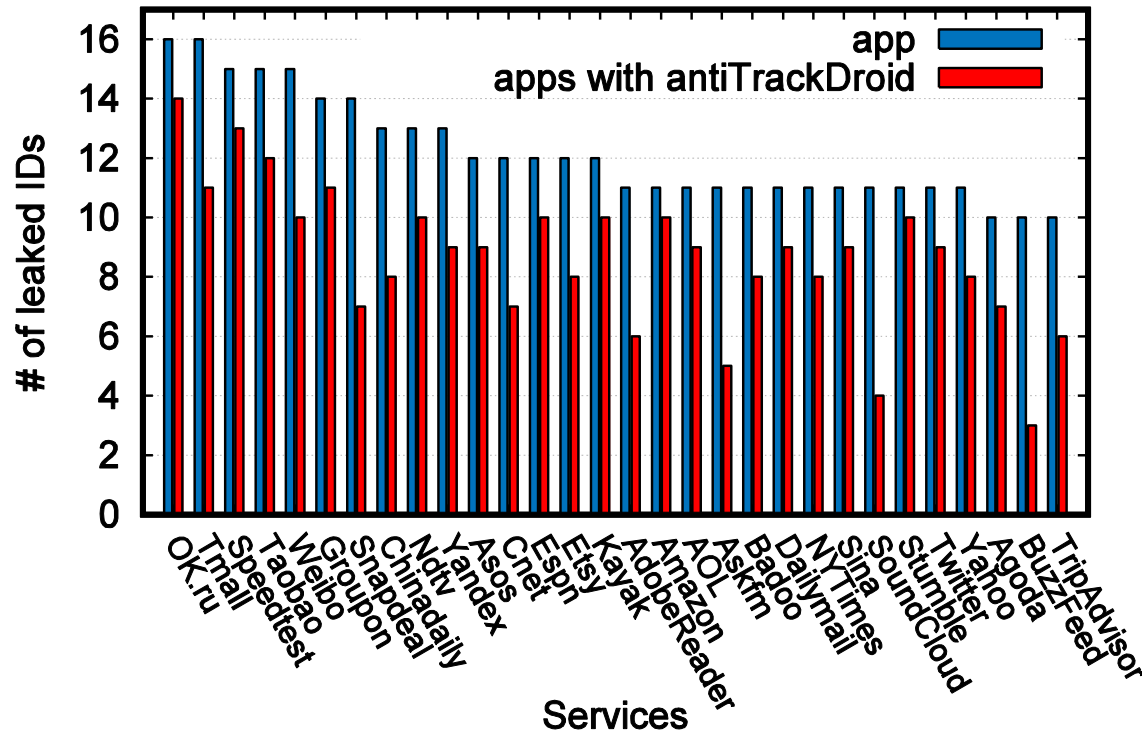


Our approach: *antiTrackDroid*

- filters and blocks outgoing requests leaking personal and device information to 3rd party trackers
- core design principles:
 - ✓ app-independent
 - ✓ no additional infrastructure (VPN, proxy)
- by leveraging Xposed framework:
 - ✓ intercepts every outgoing request
 - ✓ checks destination's domain name against a blacklist of mobile trackers.



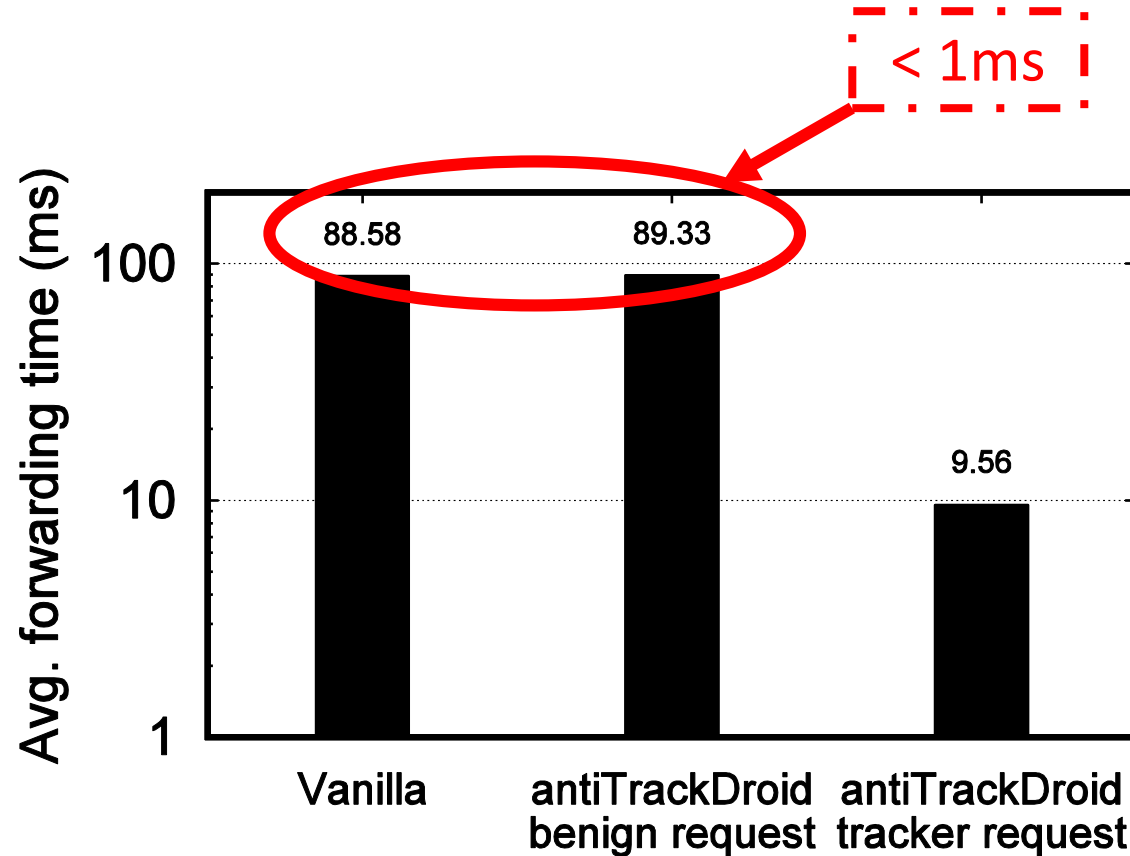
antiTrackDroid - Privacy Performance



- Run the 30 top leaking apps w/ and w/o antiTrackDroid.
- Reduction of leaked IDs by 27.41% on the average

• We block 3rd parties the rest of the leaking IDs regard requests first party domains and content providers (e.g. CDNs).

antiTrackDroid – Latency overhead



antiTrackDroid:



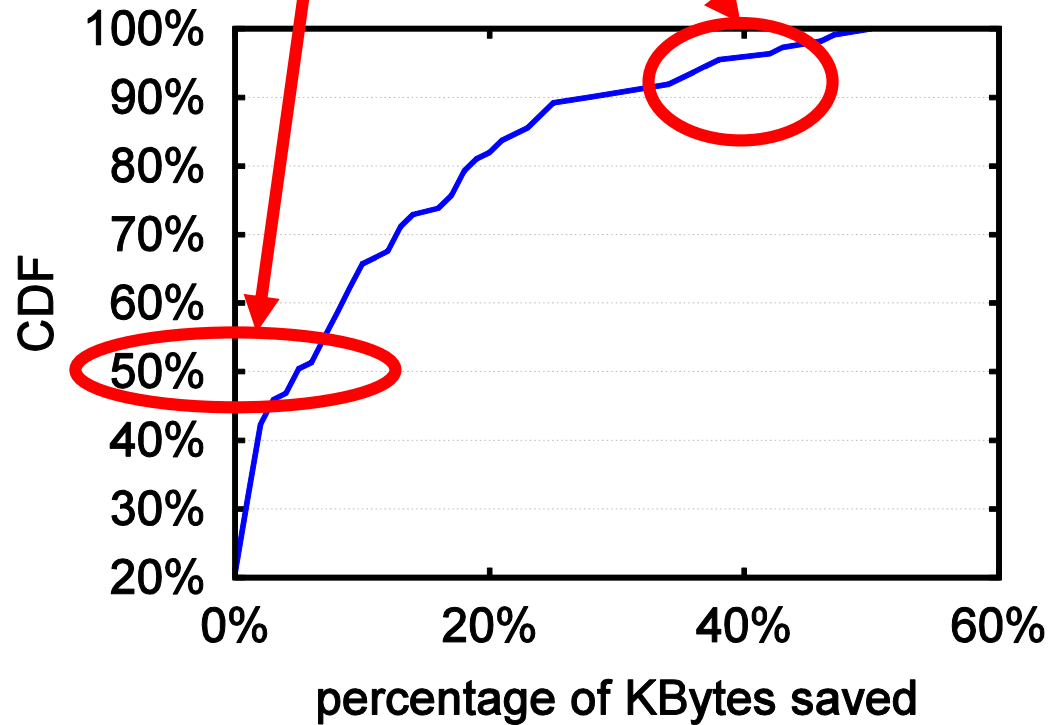
adds overhead in benign requests (additional check in blacklist) < 1ms



reduces overall latency in case of blocked requests

antiTrackDroid – Benefits

- 8% reduction for the median app,
- can reach even more than 40%



- blocking requests saves significant amount of data
- run every app with and without *antiTrackDroid*
- reduction of the transferred bytes by 8% for the median app.

In summary...

- we performed a head-to-head comparison to identify which harms the least the user's privacy: **web or apps?**
- **Apps leak significantly more** (installed + running apps, nearby APs, etc.)
 - allowing trackers to infer user interests, gender, even behavioral patterns.
- ***antiTrackDroid***: an anti-tracking mechanism for Android apps
 - reduce privacy leaks by 27.41%
 - <1 ms/req overhead.

