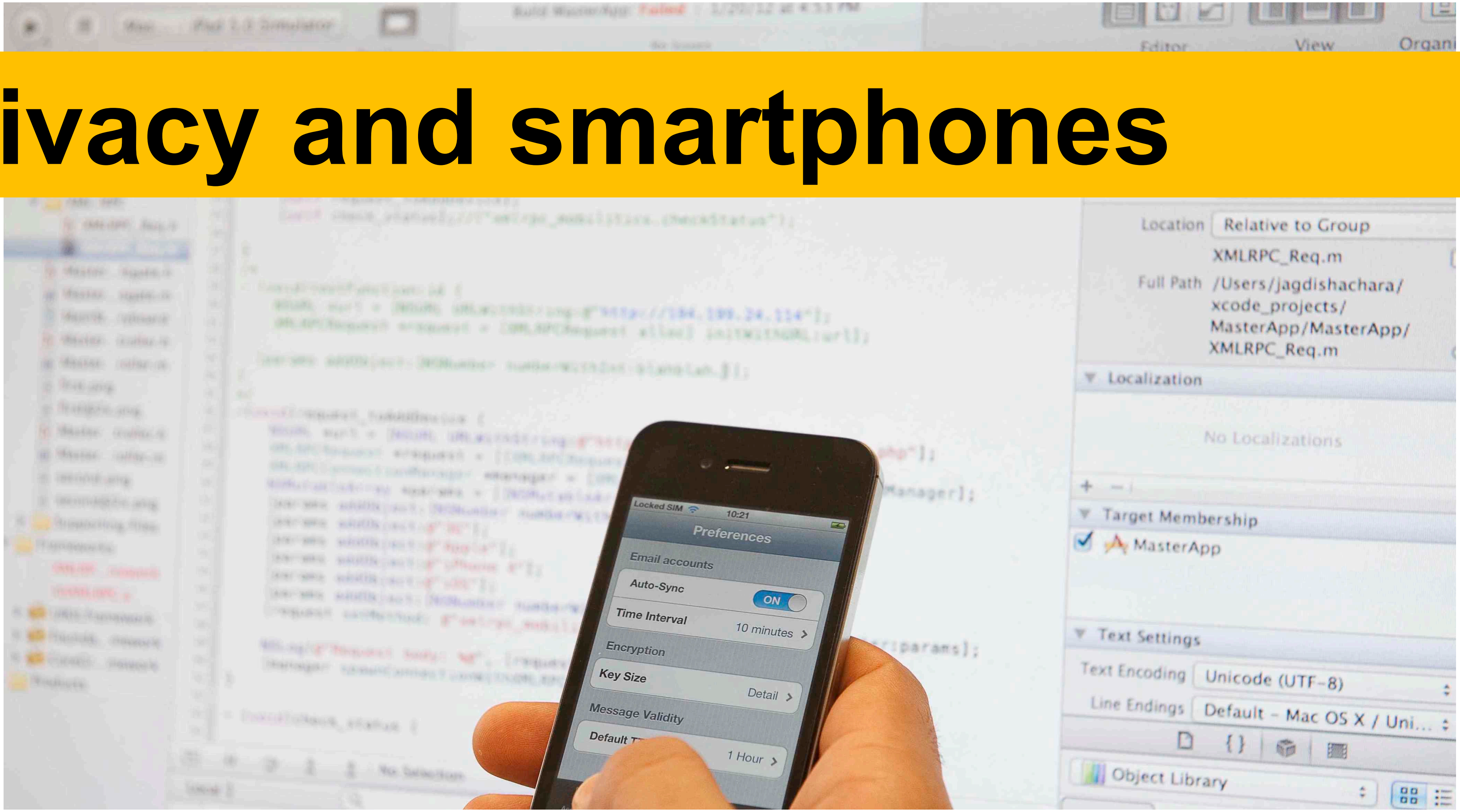
Privacy and smartphones



© Inria / Photo H. Raguet

Vincent Roca, Inria PRIVATICS, vincent.roca@inria.fr

November 29th, 2022

Inria Grenoble-Lyon-Sophia, PRIVATICS team

- understanding and formalizing privacy
- building privacy preserving systems

contact : vincent.roca@inria.fr

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

Outline

- **Personal data and the French/EU law**
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

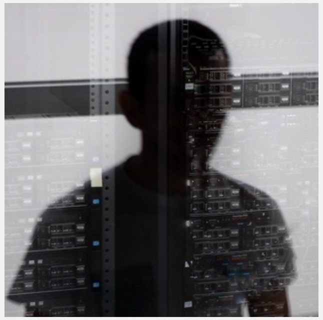
Some vocabulary…

Private company, administration

“data controller”

(responsable de traitements)

has the responsibility of



Data Base containing

“Personal Information”

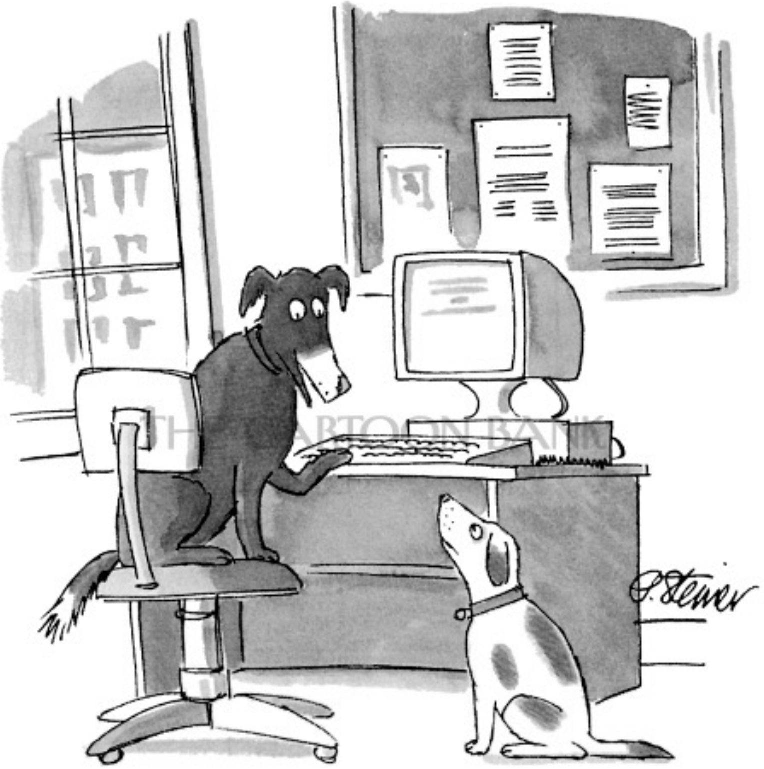
(données à caractère personnel)

relative to

Physical persons

Outline

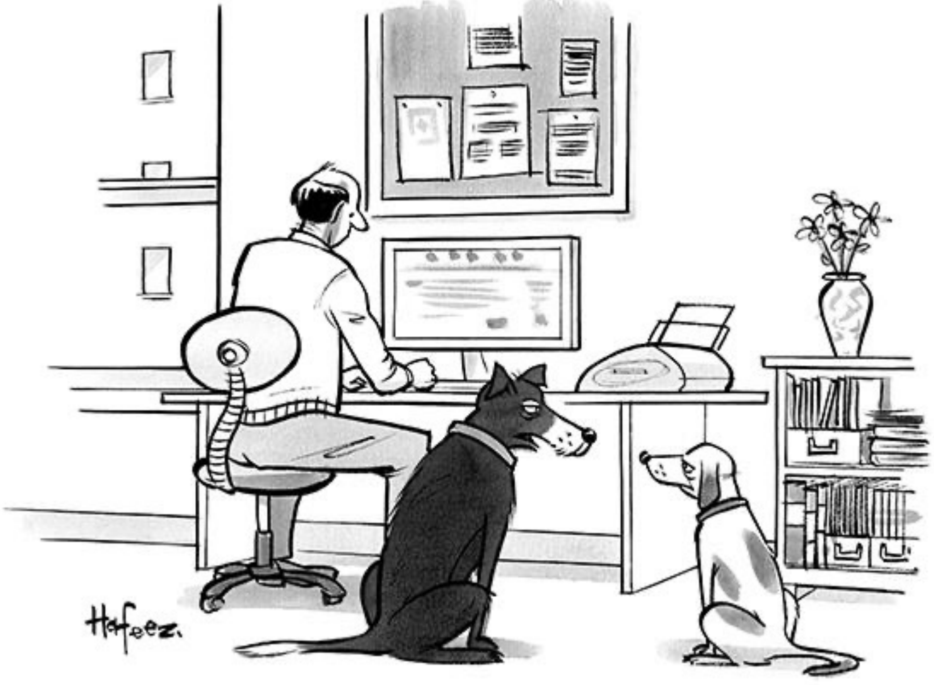
- Personal data and the French/EU law
- **Context: a massive worldwide surveillance**
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle



"On the Internet, nobody knows you're a dog."

In 1993…

In 2015…



"Remember when, on the Internet, nobody knew who you were?"

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- **Why do smartphones interest so many people?**
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

What does a smartphone consist in? (1)

- an application processor;
- an operating system (OS) (Android / Google or iOS / Apple)
- applications.

the visible side

- Subject of this lecture

What does a smartphone consist in? (2)

- a full system (processor + OS) for baseband communications
  - ✓ totally hidden to the user;
  - ✓ proprietary technology without any open specifications;
  - ✓ little is known…

the invisible side

- Should we be suspicious?
  - ✓ The community cannot answer given the intrinsic complexity of the required analyses.

http://events.ccc.de/congress/2011/Fahrplan/attachments/2022_11-ccc-qcombbdbg.pdf

At the center of PI collection (1)

- Our everyday “companions”…
  - ✓ useful, always connected, easy to customize

- but they also

concentrate

personal information

when we use them: phone calls, SMS, web, applications, etc.

generate

personal information

GPS, NFC, WiFi, camera, fingerprint sensor, heart rate sensor, etc.

At the center of PI collection (2)

- A smartphone knows a lot on our **cyber-activities on Internet**
  - ✓ Just like a web browser.
- But also in the **physical world**…
  - ✓ And this is new!
- As well as our **points of interest** (e.g., through the list of installed apps)
- Many actors are interested by this wealth of PI

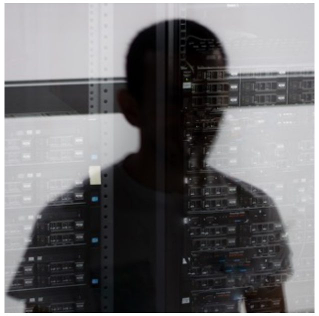
Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- **The ecosystem around applications for smartphones**
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

Many actors are involved

App. developer
(or first party)

Advertising and Analytics (A&A)
company (or third party)



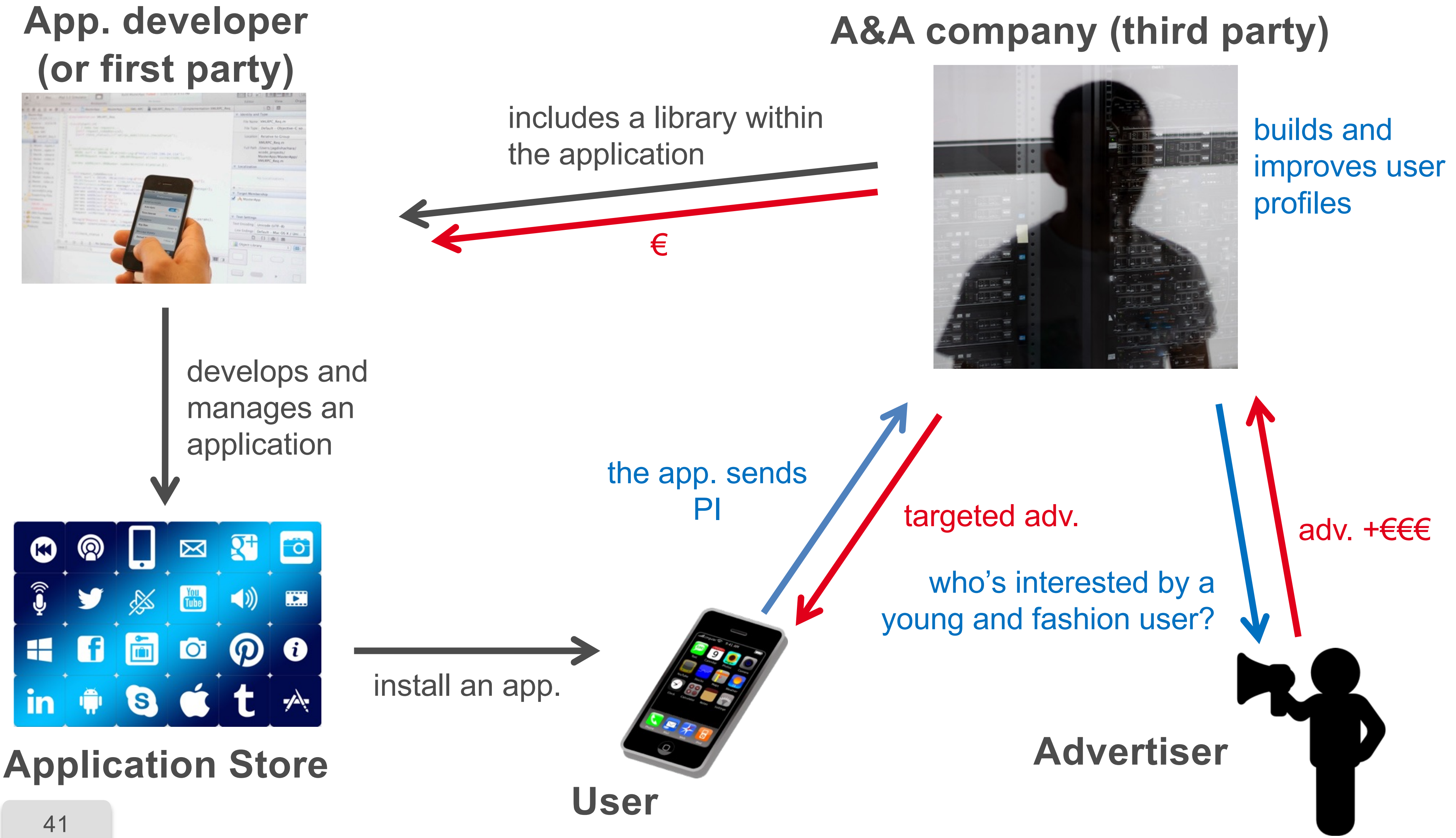
Application Store

User

Advertiser

An ecosystem centered around the A&A company

- At the interface between developers, users, and advertisers.
- Through the applications, it **collects** users’ PI.
  - ✓ *e.g., Applications used, geolocation, and technical identifiers.*
- Creates and progressively improves the accuracy of **user profiles.**
- Launches **Real-Time Bidding** (RTB).
  - ✓ “Who’s interested by this user profile?”
- Triggers the display of **targeted advertising** within the application.



App. developer (or first party)

A&A company (third party)

includes a library within the application

€

builds and improves user profiles

develops and manages an application

the app. sends PI

targeted adv.

adv. +€€€

who's interested by a young and fashion user?

install an app.

Application Store

User

Advertiser

A few examples of A&A companies…

AdMob by Google

FLURRY

bought by Yahoo! in 2014…

YAHOO!
DEVELOPER NETWORK

INMOBI™

(fined by FTC in 2016…)

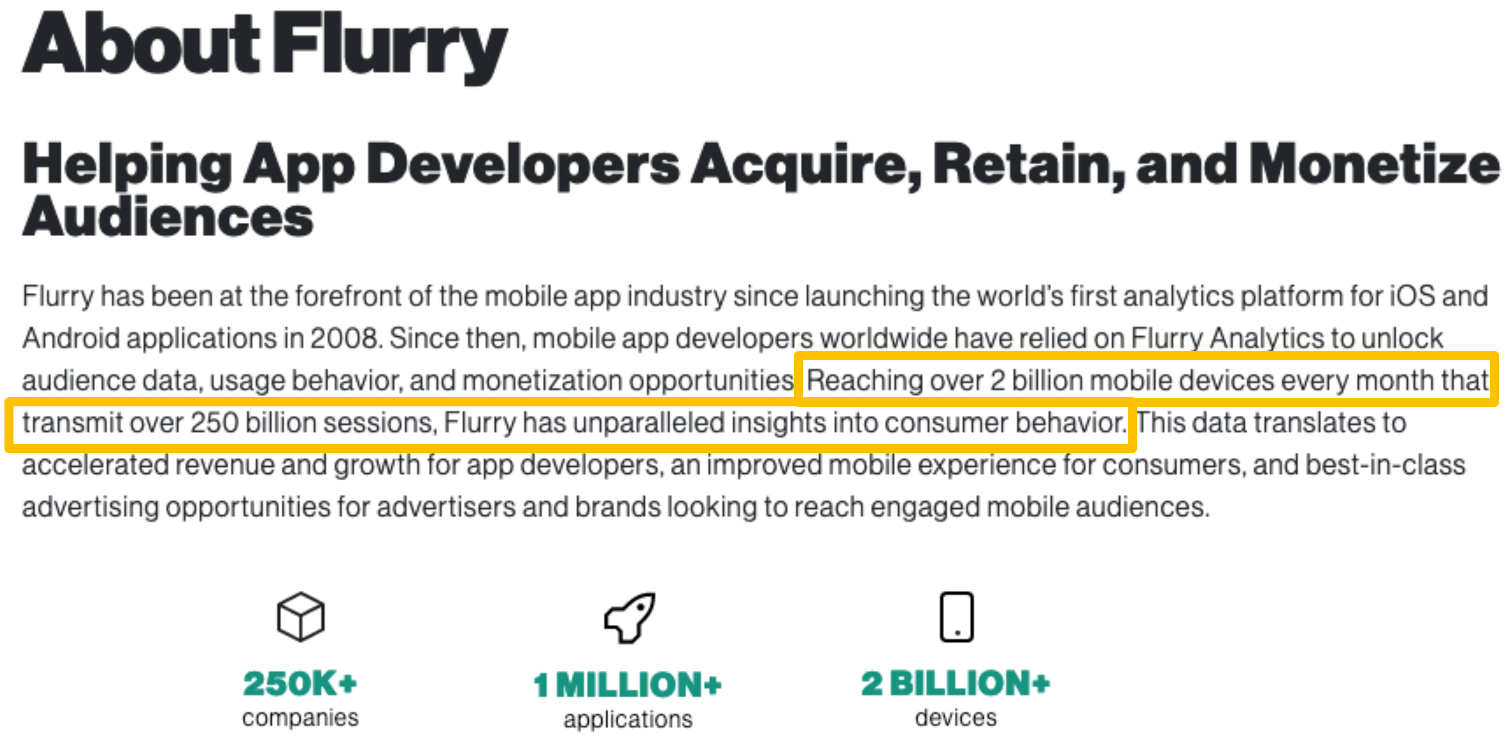
millennial media®

bought by AOL in 2015…

① by Aol.

More references at:
http://www.mobyaffiliates.com/guides/mobile-advertising-companies/
http://gulyani.com/complete-list-of-mobile-ad-networks-companies/

Very impressive amounts of data transfers!



About Flurry

Helping App Developers Acquire, Retain, and Monetize Audiences

Flurry has been at the forefront of the mobile app industry since launching the world's first analytics platform for iOS and Android applications in 2008. Since then, mobile app developers worldwide have relied on Flurry Analytics to unlock audience data, usage behavior, and monetization opportunities. Reaching over 2 billion mobile devices every month that transmit over 250 billion sessions, Flurry has unparalleled insights into consumer behavior. This data translates to accelerated revenue and growth for app developers, an improved mobile experience for consumers, and best-in-class advertising opportunities for advertisers and brands looking to reach engaged mobile audiences.

250K+ companies

1 MILLION+ applications

2 BILLION+ devices

FLURRY

now

YAHOO!
DEVELOPER NETWORK

Data-bases in the order of petabytes (10^{15}).

Source: Flurry web site, February 2022.

… And gross revenues that are impressive too!

- **Alphabet** (owner of Google):
  - 32.6 Billion $ gross revenue for targeted advertising in Oct – Dec 2018 (3 months)
    - ✓ out of a total of 39.1 Billion $ of gross revenue;
    - ✓ advertising represents 116 Billion $ in 2018 out of 136 Billion $ (i.e., 85% of gross revenue)

http://www.zdnet.fr/actualites/trimestriels-le-ca-d-alphabet-en-hausse-de-21-malgre-l-amende-de-l-ue-39855362.htm

https://abc.xyz/investor/news/earnings/2018/Q4_alphabet_earnings/

Ressources

Exemples de régies publicitaires cités dans la séquence :

- https://www.google.com/admob/
- https://developer.yahoo.com
- http://www.millennialmedia.com/
- http://www.onebyaol.com/
- http://www.inmobi.com/

Autres exemples :

- http://www.mobyaffiliates.com/guides/mobile-advertising-companies/
- http://gulyani.com/complete-list-of-mobile-ad-networks-companies/

ZdNet : http://www.zdnet.fr/actualites/trimestriels-le-ca-d-alphabet-en-hausse-de-21-malgre-l-amende-de-l-ue-39855362.htm

Alphabet : https://abc.xyz/investor/news/earnings/2017/Q2_alphabet_earnings/

Outline

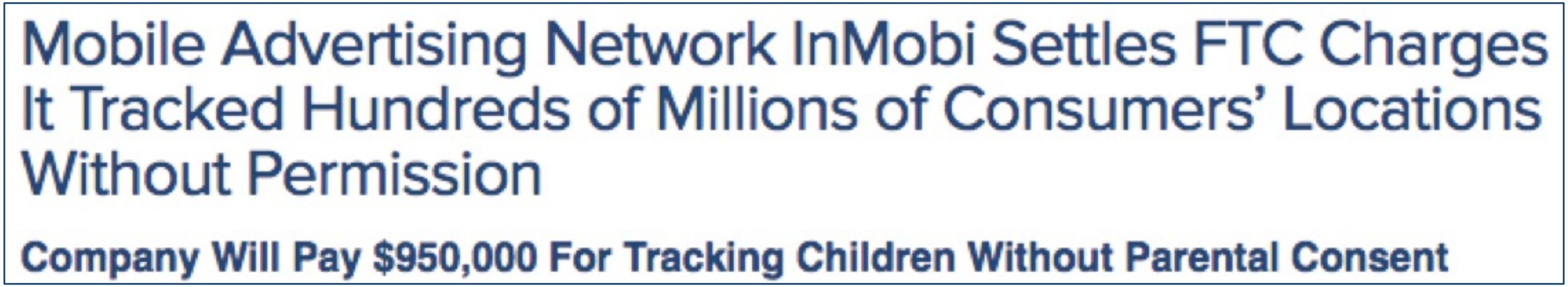
- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- **Free apps/services in exchange of targeted advertising: where's the problem?**
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

Don’t be naive…

- Everyday we use…
  - ✓ high quality, free **services**;
  - ✓ high quality, free **applications**.

- Possible thanks to a business model essentially based on **targeted advertising:**
  - ✓ The advertiser pays for the user.
- This requires a **profiling of users…**
  - ✓ … in order to know their centers of interest.

… But there are limits!



Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission

Company Will Pay $950,000 For Tracking Children Without Parental Consent

https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked

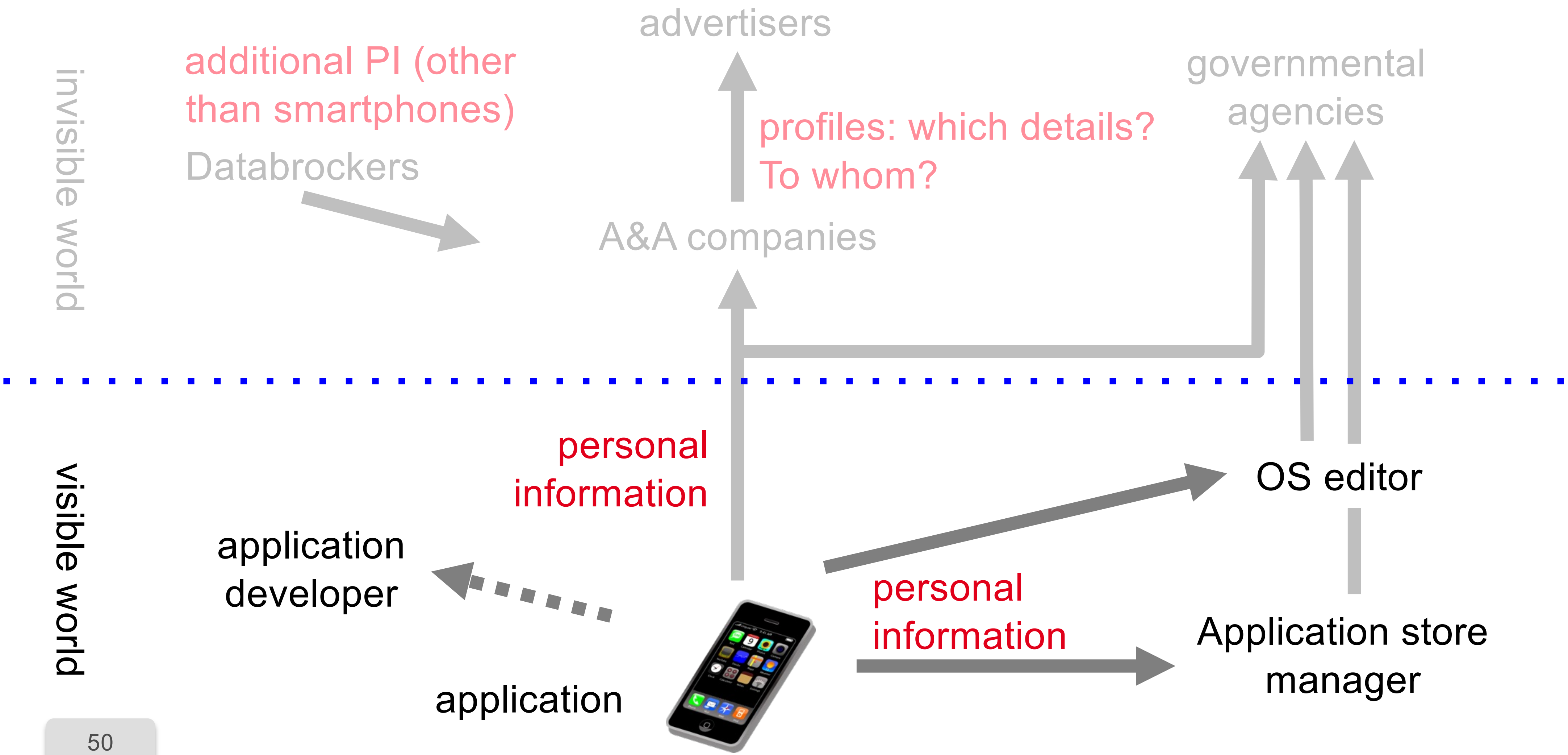
Fair business model or not?

- "Free in exchange for targeted advertising" could be a reasonable business model…

« Les données personnelles sont le nouveau pétrole de l'internet et la nouvelle monnaie du monde numérique. »
M. Kuneva, Commissaire europ. à la consommation, 2009

- … but currently a few fundamental issues remain:
  - ✓ Complexity ;
  - ✓ Disproportion ;
  - ✓ Lack of information ;
  - ✓ Lack of control.

1- The ecosystem is so complex we cannot trust them all



invisible world

additional PI (other than smartphones)

Databrockers

advertisers

profiles: which details? To whom?

A&A companies

governmental agencies

visible world

personal information

application developer

application

OS editor

personal information

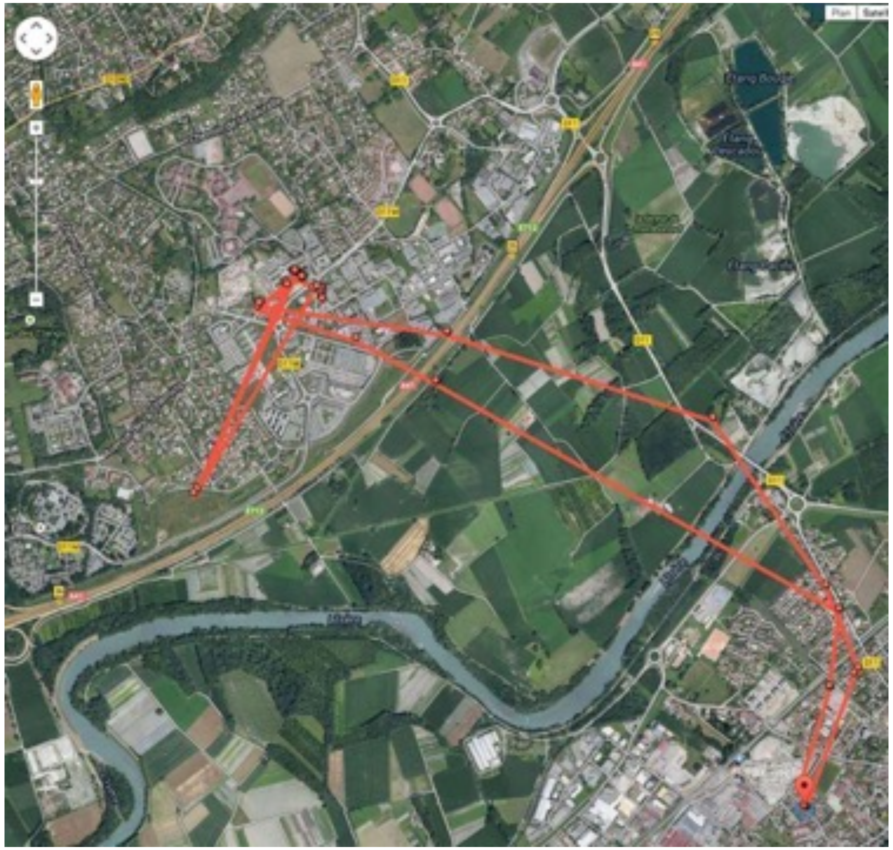
Application store manager

2- A potential disproportion of data collection (1)

- Example: historic of positions recorded by my Android smartphone for Google services.
  - ✓ https://maps.google.com/locationhistory/

2- A potential disproportion of data collection (2)

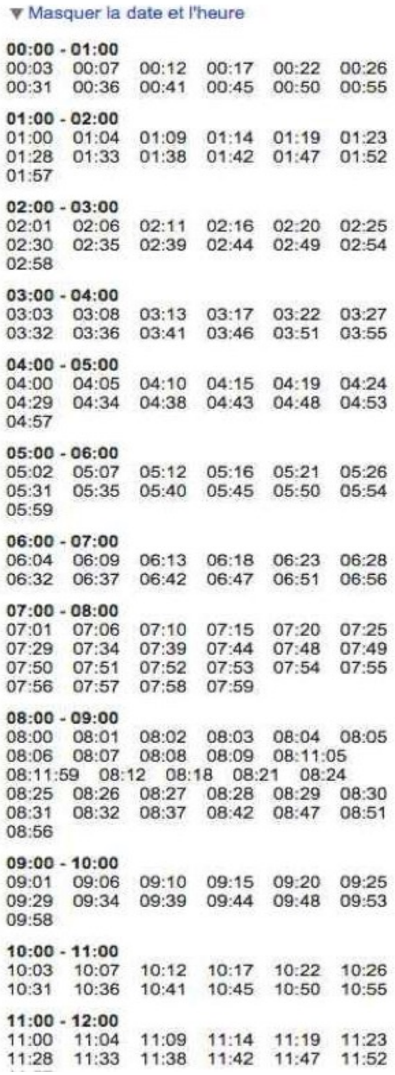
- Google knows where I work, where I live, what I'm doing during the day, how I move from one place to another, and much more…



2- A potential disproportion of data collection (3)

- All this with an incredible accuracy:
  - ✓ Here is the full list of positions recorded by Google that day.

- A record **every 5 minutes** during the night…
- … and **each minute** if I'm moving!



▼ Masquer la date et l'heure

00:00 - 01:00
00:03 00:07 00:12 00:17 00:22 00:26
00:31 00:36 00:41 00:45 00:50 00:55

01:00 - 02:00
01:00 01:04 01:09 01:14 01:19 01:23
01:28 01:33 01:38 01:42 01:47 01:52
01:57

02:00 - 03:00
02:01 02:06 02:11 02:16 02:20 02:25
02:30 02:35 02:39 02:44 02:49 02:54
02:58

03:00 - 04:00
03:03 03:08 03:13 03:17 03:22 03:27
03:32 03:36 03:41 03:46 03:51 03:55

04:00 - 05:00
04:00 04:05 04:10 04:15 04:19 04:24
04:29 04:34 04:38 04:43 04:48 04:53
04:57

05:00 - 06:00
05:02 05:07 05:12 05:16 05:21 05:26
05:31 05:35 05:40 05:45 05:50 05:54
05:59

06:00 - 07:00
06:04 06:09 06:13 06:18 06:23 06:28
06:32 06:37 06:42 06:47 06:51 06:56

07:00 - 08:00
07:01 07:06 07:10 07:15 07:20 07:25
07:29 07:34 07:39 07:44 07:48 07:49
07:50 07:51 07:52 07:53 07:54 07:55
07:56 07:57 07:58 07:59

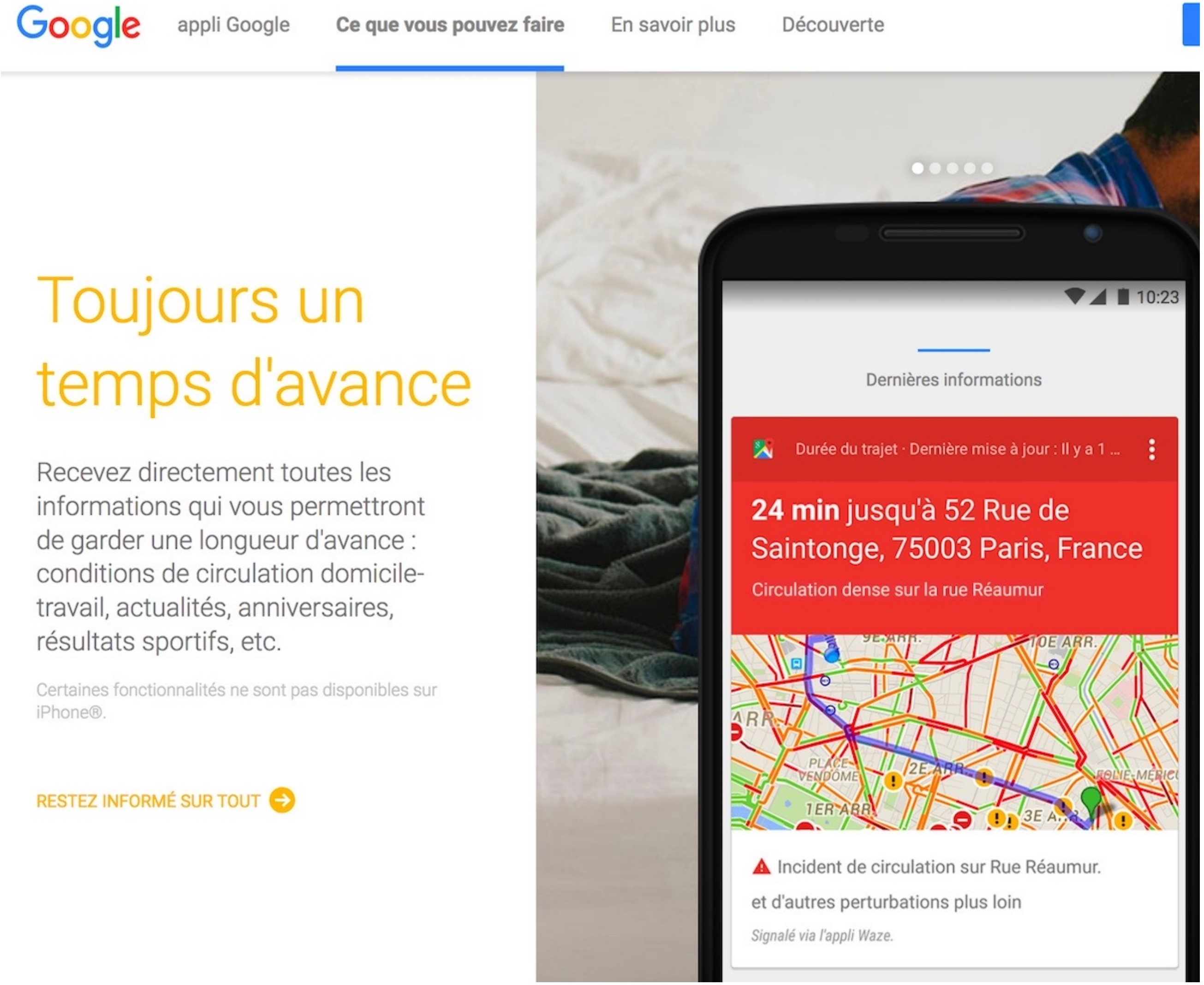
08:00 - 09:00
08:00 08:01 08:02 08:03 08:04 08:05
08:06 08:07 08:08 08:09 08:11:05
08:11:59 08:12 08:18 08:21 08:24
08:25 08:26 08:27 08:28 08:29 08:30
08:31 08:32 08:37 08:42 08:47 08:51
08:56

09:00 - 10:00
09:01 09:06 09:10 09:15 09:20 09:25
09:29 09:34 09:39 09:44 09:48 09:53
09:58

10:00 - 11:00
10:03 10:07 10:12 10:17 10:22 10:26
10:31 10:36 10:41 10:45 10:50 10:55

11:00 - 12:00
11:00 11:04 11:09 11:14 11:19 11:23
11:28 11:33 11:38 11:42 11:47 11:52

2- A potential disproportion of data collection (4)



Toujours un temps d'avance

Recevez directement toutes les informations qui vous permettront de garder une longueur d'avance : conditions de circulation domicile-travail, actualités, anniversaires, résultats sportifs, etc.

Certaines fonctionnalités ne sont pas disponibles sur iPhone®.

RESTEZ INFORMÉ SUR TOUT

Durée du trajet · Dernière mise à jour : Il y a 1 ...

24 min jusqu'à 52 Rue de Saintonge, 75003 Paris, France

Circulation dense sur la rue Réaumur

Incident de circulation sur Rue Réaumur.

et d'autres perturbations plus loin

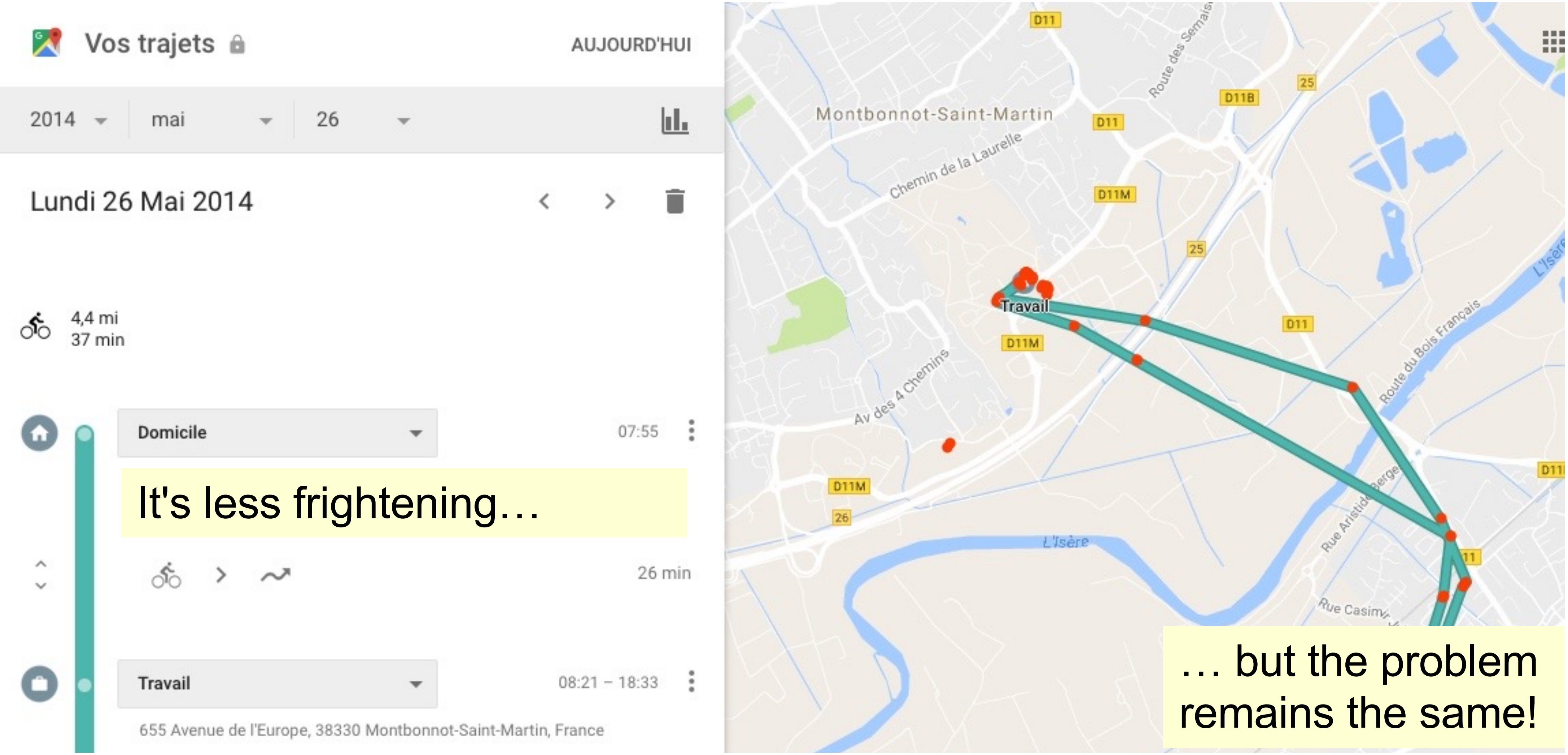
Signalé via l'appli Waze.

- I have enabled Google Now!
  - ✓ Now called « appli. Google ».

  https://www.google.com/search/about/

- Disproportionate collection of PI with respect to the service provided?
  - ✓ this is my opinion, but you may disagree…

BTW, Google simplified the page design!



Vos trajets

AUJOURD'HUI

2014 ▾ mai ▾ 26 ▾

Lundi 26 Mai 2014

4,4 mi
37 min

Domicile ▾ 07:55

26 min

Travail ▾ 08:21 – 18:33

655 Avenue de l'Europe, 38330 Montbonnot-Saint-Martin, France

It's less frightening…

… but the problem remains the same!

2- A potential disproportion of data collection (5)

- Geolocation information is meaningful.
  - ✓ Google knows if I’m going to a place of worship.
  - ✓ Google knows if I’m going to an hospital.

- Those are **sensitive data** according to the “loi Informatique et Liberté”.
  - ✓ CANNOT be collected or processed!

3- Lack of information on PI collection

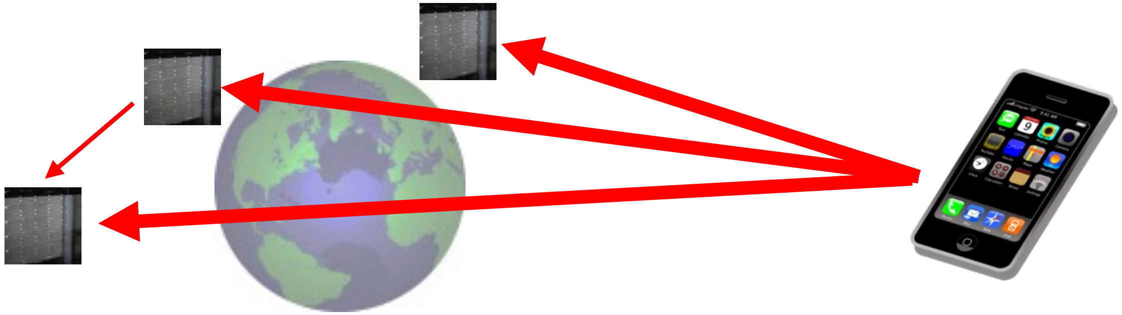
- We don’t know everything…
  - ✓ see the RATP application, 2013 version.
  - ✓ This RATP app. changed a lot since that version, but many others keep on leaking personal information without the user knowing.

- Possible because:
  - ✓ most of the privacy policies (meant to inform the user) are **not written to be understood**;
  - ✓ **lack of transparency** on practices.

Source : https://play.google.com/store/apps/details?id=com.fabernovel.ratp&hl=fr

4- Lack of control on PI collection

- Data is immediately **exfiltrated** beyond EU without any control
  - ✓ the GDPR applies but may be difficult to enforce and checked checked in those countries...



- **No guaranty** regarding the storage, security, usage, exchange of our PI with other actors.

This is just the beginning

- PI collection will become **more and more intrusive** with:
  - ✓ generalization of smartphone payment
  - ✓ home connected devices
    - ○ e.g., smart speakers
  - ✓ “quantified self” trend
    - ○ it’s sensitive, health data!
  - ✓ connected cars
    - ○ wherever you go, they’ll know if you authorize them
  - ✓ IoT…

In summary

- “Free in exchange for targeted advertising” could be a reasonable business model…
  - ✓ Remember there’s no free beer!

- … but currently a few fundamental issues remain:
  - ✓ Complexity, disproportion, lack of information, lack of control.

- It’s essential to find solutions.
  - ✓ A increasing number of domains, currently untouched, will be concerned.

Ressources

Federal Trade Commission. *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*. June 22, 2016 : https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked

Appli. Google : https://www.google.com/search/about/

Vos trajets / Appli Google : https://maps.google.com/locationhistory/

Google Play – Application RATP :
https://play.google.com/store/apps/details?id=com.fabernovel.ratp&hl=fr

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- **What is personal in my smartphone: a close-up on technical identifiers**
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

What is personal on my smartphone?

- Many things…

concentrate
personal information
when we use them: phone calls, SMS, web, applications, etc.

generate
personal information
GPS, NFC, WiFi, camera, fingerprint sensor, heart rate sensor, etc.

- This is the case of **technical identifiers** that focus a lot of interest.
  - They look like random numbers.
  - They look like harmless.

Examples of technical identifiers

- AndroidID
  - ✓ random number that **quasi-uniquely** identifies an Android smartphone
- MAC address of Wi-Fi (or Bluetooth) interface
  - ✓ **uniquely** identifies the network interface (e.g., 68:a8:6d:28:ce:1f)
- IMEI (International Mobile Equipment Identity)
  - ✓ **uniquely** identifies a smartphone (used for instance to block a stolen phone)
- IMSI (International Mobile Subscriber Identity)
  - ✓ **uniquely** identifies a user at his/her cell phone operator

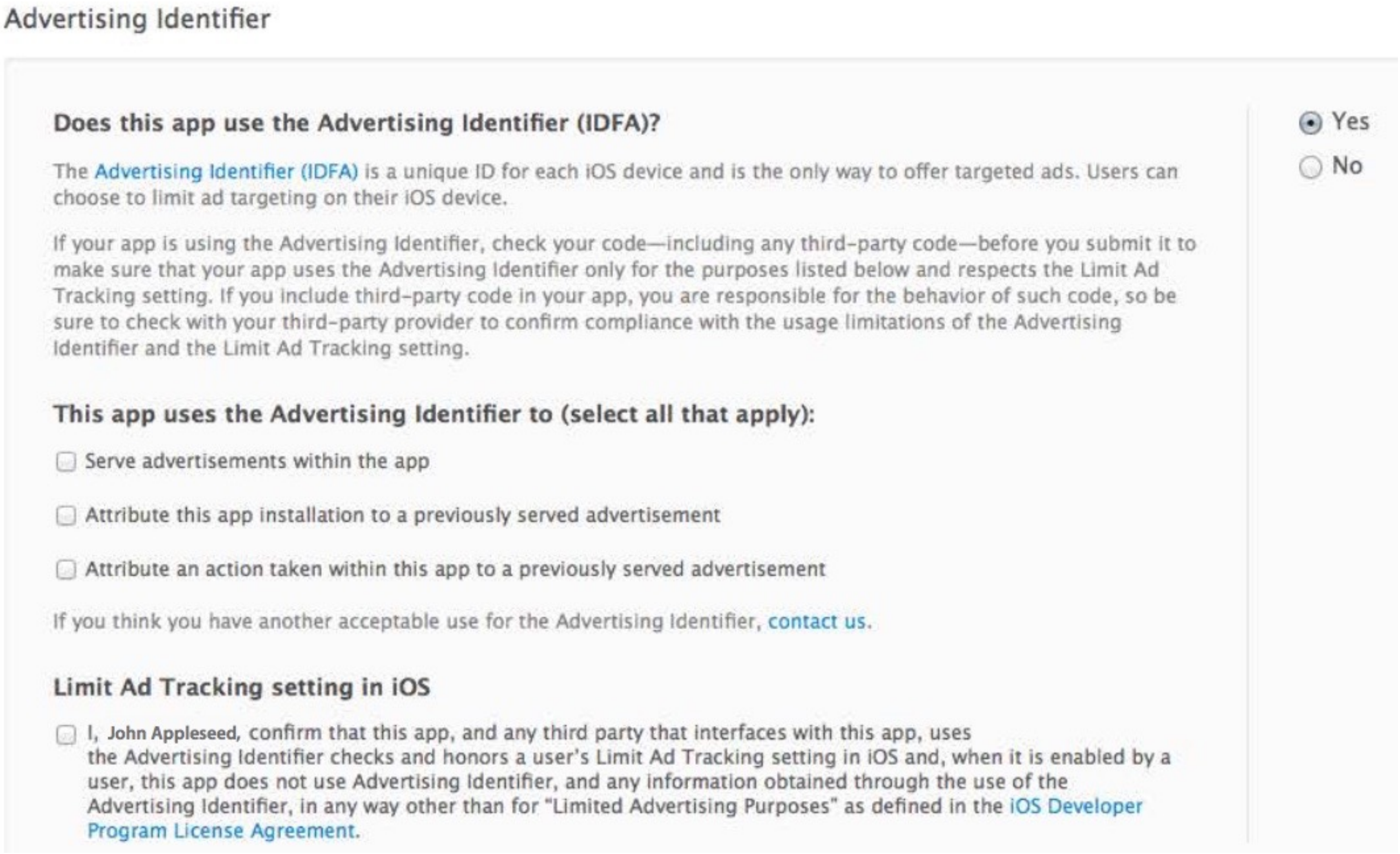
- and the AdID (Advertising Identifier)/IDFA (ID for Advertisers)…

About the Advertising Identifier, or AdID (1)

- Quasi-unique identifier used explicitly for **targeted advertising.**
  - ✓ Historically created by Apple (IDFA, “Identifier for advertising”).
  - ✓ Later added by Google (AdID, “advertising Identifier).
  - ▪ The user can **reinitialize** the AdID at any time ☺.
  - ▪ Apple also enables the user to ask not to be tracked.

- Two benefits:
  - ▪ **Transparency**: it’s designed for advertising only.
  - ▪ Gives back **control** to the user.

About the Advertising Identifier, or AdID (2)



Advertising Identifier

Does this app use the Advertising Identifier (IDFA)?

● Yes

○ No

The Advertising Identifier (IDFA) is a unique ID for each iOS device and is the only way to offer targeted ads. Users can choose to limit ad targeting on their iOS device.

If your app is using the Advertising Identifier, check your code—including any third-party code—before you submit it to make sure that your app uses the Advertising Identifier only for the purposes listed below and respects the Limit Ad Tracking setting. If you include third-party code in your app, you are responsible for the behavior of such code, so be sure to check with your third-party provider to confirm compliance with the usage limitations of the Advertising Identifier and the Limit Ad Tracking setting.

This app uses the Advertising Identifier to (select all that apply):

□ Serve advertisements within the app

□ Attribute this app installation to a previously served advertisement

□ Attribute an action taken within this app to a previously served advertisement

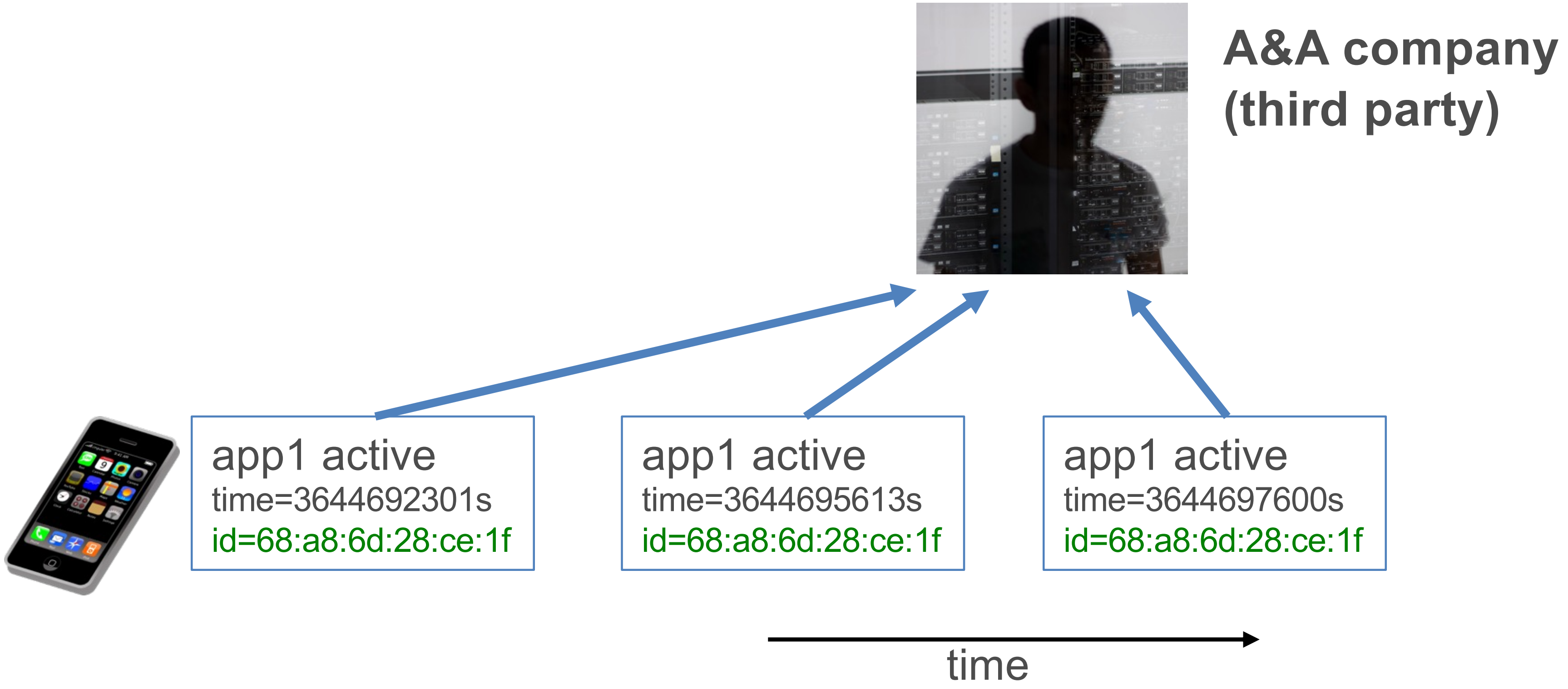
If you think you have another acceptable use for the Advertising Identifier, contact us.

Limit Ad Tracking setting in iOS

□ I, **John Appleseed**, confirm that this app, and any third party that interfaces with this app, uses the Advertising Identifier checks and honors a user's Limit Ad Tracking setting in iOS and, when it is enabled by a user, this app does not use Advertising Identifier, and any information obtained through the use of the Advertising Identifier, in any way other than for "Limited Advertising Purposes" as defined in the iOS Developer Program License Agreement.

Technical IDs are very useful for tracking (1)

- Stable IDs are perfect for **tracking users** on the long term.



A&A company (third party)

app1 active
time=3644692301s
id=68:a8:6d:28:ce:1f

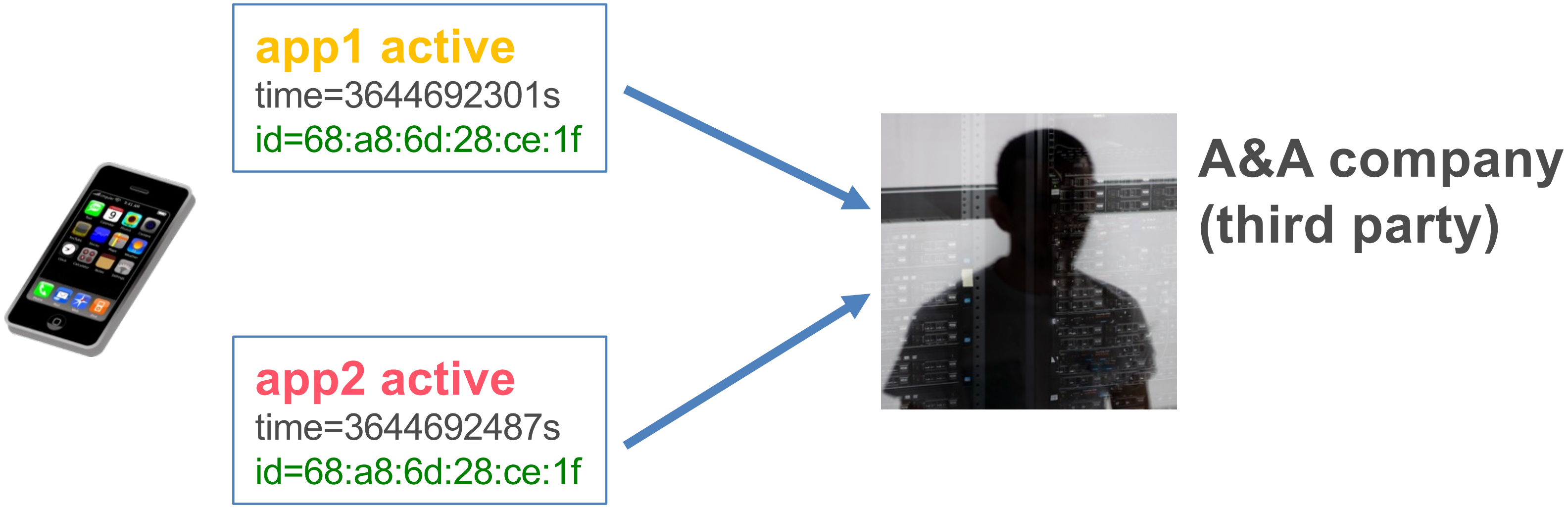
app1 active
time=3644695613s
id=68:a8:6d:28:ce:1f

app1 active
time=3644697600s
id=68:a8:6d:28:ce:1f

time

Technical IDs are very useful for tracking (2)

- stable IDs are perfect to **correlate** information collected from several Apps
  - and therefore refine a **user profile**
  - one knows a subset of applications used by this user!



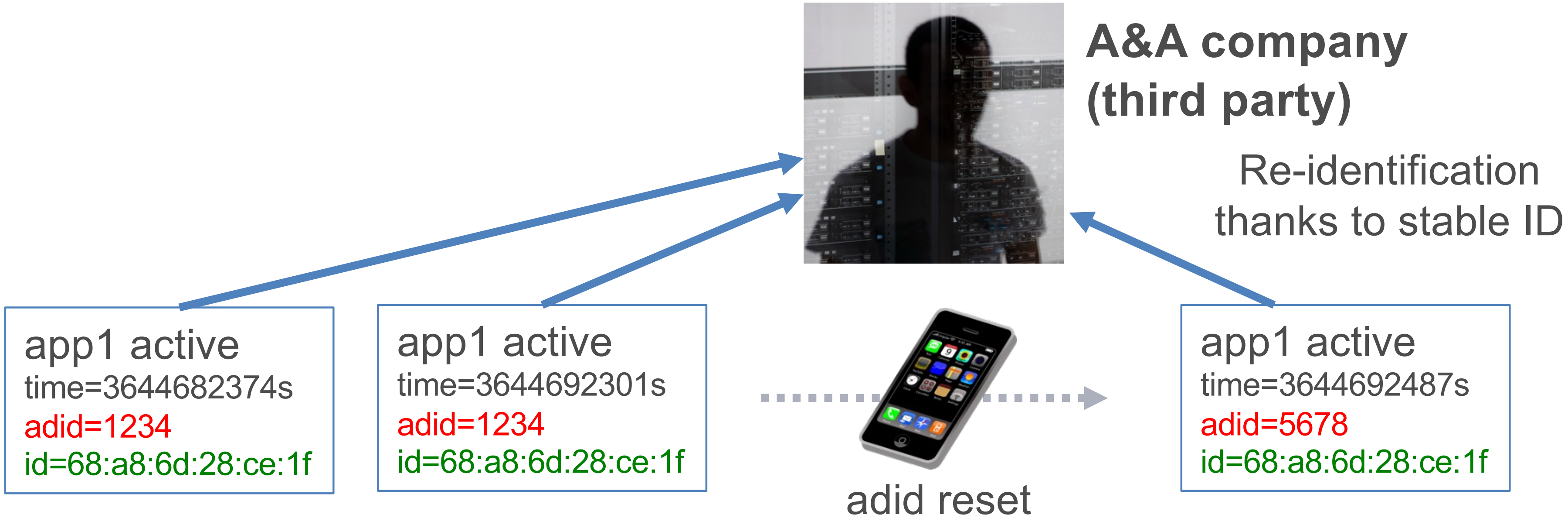
app1 active
time=3644692301s
id=68:a8:6d:28:ce:1f

app2 active
time=3644692487s
id=68:a8:6d:28:ce:1f

A&A company (third party)

Technical IDs are very useful for tracking (3)

- Stable IDs are perfect to **bypass** any tracking for advertising limitation system.
  - voids the *Advertising Identifier* reset whereas the user thinks the contrary.



A&A company (third party)

Re-identification thanks to stable ID

app1 active
time=3644682374s
adid=1234
id=68:a8:6d:28:ce:1f

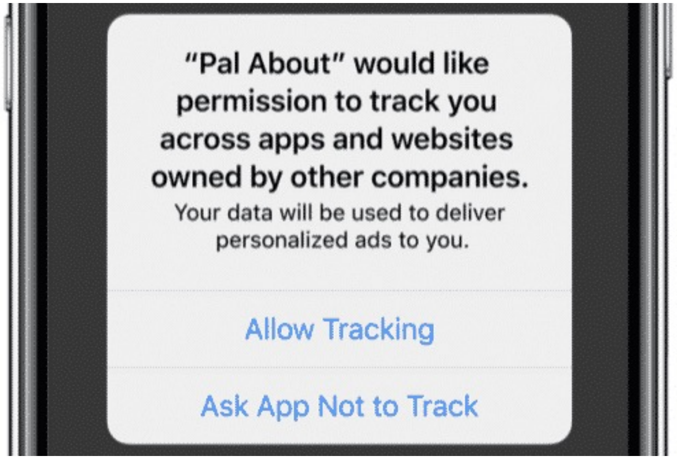
app1 active
time=3644692301s
adid=1234
id=68:a8:6d:28:ce:1f

adid reset

app1 active
time=3644692487s
adid=5678
id=68:a8:6d:28:ce:1f

Access to technical IDs: Apple

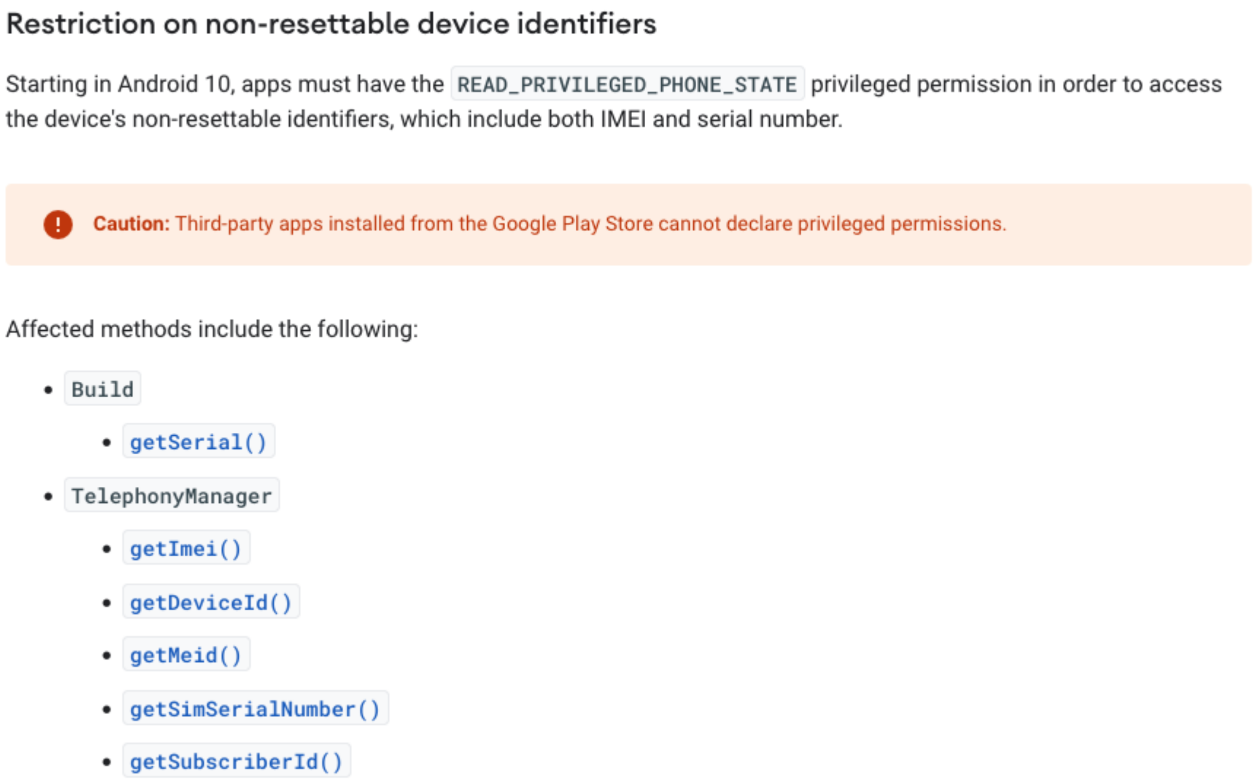
- **Apple** progressively banned access to stable identifiers since 2013 ☺
  - UDID : May 2013.
  - Wi-Fi MAC address: iOS7, September 2013.
  - The AdID was the only one authorized…
    - Greatly limits (but does not totally prevent) tracking possibilities.
- Further restrictions with iOS 14.5 (2021) for AdID (opt-out ➔ opt-in ➔ removal)
  - Ask the user, unless user already set “limit app tracking” turned on… In practice users refuse.



“Pal About” would like permission to track you across apps and websites owned by other companies.

Your data will be used to deliver personalized ads to you.

Access to technical IDs: Google



Restriction on non-resettable device identifiers

Starting in Android 10, apps must have the `READ_PRIVILEGED_PHONE_STATE` privileged permission in order to access the device's non-resettable identifiers, which include both IMEI and serial number.

Caution: Third-party apps installed from the Google Play Store cannot declare privileged permissions.

Affected methods include the following:

- `Build`
    - `getSerial()`
- `TelephonyManager`
    - `getImei()`
    - `getDeviceId()`
    - `getMeid()`
    - `getSimSerialNumber()`
    - `getSubscriberId()`

- Before 2019, access to technical IDs was easy
    - ✓ Google kindly asked A&A companies to use the AdID and not to cheat!

- Google only recently changed strategy with Android10 (2019)
    - ✓ Major change: 3rd party App cannot access them
    - ○ Google introduced technical limits in addition to guidelines

https://developer.android.com/training/articles/user-data-ids

In summary

- Technical identifiers focus a lot of interest because they are **stable**.
- Used:
  - ✓ to track users;
  - ✓ to correlate information collected separately;
  - ✓ potentially to bypass AdID reset.

- **The Advertising Identifier (AdID)** brings transparency and control back to the user.
  - ✓ The user knows its purpose and can reset it at any time/.

- Apple has soon be virtuous, they now go further (opt-in), Google only recently changed their strategy.

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- **User control**
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

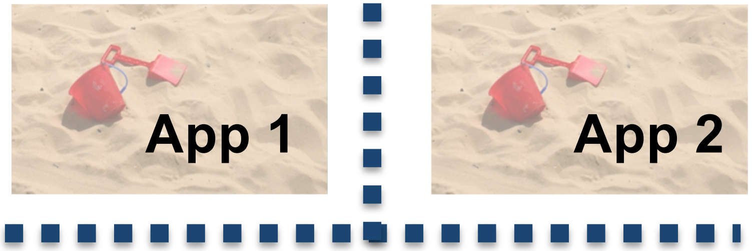
Notion of authorizations (1)

- For instance:
  - ✓ *for Internet (transmission/reception).*
  - ✓ *to access Contacts.*

- Goal: get the **"free, informed, specific and unequivocal consent"** of the user when "consent" is the legal basis:
  - ✓ **"Free":** the user can refuse an authorization without consequence.
  - ✓ **"Informed":** the user knows the implications of the authorization.
  - ✓ **"specific":** for a single purpose
  - ✓ **"unequivocal":** need a clear user action, no opt-out consent

➔ is it really the case ?

Notion of authorizations (2)



- Each application is **isolated**.
  - ✓ Runs in a closed environment (“sandbox”).
  - ✓ By default, an application cannot access remote resources.
  - ✓ Required for security purposes in the smartphone.

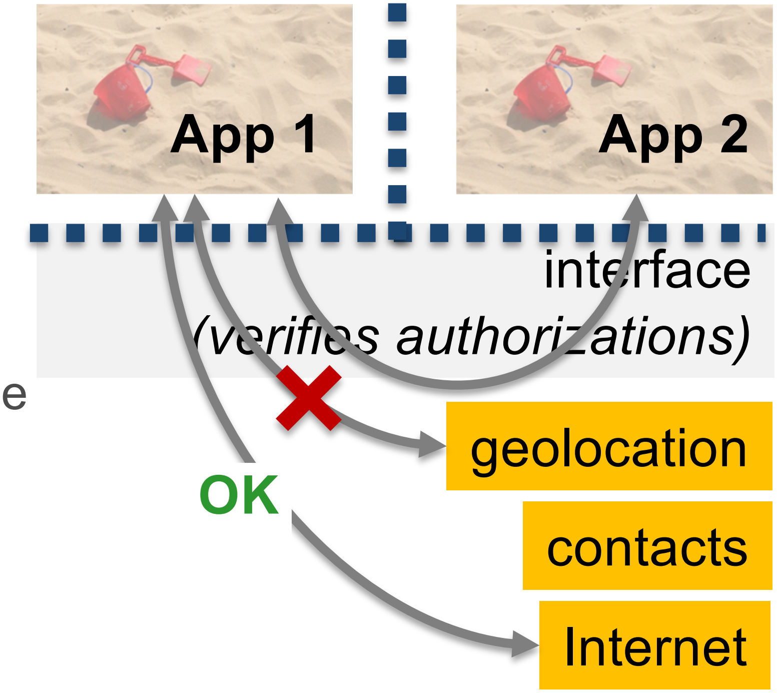
geolocation

contacts

Internet

Notion of authorizations (3)

- Access to external information requires:
  - ✓ having the associated authorization;
  - ✓ using a dedicated interface (API) that will authorize or ban the access.



The user must grant (or refuse) each authorization asked by the application.

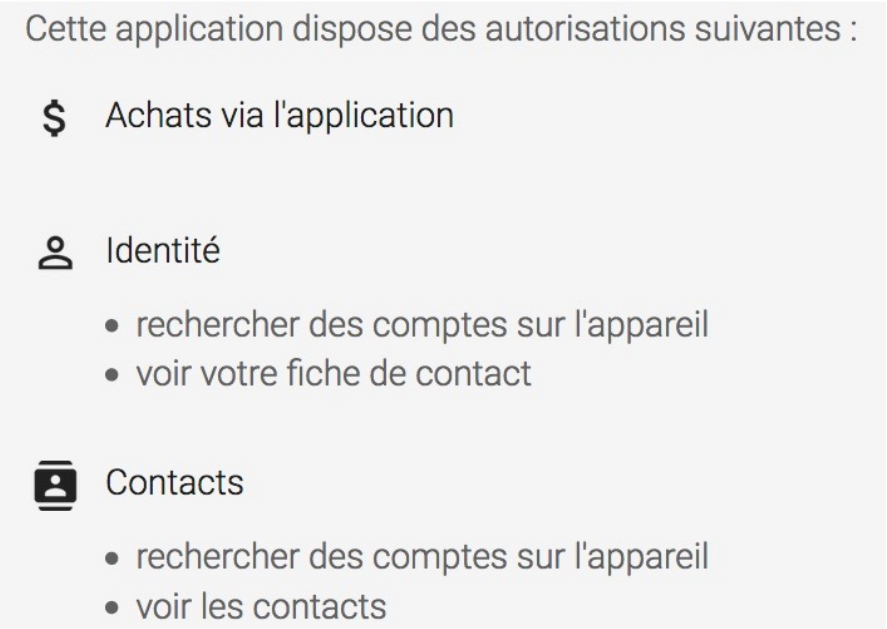
A shared responsibility between G/A and users

- **Store centric:** Apple/Google check Apps before accepting them:
  - ✓ Enforce the App conformance with the rules.
  - ○ (e.g., do companies try to bypass rules, leveraging on technically feasible tricks?)

- **User centric:** ask the authorization to the user:
  1. **a priori :** during application **installation**;
  2. **a posteriori : dynamically,** upon application usage.

At installation time authorizations - Android

- Ask the user to grant authorizations **at installation time**.
  - ✓ The Android historical **"Permissions"**.
  - ✓ The only approach for Android until **Android 5.1**.
  - ✓ Either "accept all", or go away (no installation possible).



Cette application dispose des autorisations suivantes :

$ Achats via l'application

Identité

- rechercher des comptes sur l'appareil
- voir votre fiche de contact

Contacts

- rechercher des comptes sur l'appareil
- voir les contacts

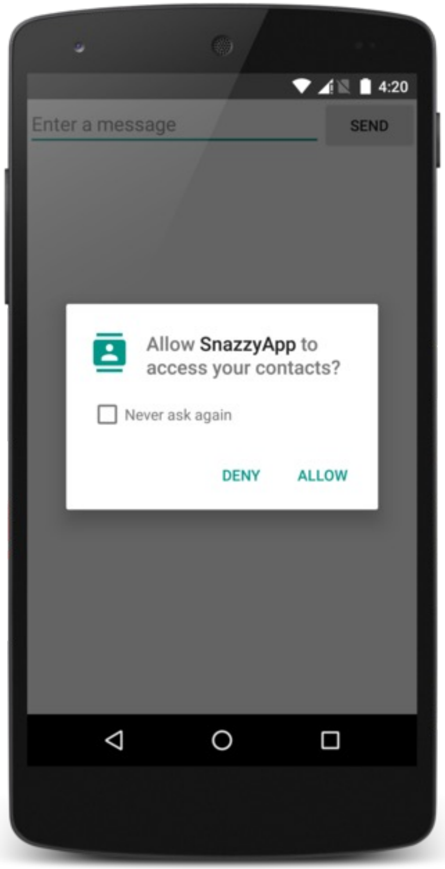
less used

Dynamic Authorizations – Android (1)

- Ask the user to grant explicit authorizations **at execution time**, when/if needed.
  - ✓ Google privileged approach since **Android 6.0 (end of 2015).**

- The user has more control (idem Apple/iOS):
  - ✓ The user authorizes or refuses individually each authorization ☺.
  - ✓ The user can change his mind at any time ☺.

- Google talks about “fluid installation”…
  - ✓ Sure, but authorizations asked by a certain application are no longer displayed. The user needs to search them ☹.

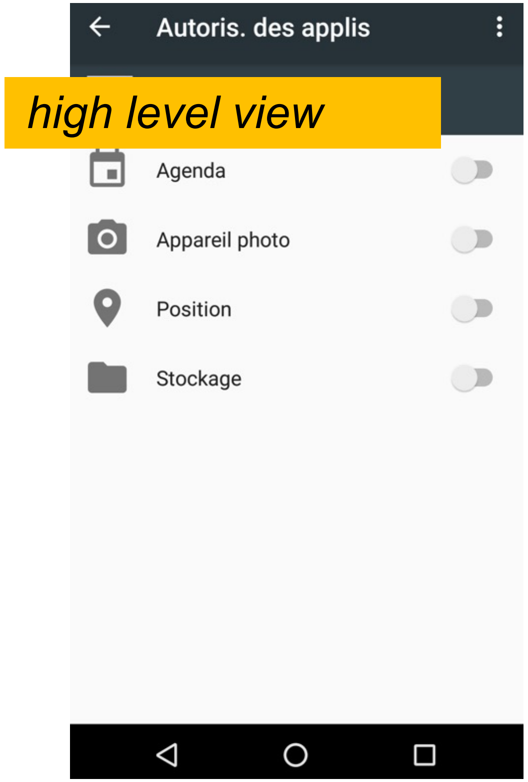


Allow **SnazzyApp** to access your contacts?

□ Never ask again

Dynamic Authorizations – Android (2)

- List all authorizations **for a given application**.
  - ✓ High level view: Parameters > Applications > appli > Authorizations
  - ✓ Detailed view: “All authorizations”



high level view

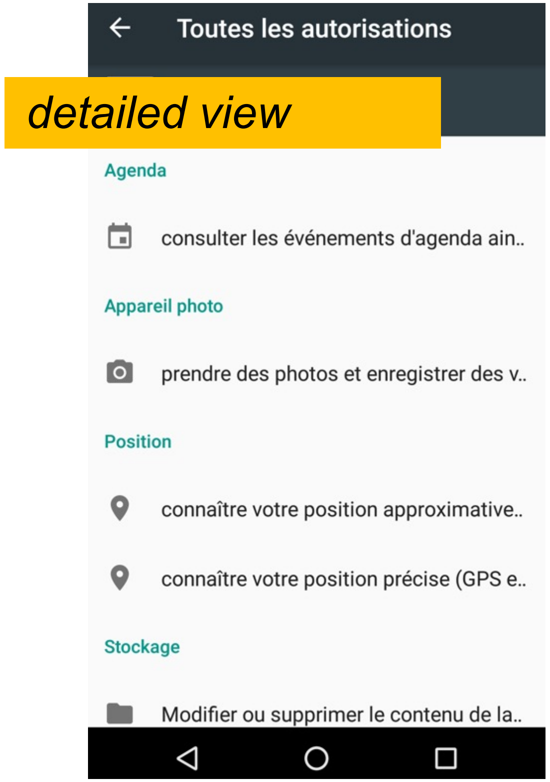
Autoris. des applis

Agenda

Appareil photo

Position

Stockage



detailed view

Toutes les autorisations

Agenda

consulter les événements d'agenda ain..

Appareil photo

prendre des photos et enregistrer des v..

Position

connaître votre position approximative..

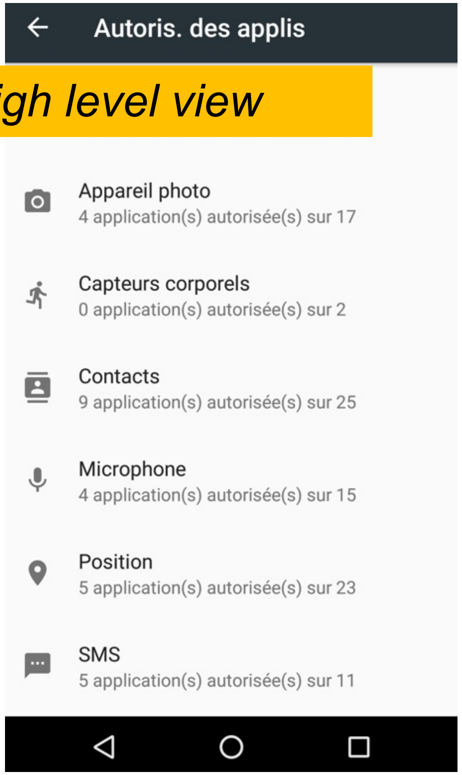
connaître votre position précise (GPS e..

Stockage

Modifier ou supprimer le contenu de la..

Dynamic Authorizations – Android (3)

- List all applications **for a given authorization**.
  - ✓ Android 6 : Applications > Configure the applis > Autoris. of applis
  - ✓ Android 8 : Apps & notifications > App permissions



High level view

Autoris. des applis

Appareil photo
4 application(s) autorisée(s) sur 17

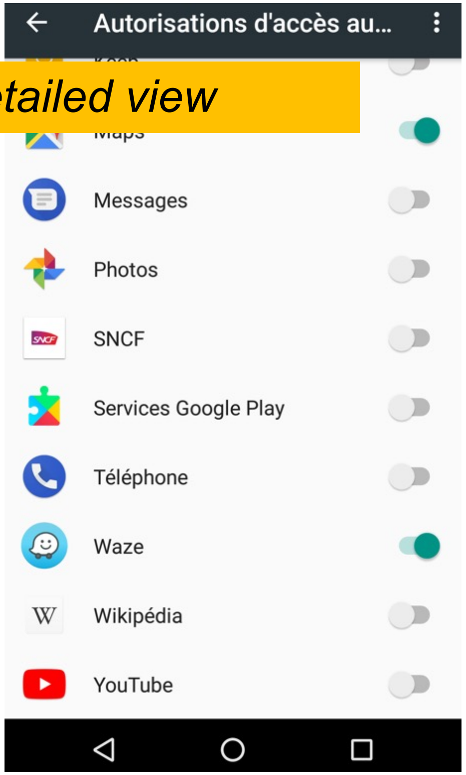
Capteurs corporels
0 application(s) autorisée(s) sur 2

Contacts
9 application(s) autorisée(s) sur 25

Microphone
4 application(s) autorisée(s) sur 15

Position
5 application(s) autorisée(s) sur 23

SMS
5 application(s) autorisée(s) sur 11



Detailed view

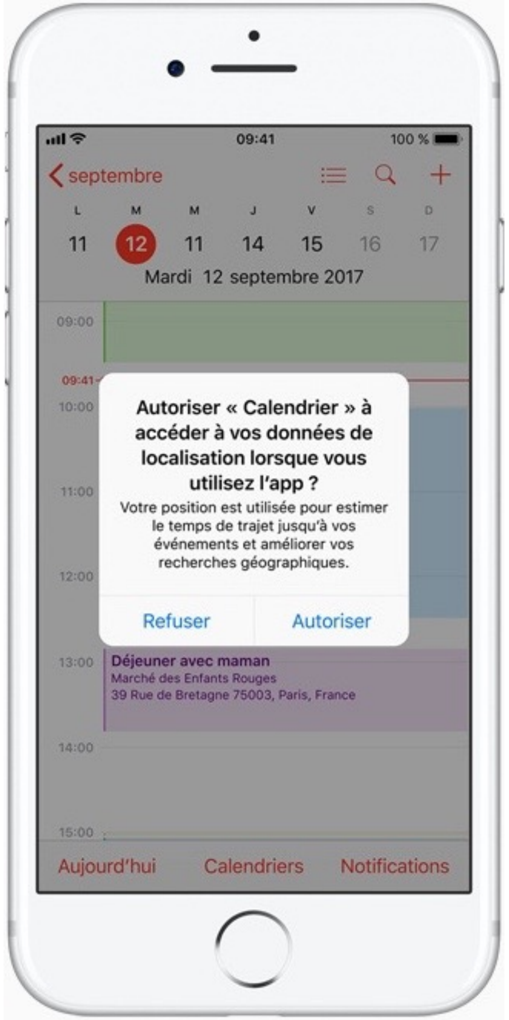
Autorisations d'accès au...

Maps	●
Messages	○
Photos	○
SNCF	○
Services Google Play	○
Téléphone	○
Waze	●
Wikipédia	○
YouTube	○

Dynamic Authorizations – iOS (1)

- Ask an explicit and targeted authorization upon **execution**.
  - ✓ Solution chosen by Apple since the beginning.
  - ✓ The user authorizes or refuses individually each authorization ☺.
  - ✓ The user can change his mind at any time ☺.

https://www.apple.com/fr/privacy/manage-your-privacy/



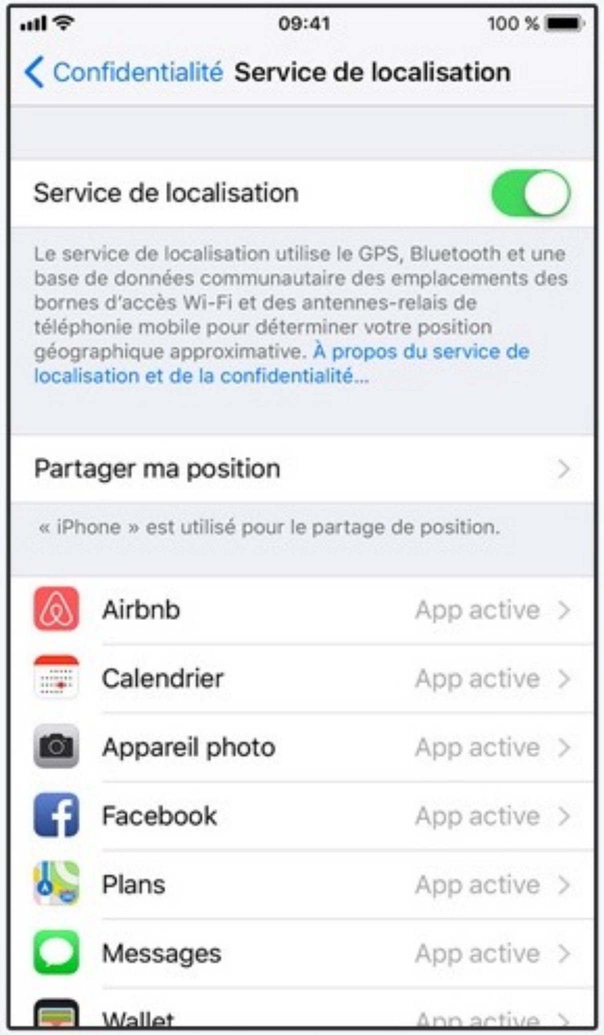
Autoriser « Calendrier » à accéder à vos données de localisation lorsque vous utilisez l'app ?

Votre position est utilisée pour estimer le temps de trajet jusqu'à vos événements et améliorer vos recherches géographiques.

Déjeuner avec maman
Marché des Enfants Rouges
39 Rue de Bretagne 75003, Paris, France

Dynamic Authorizations – iOS (2)

- Several control panels exist in order to:
  - ✓ list all applications asking certain authorizations;
  - ✓ list all authorizations asked by a given application.



09:41 100 %

Confidentialité **Service de localisation**

Service de localisation

Le service de localisation utilise le GPS, Bluetooth et une base de données communautaire des emplacements des bornes d'accès Wi-Fi et des antennes-relais de téléphonie mobile pour déterminer votre position géographique approximative. À propos du service de localisation et de la confidentialité...

Partager ma position

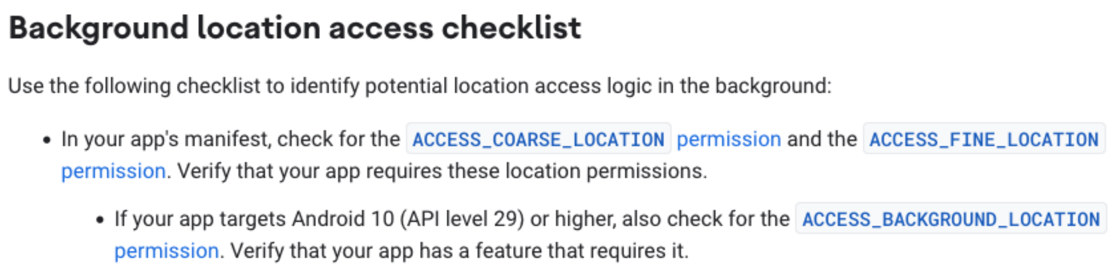
« iPhone » est utilisé pour le partage de position.

Airbnb	App active
Calendrier	App active
Appareil photo	App active
Facebook	App active
Plans	App active
Messages	App active
Wallet	App active

Excellent: “adding background activity limitation”

- App **behavioral control** was long needed
  - ✓ Example: authorizing an application to access my geolocation and Internet for a punctual need does not mean I authorize this application to send my geolocation every minute to remote servers (*a fortiori* in non-EU countries)!

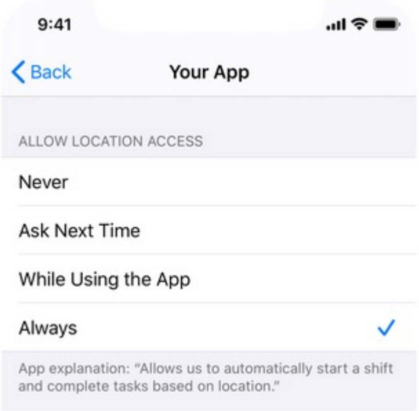
- A nice thing: “background activity limitation” in Android 10 and iOS 13
  - ✓ e.g., no access to user location by apps that run in the background



Background location access checklist

Use the following checklist to identify potential location access logic in the background:

- In your app's manifest, check for the `ACCESS_COARSE_LOCATION` permission and the `ACCESS_FINE_LOCATION` permission. Verify that your app requires these location permissions.
  - If your app targets Android 10 (API level 29) or higher, also check for the `ACCESS_BACKGROUND_LOCATION` permission. Verify that your app has a feature that requires it.



ALLOW LOCATION ACCESS

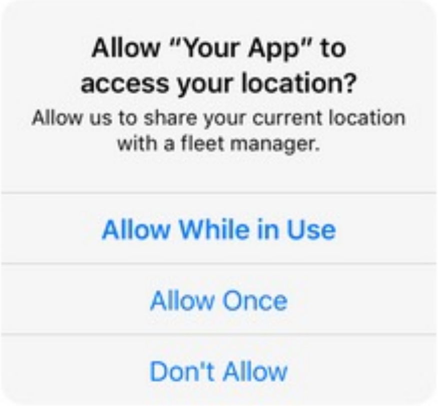
Never

Ask Next Time

While Using the App

Always ✓

App explanation: “Allows us to automatically start a shift and complete tasks based on location.”



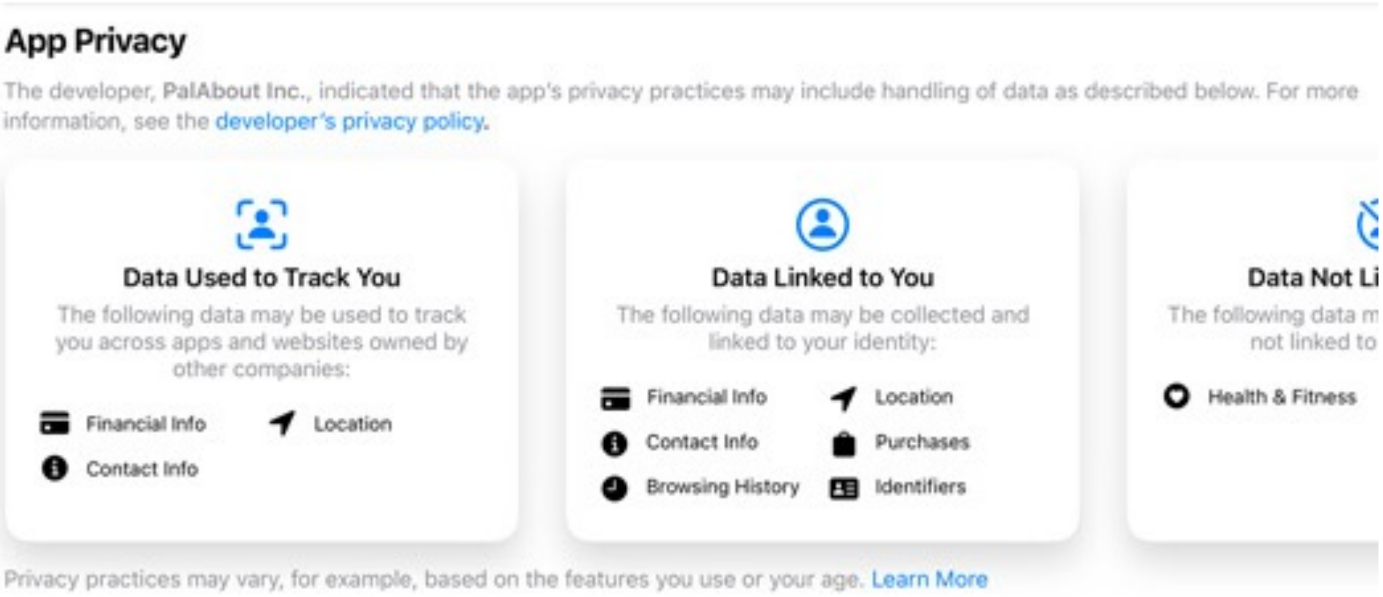
Allow “Your App” to access your location?

Allow us to share your current location with a fleet manager.

Excellent: “Apple requires per–app privacy details”

“About privacy information on the App Store and the choices you have to control your data
The App Store now includes detailed privacy information that helps you understand each app's data collection practices.
In June 2020, Apple announced a new privacy information section for product pages on the App Store. This is the beginning of an innovative new program to help customers have more transparency and understanding about what data apps may gather about them."

https://support.apple.com/en-lamr/HT211970



App Privacy

The developer, **PalAbout Inc.**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Financial Info
- Location
- Contact Info

Data Linked to You

The following data may be collected and linked to your identity:

- Financial Info
- Location
- Contact Info
- Purchases
- Browsing History
- Identifiers

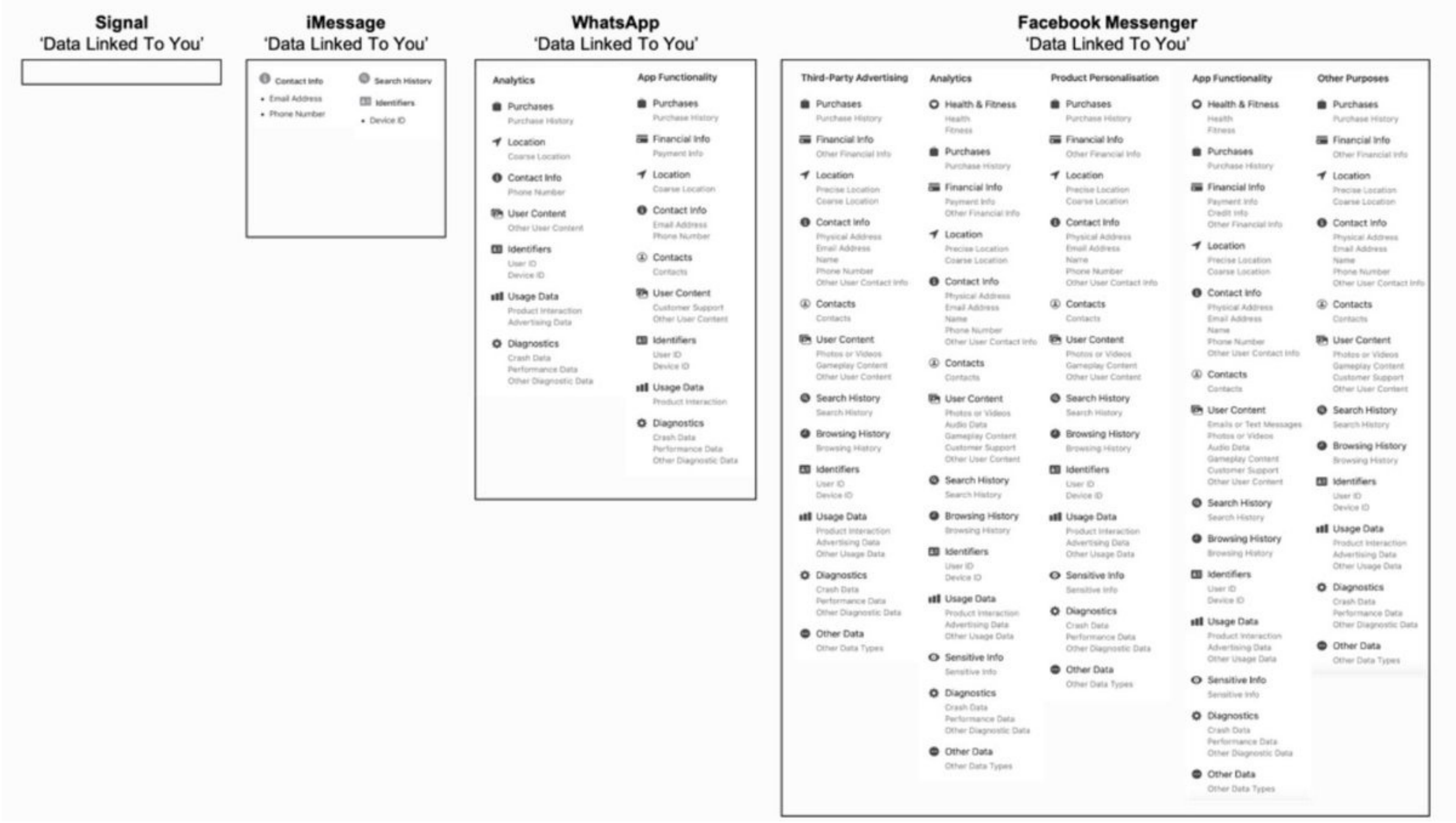
Data Not Li

The following data m
not linked to

- Health & Fitness

Privacy practices may vary, for example, based on the features you use or your age. Learn More

Excellent: “Apple requires privacy details” (2)



Signal
‘Data Linked To You’

iMessage
‘Data Linked To You’

Contact Info
- Email Address
- Phone Number

Search History

Identifiers
- Device ID

WhatsApp
‘Data Linked To You’

Analytics

Purchases
Purchase History

Location
Coarse Location

Contact Info
Phone Number

User Content
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

App Functionality

Purchases
Purchase History

Financial Info
Payment Info

Location
Coarse Location

Contact Info
Email Address
Phone Number

Contacts
Contacts

User Content
Customer Support
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Facebook Messenger
‘Data Linked To You’

Third-Party Advertising

Purchases
Purchase History

Financial Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Gameplay Content
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Analytics

Health & Fitness
Health
Fitness

Purchases
Purchase History

Financial Info
Payment Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Audio Data
Gameplay Content
Customer Support
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Sensitive Info
Sensitive Info

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Product Personalisation

Purchases
Purchase History

Financial Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Gameplay Content
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Sensitive Info
Sensitive Info

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

App Functionality

Health & Fitness
Health
Fitness

Purchases
Purchase History

Financial Info
Payment Info
Credit Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Emails or Text Messages
Photos or Videos
Audio Data
Gameplay Content
Customer Support
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Sensitive Info
Sensitive Info

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

Other Purposes

Purchases
Purchase History

Financial Info
Other Financial Info

Location
Precise Location
Coarse Location

Contact Info
Physical Address
Email Address
Name
Phone Number
Other User Contact Info

Contacts
Contacts

User Content
Photos or Videos
Gameplay Content
Customer Support
Other User Content

Search History
Search History

Browsing History
Browsing History

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data
Other Usage Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Other Data
Other Data Types

In summary

- When consent is the legal basis:
  - ✓ authorizations are meant to get the **“free, informed, specific and unequivocal consent”** of the user
  - ✓ it’s also a way for the user to **control** an app.

- Two different approaches:
  - ✓ at **installation time**: limited (we’re not living in a binary world), less used;
  - ✓ and/or **dynamically**: much better control.

- However, several nice initiatives
  - ✓ excellent initiative for more transparency.

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- **Limits of the user control**
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

Proposed authorizations approaches have limits

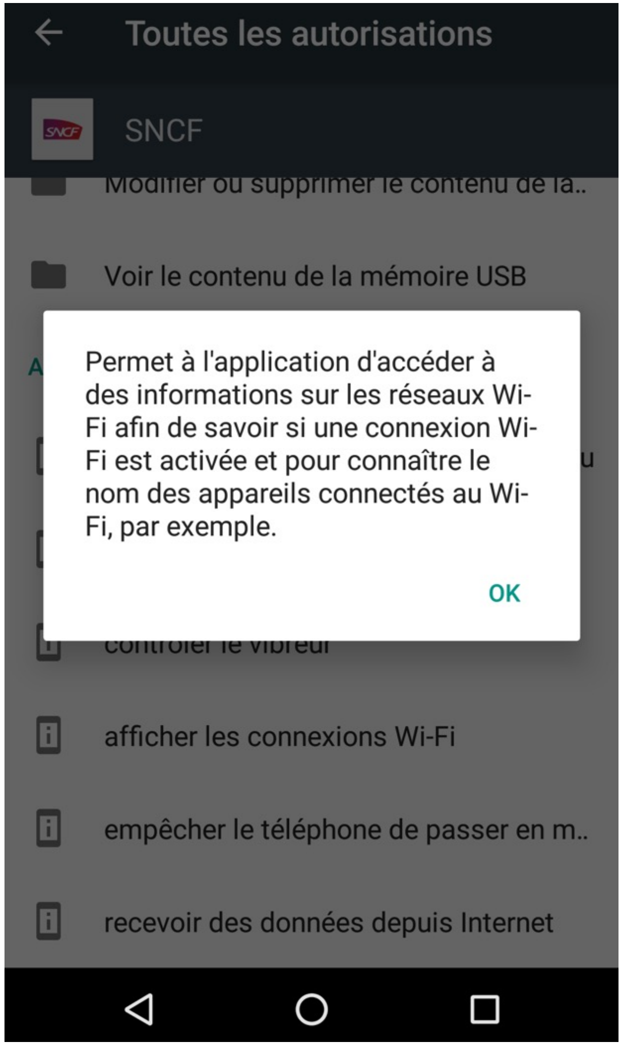
- Limits on the Android side.

- Limits common to Android and iOS :
  - ✓ lack of control on the **composition** of authorizations.

Limits of Android authorization system (1)

- The authorization system is **complex** ☹
  - A total of **147 authorizations** (Oct. 2017).
  - Users **cannot always assess the implications of authorizations**
  - Example : *« afficher les connections Wi-Fi »*
    - ✓ ambiguous (“Name of connected devices”? All of them?)
    - ✓ non exhaustive list provided
    - ✓ also grants access to the Wi-Fi MAC address…

      Useful to track me but it’s never said.



Toutes les autorisations

SNCF

Modifier ou supprimer le contenu de la..

Voir le contenu de la mémoire USB

Permet à l'application d'accéder à des informations sur les réseaux Wi-Fi afin de savoir si une connexion Wi-Fi est activée et pour connaître le nom des appareils connectés au Wi-Fi, par exemple.

OK

contrôler le vibreur

afficher les connexions Wi-Fi

empêcher le téléphone de passer en m..

recevoir des données depuis Internet

Limits of Android authorization system (2)

- Google made a **questionable classification**
  - ✓ **“normal”** authorizations
    - ○ No explicit information nor user solicitation is needed for “normal” authorizations!
    - ○ It’s up to the user search authorizations in the Play Store or in the smartphone’s Parameters!
  - ✓ **“dangerous”** authorizations

Limits of Android authorization system (3)

> https://developer.android.com/guide/topics/permissions/normal-permissions.html
>
> **Normal Permissions**
> “Many permissions are designated as PROTECTION_NORMAL, which indicates that there's no great risk to the user's privacy or security in letting apps have those permissions. […]
>
> If an app declares in its manifest that it needs a normal permission, the system automatically grants the app that permission at install time. The system does not prompt the user to grant normal permissions, and users cannot revoke these permissions.”

- Do you really think there’s no risk for the user privacy?
- These authorizations enable, for instance to:
  - ✓ access stable identifiers to track the user;
  - ✓ know the list of Wi-Fi networks used in the past;
  - ✓ access Internet (e.g. to send personal information to remote servers);
  - ✓ activate Wi-Fi ;
  - ✓ etc.

Limits common to Android and iOS

- No control on the **composition of authorizations** ☹

  ✓ Example: authorizing an application to access my geolocation and Internet does not mean I authorize this application to send my geolocation to remote servers (*a fortiori* in non-EU countries)!

A common drift

- It’s not because it’s technically feasible that:
  - ✓ (1) it’s legal;
  - ✓ (2) the user gave his/her consent.

- The InMobi A&A company has been condemned because of their bad practices
  - ▪ see ACCESS_WIFI_STATE later…
    - ✓ https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked

In summary

- The Android approach is **far from satisfying** IMHO.
  - ✓ The trend to dynamic authorizations is a real plus.
  - ✓ However Android permissions remain questionable.

- The iOS approach is **more virtuous** (started earlier, goes further)
  - ✓ A deliberate choice of Apple to favor privacy in his commercial offer.

- Improvements remain possible in both environments.
  - ✓ Offering more control and information to the user while keeping a simple and attractive GUI remains a challenge.

Further references

- CNIL – Inria, « Mobilitics, saison 2 : nouvelle plongée dans l'univers des smartphones et de leurs applications », décembre 2014. https://www.cnil.fr/fr/mobilitics-saison-2-nouvelle-plongee-dans-lunivers-des-smartphones-et-de-leurs-applications

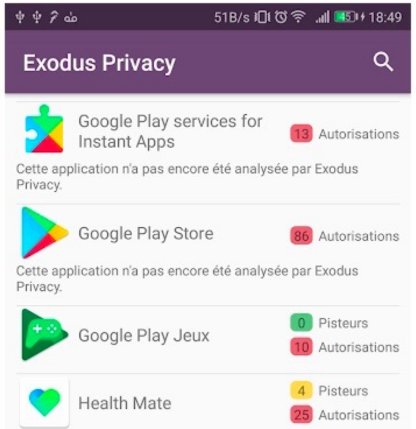
- J. Achara, M. Cunche, V. Roca, A. Francillon, **« Short Paper: WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission »,** 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)), July 2014. http://hal.inria.fr/hal-00997716/en/
  - ✓ Traite des dérives permises par la permission ACCESS_WIFI_STATE telle que définie avant Android 6.0.

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- **Tracking the trackers with Exodus-Privacy**
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

Tracking the trackers with Exodus-Privacy

- An impressive analysis service to track trackers in Android apps!
  - ✓ a French 1901 law non-profit organization
- a web site with app and tracker analyses
  - ✓ https://reports.exodus-privacy.eu.org/fr/search/
  - ✓ similar in spirit to what exists for web sites
- an Android app to install on your smartphone
  - ✓ https://play.google.com/store/apps/details?id=org.eu.exodus_privacy.exodusprivacy



Google Play services for Instant Apps — 13 Autorisations

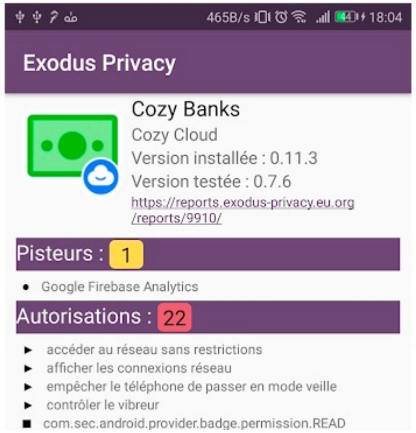
Cette application n'a pas encore été analysée par Exodus Privacy.

Google Play Store — 86 Autorisations

Cette application n'a pas encore été analysée par Exodus Privacy.

Google Play Jeux — 0 Pisteurs, 10 Autorisations

Health Mate — 4 Pisteurs, 25 Autorisations



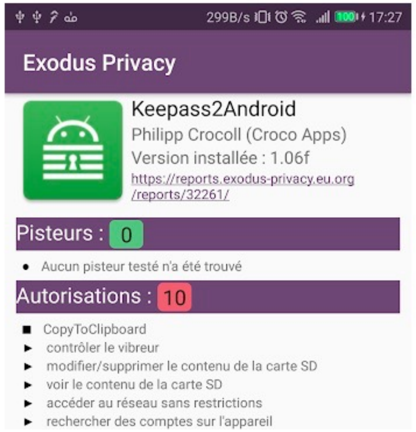
Cozy Banks
Cozy Cloud
Version installée : 0.11.3
Version testée : 0.7.6
https://reports.exodus-privacy.eu.org/reports/9910/

Pisteurs : 1

- Google Firebase Analytics

Autorisations : 22

- ▸ accéder au réseau sans restrictions
- ▸ afficher les connexions réseau
- ▸ empêcher le téléphone de passer en mode veille
- ▸ contrôler le vibreur
- ■ com.sec.android.provider.badge.permission.READ



Keepass2Android
Philipp Crocoll (Croco Apps)
Version installée : 1.06f
https://reports.exodus-privacy.eu.org/reports/32261/

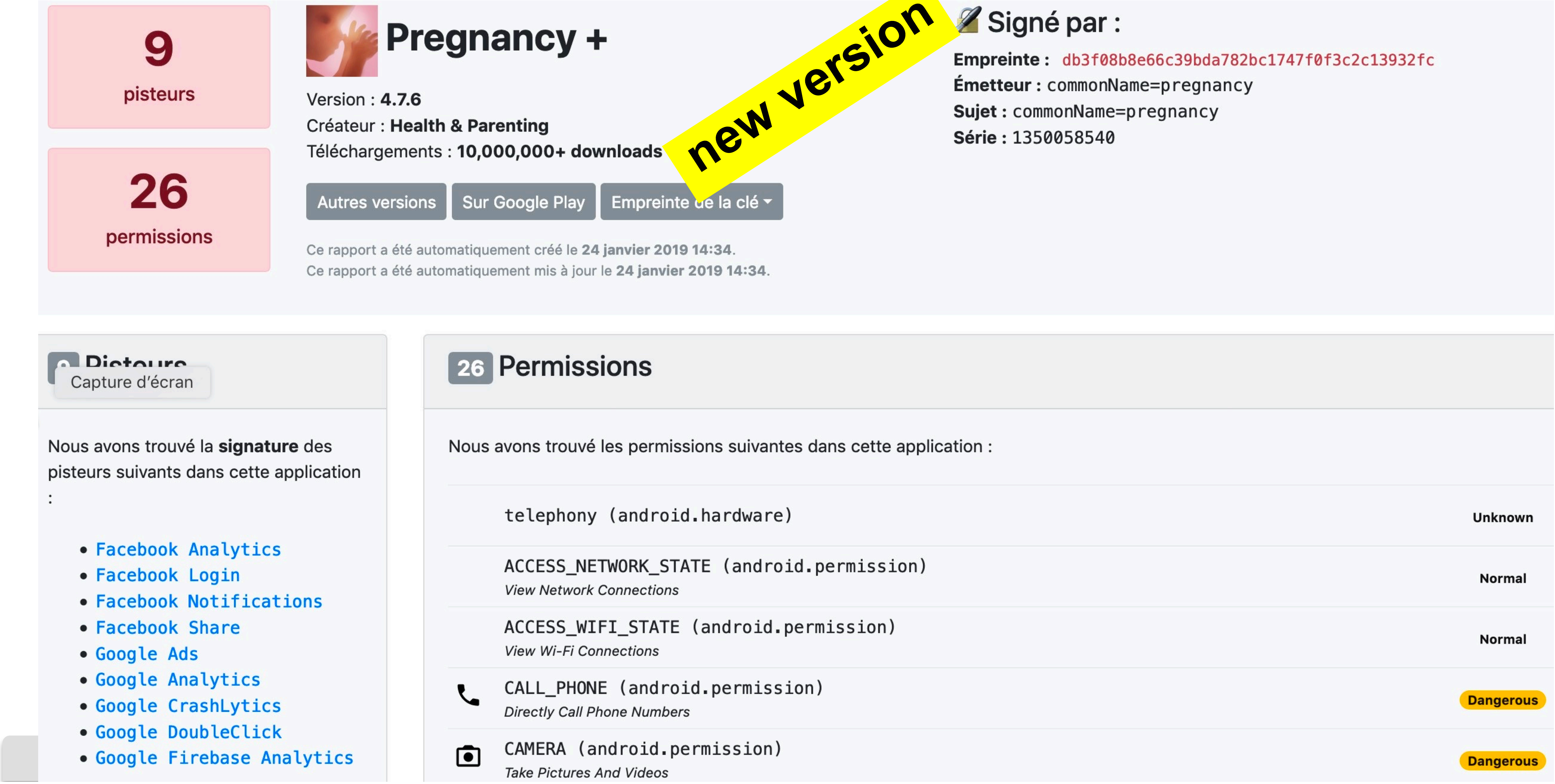
Pisteurs : 0

- Aucun pisteur testé n'a été trouvé

Autorisations : 10

- ■ CopyToClipboard
- ▸ contrôler le vibreur
- ▸ modifier/supprimer le contenu de la carte SD
- ▸ voir le contenu de la carte SD
- ▸ accéder au réseau sans restrictions
- ▸ rechercher des comptes sur l'appareil

In practice: Pregnancy+ analysis



new version

9
pisteurs

26
permissions

Pregnancy +

Version : **4.7.6**
Créateur : **Health & Parenting**
Téléchargements : **10,000,000+ downloads**

Ce rapport a été automatiquement créé le **24 janvier 2019 14:34**.
Ce rapport a été automatiquement mis à jour le **24 janvier 2019 14:34**.

Signé par :

Empreinte : `db3f08b8e66c39bda782bc1747f0f3c2c13932fc`
Émetteur : `commonName=pregnancy`
Sujet : `commonName=pregnancy`
Série : `1350058540`

9 Pisteurs

Nous avons trouvé la **signature** des pisteurs suivants dans cette application :

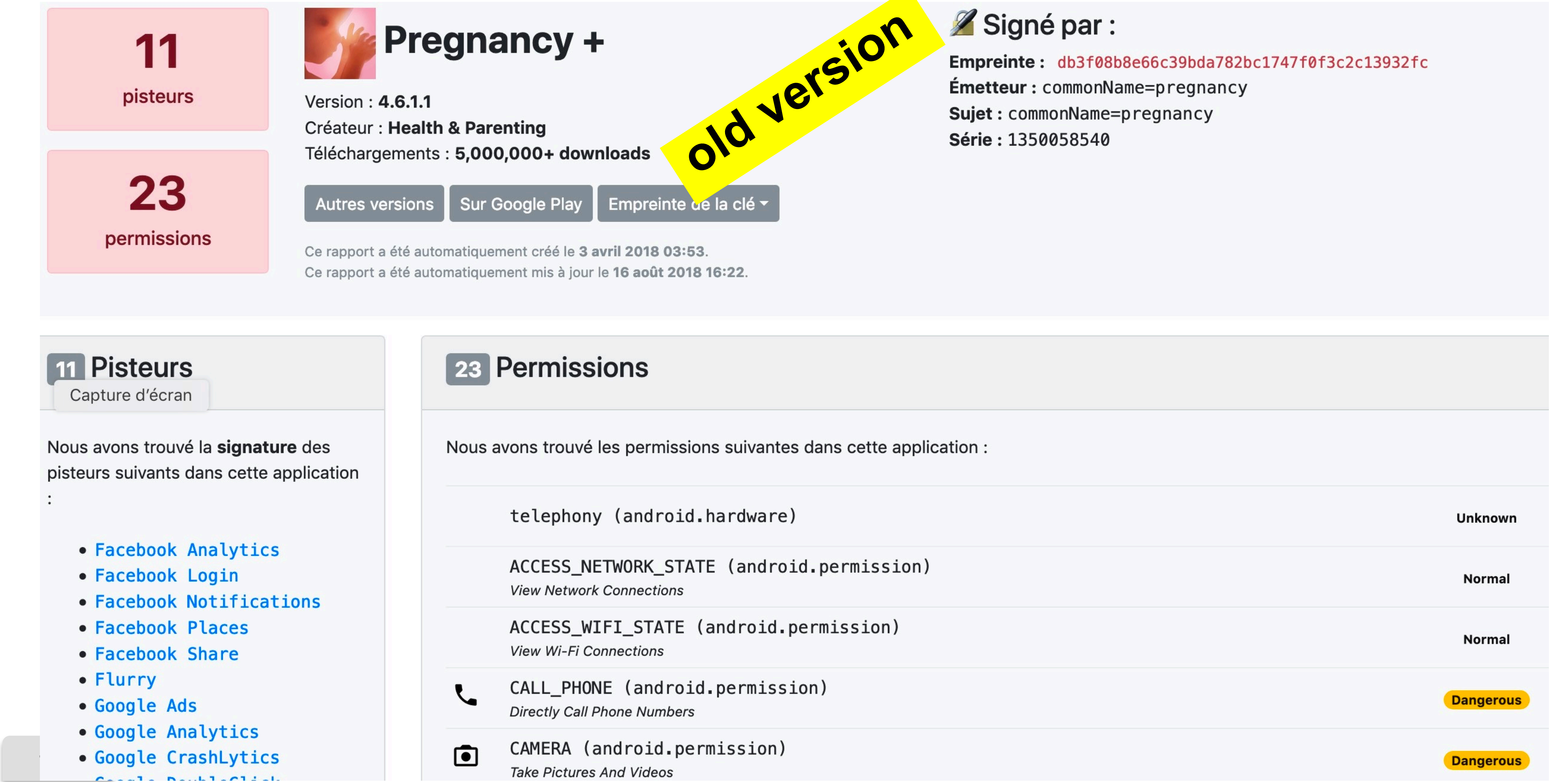
- Facebook Analytics
- Facebook Login
- Facebook Notifications
- Facebook Share
- Google Ads
- Google Analytics
- Google CrashLytics
- Google DoubleClick
- Google Firebase Analytics

26 Permissions

Nous avons trouvé les permissions suivantes dans cette application :

	`telephony (android.hardware)`	Unknown
	`ACCESS_NETWORK_STATE (android.permission)` *View Network Connections*	Normal
	`ACCESS_WIFI_STATE (android.permission)` *View Wi-Fi Connections*	Normal
☎	`CALL_PHONE (android.permission)` *Directly Call Phone Numbers*	Dangerous
📷	`CAMERA (android.permission)` *Take Pictures And Videos*	Dangerous

In practice: Pregnancy+ analysis (2)



11 pisteurs

23 permissions

Pregnancy +

Version : **4.6.1.1**
Créateur : **Health & Parenting**
Téléchargements : **5,000,000+ downloads**

Ce rapport a été automatiquement créé le **3 avril 2018 03:53**.
Ce rapport a été automatiquement mis à jour le **16 août 2018 16:22**.

Signé par :

Empreinte : `db3f08b8e66c39bda782bc1747f0f3c2c13932fc`
Émetteur : `commonName=pregnancy`
Sujet : `commonName=pregnancy`
Série : `1350058540`

11 Pisteurs

Capture d'écran

Nous avons trouvé la **signature** des pisteurs suivants dans cette application :

- Facebook Analytics
- Facebook Login
- Facebook Notifications
- Facebook Places
- Facebook Share
- Flurry
- Google Ads
- Google Analytics
- Google CrashLytics
- Google DoubleClick

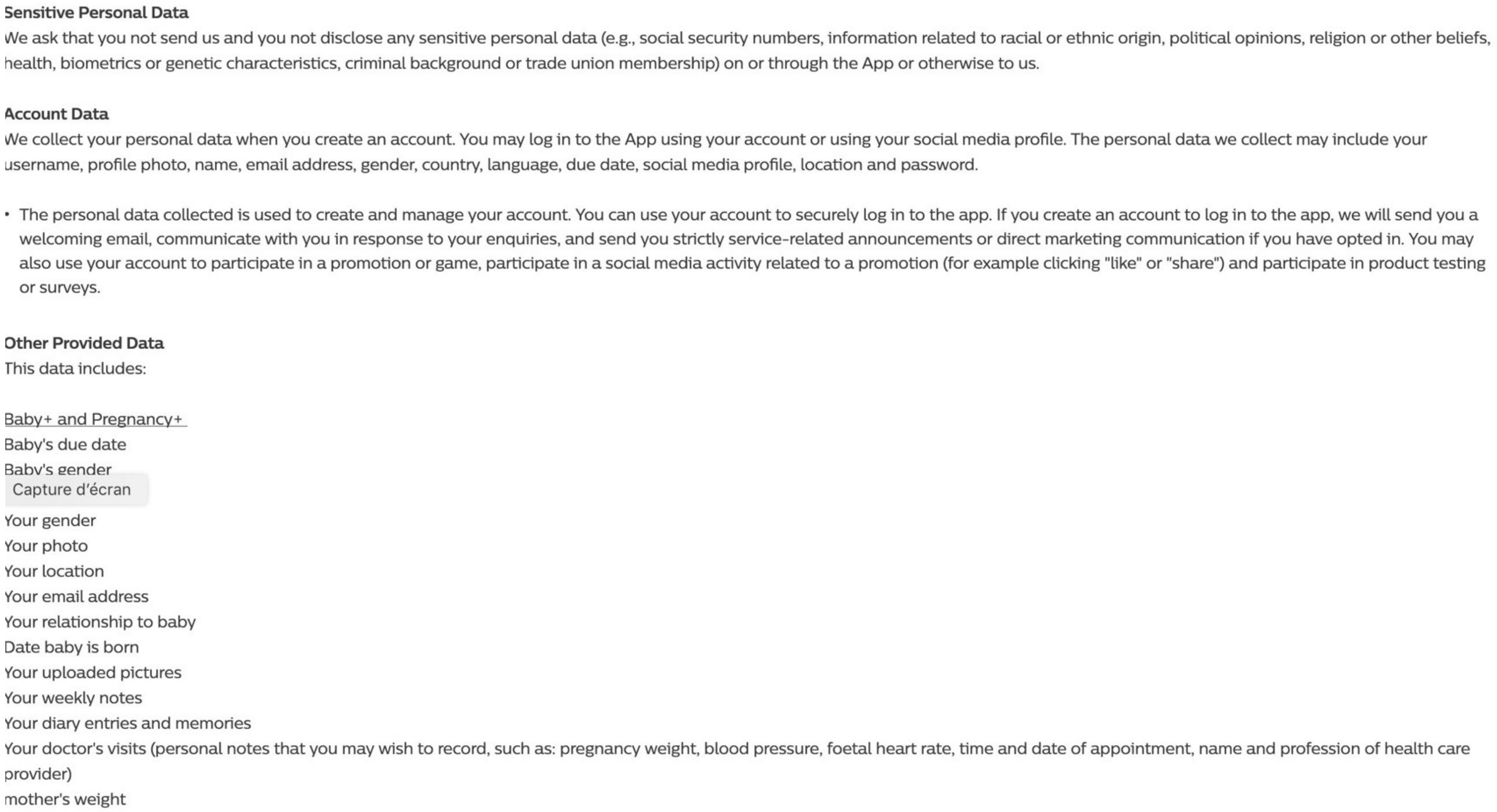
23 Permissions

Nous avons trouvé les permissions suivantes dans cette application :

	`telephony (android.hardware)`	Unknown
	`ACCESS_NETWORK_STATE (android.permission)` *View Network Connections*	Normal
	`ACCESS_WIFI_STATE (android.permission)` *View Wi-Fi Connections*	Normal
☎	`CALL_PHONE (android.permission)` *Directly Call Phone Numbers*	Dangerous
📷	`CAMERA (android.permission)` *Take Pictures And Videos*	Dangerous

In practice: Pregnancy+ analysis (3)

- Looking at **Privacy Policy** https://www.philips.co.uk/c-w/privacy/pregnancy-and-baby.html



Sensitive Personal Data

We ask that you not send us and you not disclose any sensitive personal data (e.g., social security numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background or trade union membership) on or through the App or otherwise to us.

Account Data

We collect your personal data when you create an account. You may log in to the App using your account or using your social media profile. The personal data we collect may include your username, profile photo, name, email address, gender, country, language, due date, social media profile, location and password.

- The personal data collected is used to create and manage your account. You can use your account to securely log in to the app. If you create an account to log in to the app, we will send you a welcoming email, communicate with you in response to your enquiries, and send you strictly service-related announcements or direct marketing communication if you have opted in. You may also use your account to participate in a promotion or game, participate in a social media activity related to a promotion (for example clicking "like" or "share") and participate in product testing or surveys.

Other Provided Data

This data includes:

Baby+ and Pregnancy+

Baby's due date

Baby's gender

Capture d'écran

Your gender

Your photo

Your location

Your email address

Your relationship to baby

Date baby is born

Your uploaded pictures

Your weekly notes

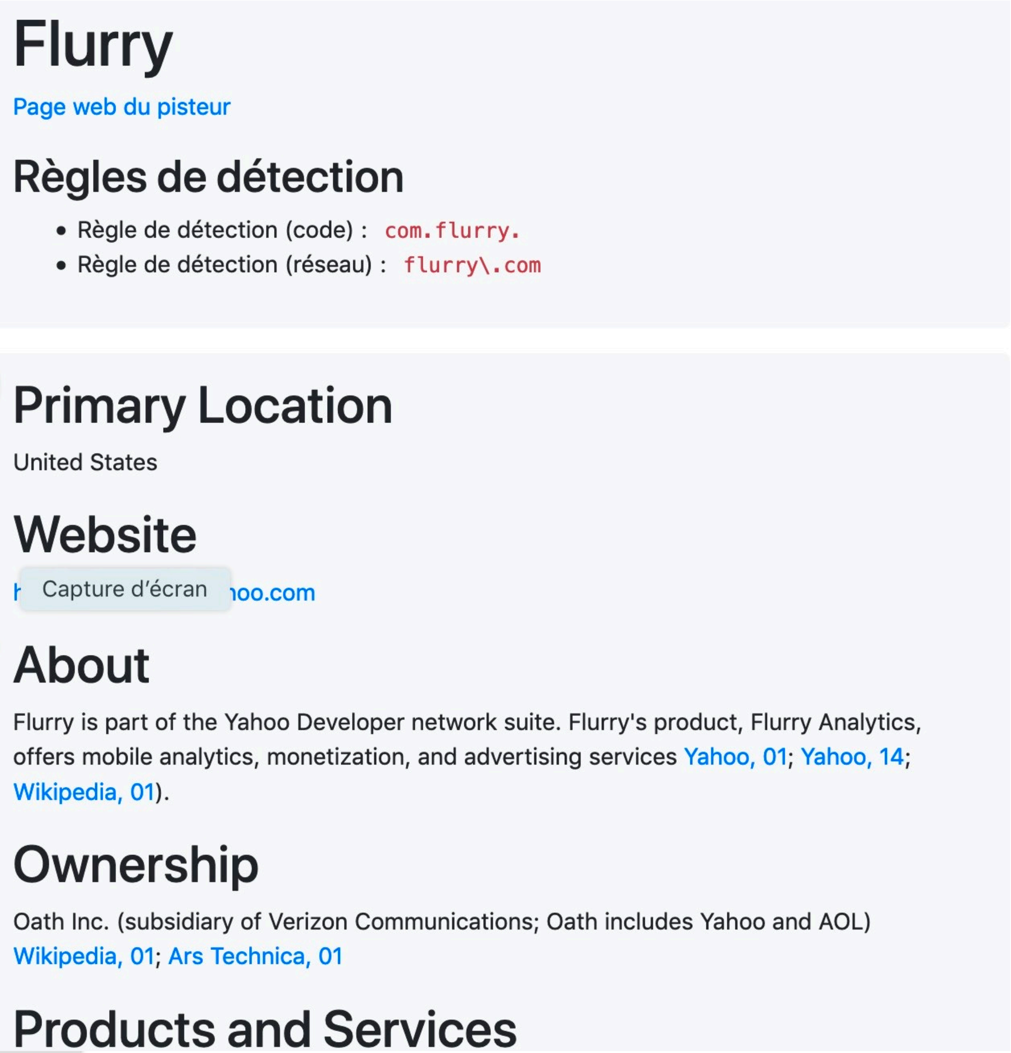
Your diary entries and memories

Your doctor's visits (personal notes that you may wish to record, such as: pregnancy weight, blood pressure, foetal heart rate, time and date of appointment, name and profession of health care provider)

mother's weight

contradiction
+
very intrusive approach, with sensitive data collection

In practice: tracker statistics (Flurry close-up)



Flurry

Page web du pisteur

Règles de détection

- Règle de détection (code) : `com.flurry.`
- Règle de détection (réseau) : `flurry\.com`

Primary Location

United States

Website

h Capture d’écran ıoo.com

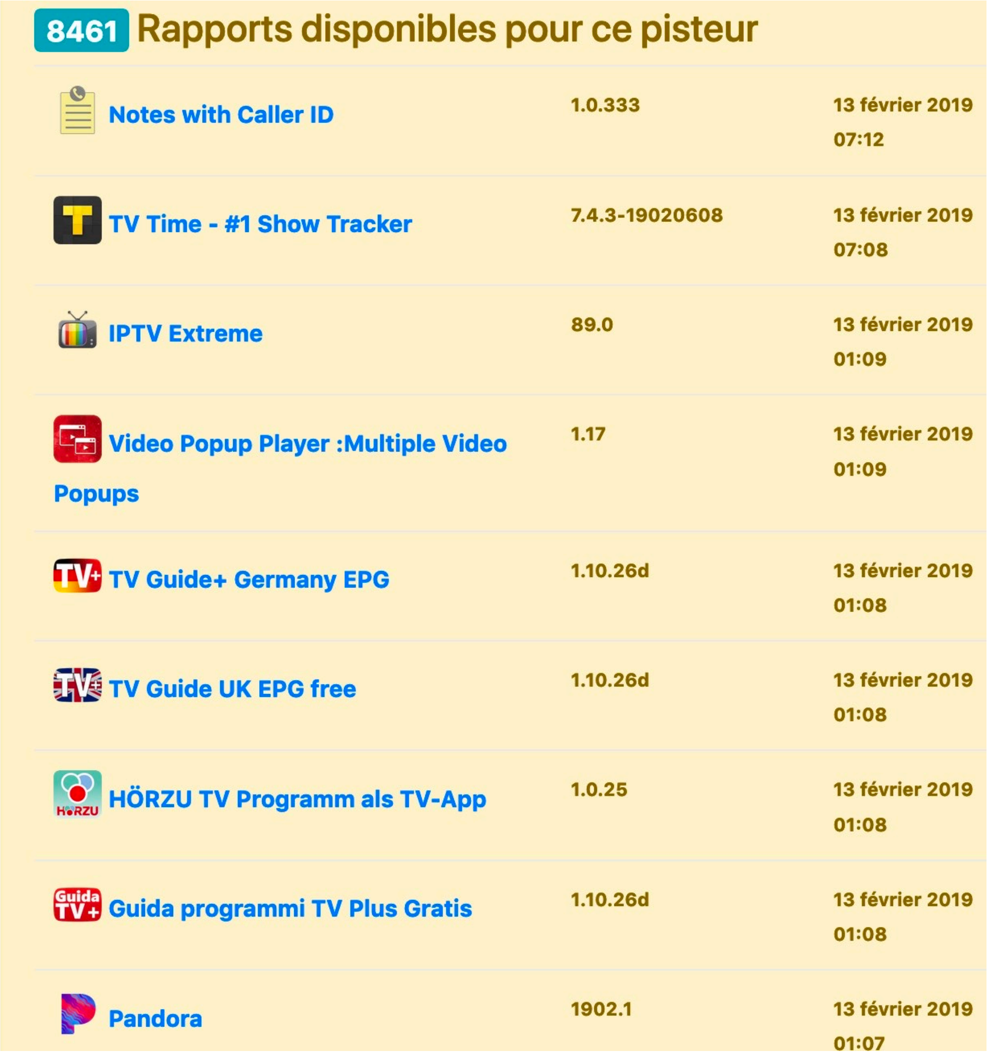
About

Flurry is part of the Yahoo Developer network suite. Flurry's product, Flurry Analytics, offers mobile analytics, monetization, and advertising services Yahoo, 01; Yahoo, 14; Wikipedia, 01).

Ownership

Oath Inc. (subsidiary of Verizon Communications; Oath includes Yahoo and AOL) Wikipedia, 01; Ars Technica, 01

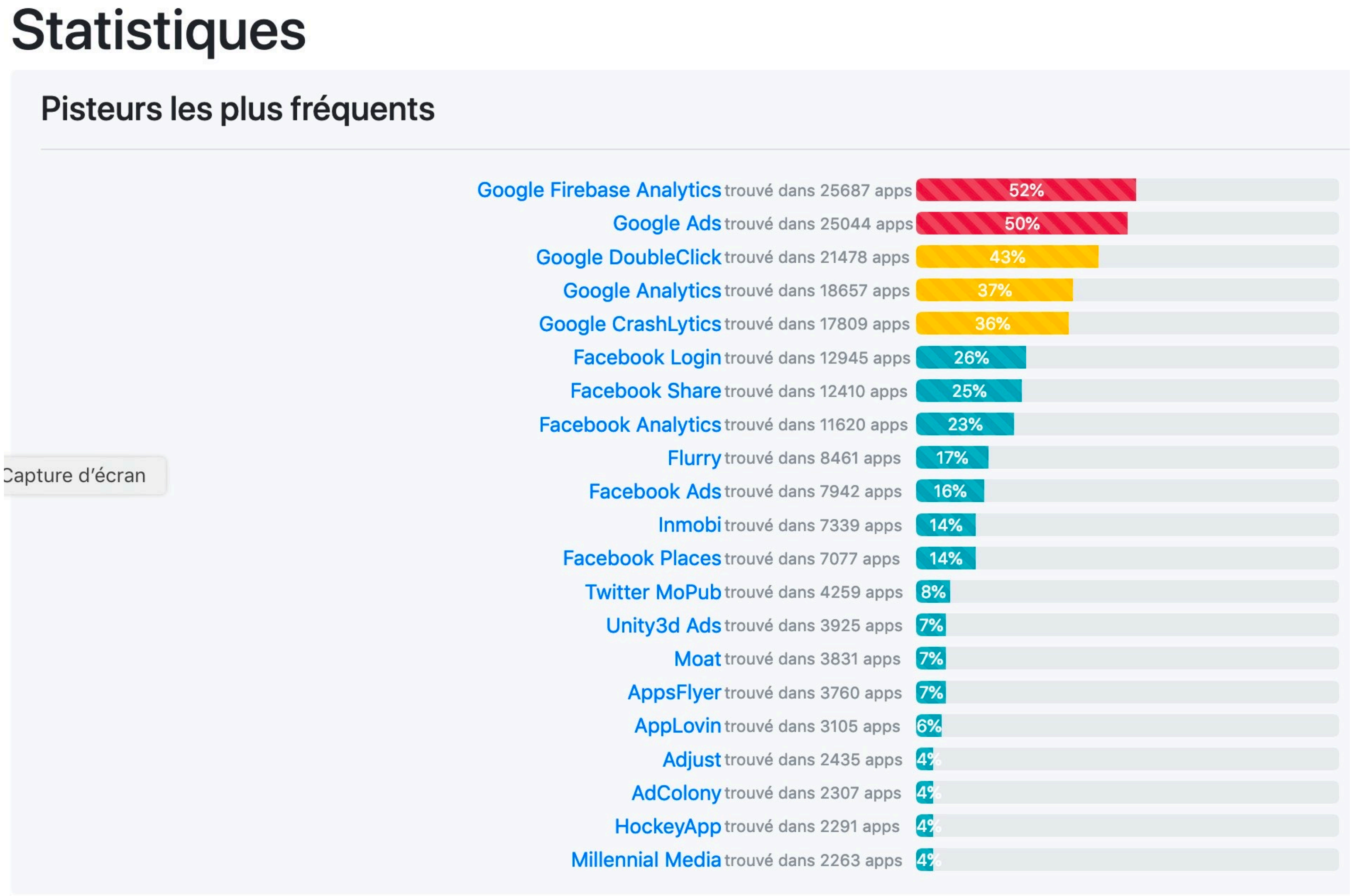
Products and Services



8461 Rapports disponibles pour ce pisteur

Notes with Caller ID	1.0.333	13 février 2019 07:12
TV Time - #1 Show Tracker	7.4.3-19020608	13 février 2019 07:08
IPTV Extreme	89.0	13 février 2019 01:09
Video Popup Player :Multiple Video Popups	1.17	13 février 2019 01:09
TV Guide+ Germany EPG	1.10.26d	13 février 2019 01:08
TV Guide UK EPG free	1.10.26d	13 février 2019 01:08
HÖRZU TV Programm als TV-App	1.0.25	13 février 2019 01:08
Guida programmi TV Plus Gratis	1.10.26d	13 février 2019 01:08
Pandora	1902.1	13 février 2019 01:07

In practice: tracker statistics (global view) (2)



Statistiques

Pisteurs les plus fréquents

Google Firebase Analytics trouvé dans 25687 apps 52%

Google Ads trouvé dans 25044 apps 50%

Google DoubleClick trouvé dans 21478 apps 43%

Google Analytics trouvé dans 18657 apps 37%

Google CrashLytics trouvé dans 17809 apps 36%

Facebook Login trouvé dans 12945 apps 26%

Facebook Share trouvé dans 12410 apps 25%

Facebook Analytics trouvé dans 11620 apps 23%

Flurry trouvé dans 8461 apps 17%

Facebook Ads trouvé dans 7942 apps 16%

Inmobi trouvé dans 7339 apps 14%

Facebook Places trouvé dans 7077 apps 14%

Twitter MoPub trouvé dans 4259 apps 8%

Unity3d Ads trouvé dans 3925 apps 7%

Moat trouvé dans 3831 apps 7%

AppsFlyer trouvé dans 3760 apps 7%

AppLovin trouvé dans 3105 apps 6%

Adjust trouvé dans 2435 apps 4%

AdColony trouvé dans 2307 apps 4%

HockeyApp trouvé dans 2291 apps 4%

Millennial Media trouvé dans 2263 apps 4%

Capture d’écran

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Tracking the trackers in practice
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- **Conclusion: towards a virtuous circle**

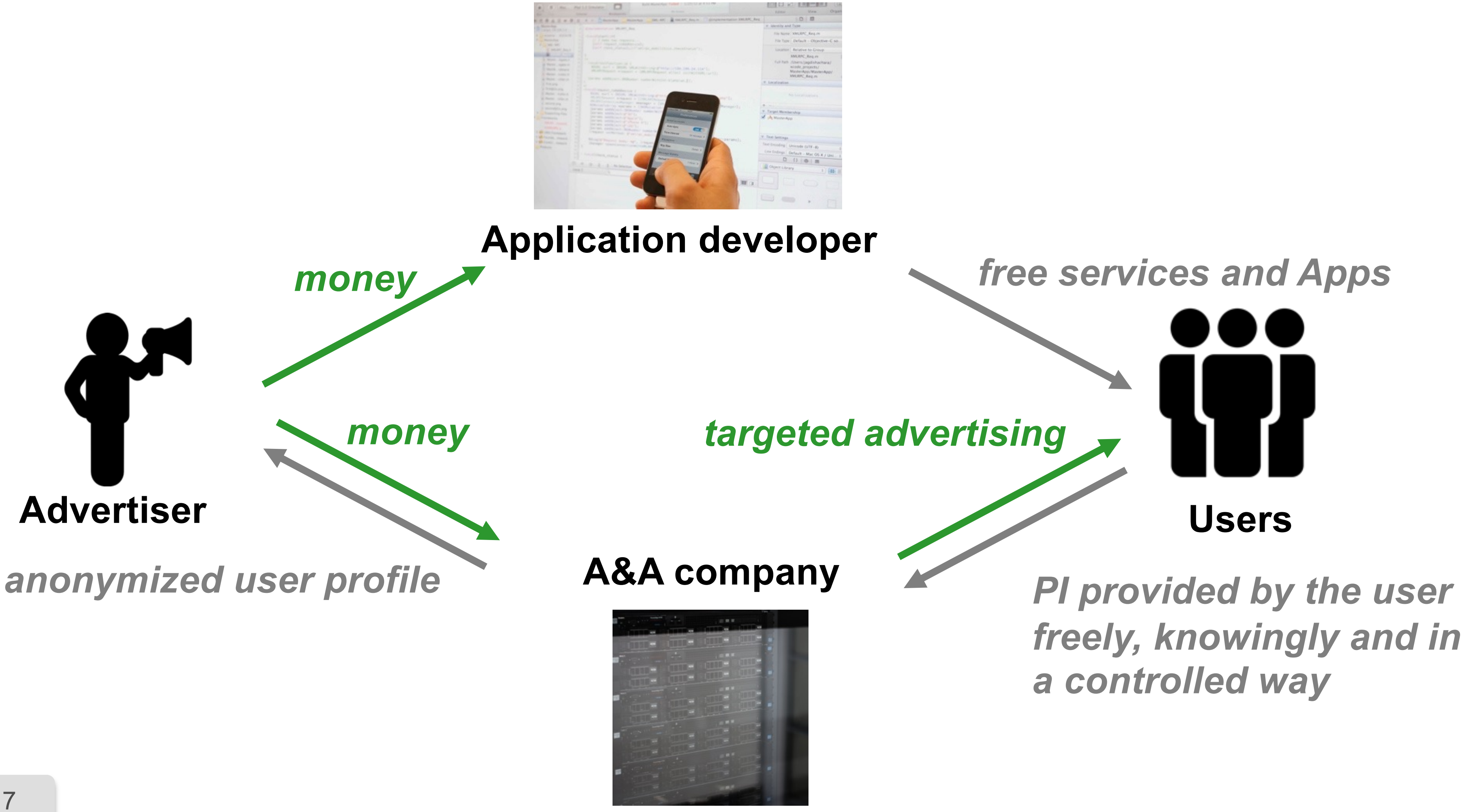
A shared responsibility

- **The user** has a key role but also a **limited power**.
  - ✓ Common sense rules can reduce the risks…
  - ✓ … but there are limits (especially with Android).

- **The Operating System editor** has a **key role**.
  - ✓ He defines the **rules!**
  - ✓ Differences between Google and Apple. Is it surprising given their business model?

- **The regulator** has a **key role**.
  - ✓ FR and EU laws are very protective.
  - ✓ New EU regulation (GDPR) further reinforces the power of EU with respect to foreign companies.

Virtuous Circle: the free model



Application developer

money

free services and Apps

Advertiser

money

targeted advertising

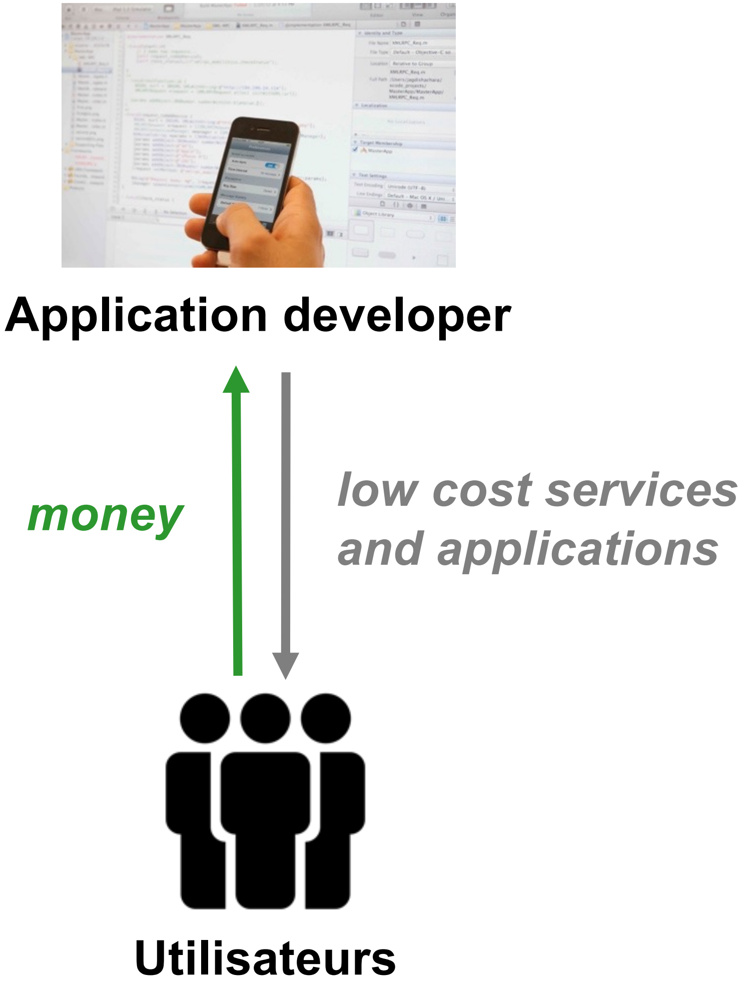
Users

anonymized user profile

A&A company

PI provided by the user
freely, knowingly and in
a controlled way

Virtuous Circle: the paying model



Application developer

money

low cost services
and applications

Utilisateurs

There are several conditions

- The **users**:
  - ✓ are “responsible”: someone must **financially support** the work of developers;
  - ✓ have **control** on the provided information.

- Each **actor**:
  - ✓ is **transparent** with respect to his practices;
  - ✓ can **prove** his practices, also known as **accountability**.

- **Trusted third parties** are needed:
  - ✓ in order to **check** practices.

An utopia?

- Of course, we all know the "**privacy paradox**"
  - ✓ Users say they worry about privacy but at the same time they act in the opposite way.
  - ✓ Isn't it the result of the recognition they have lost control?

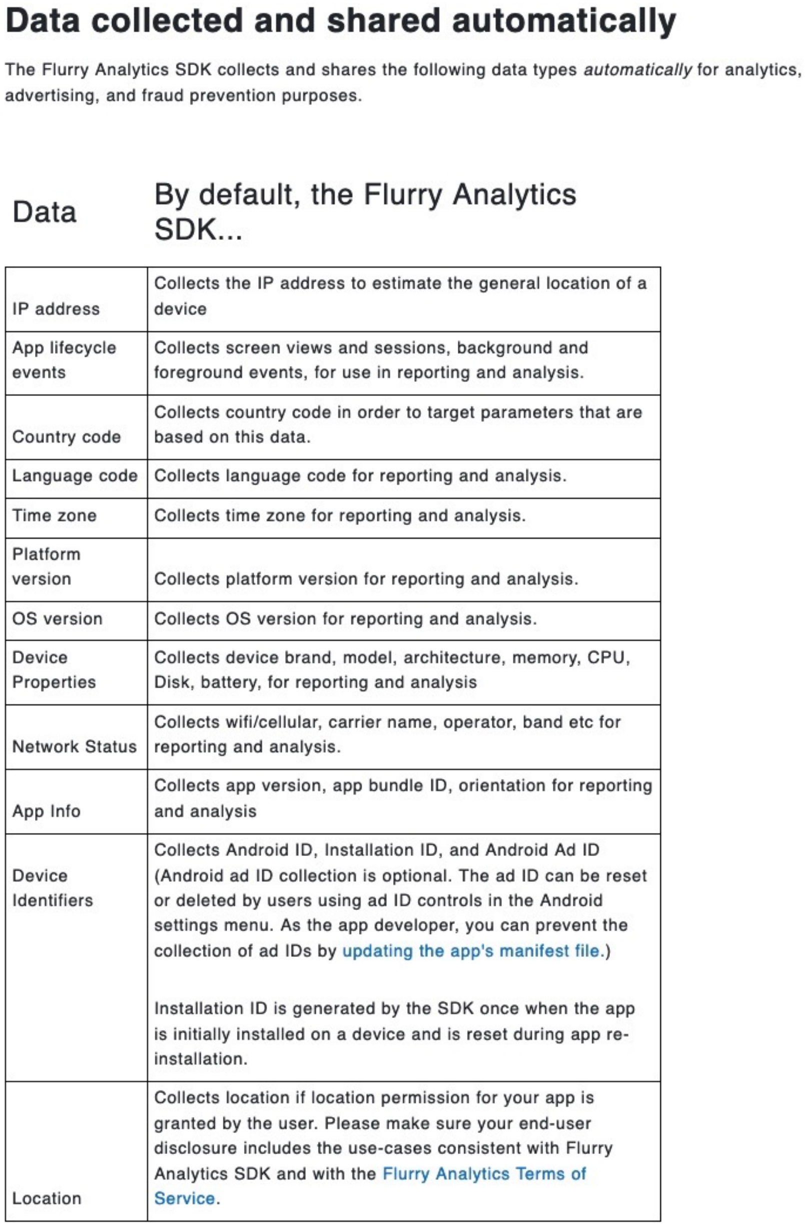
- In economy, **markets with a strong information asymmetry are known to be fragile**
  - ✓ they are not sustainable during long periods
  - ✓ Users do not trust them;
  - ✓ Alternative solutions appear.

- … it's everybody's interest at **mid/long term.**

- The Exodus Privacy service (and app) to identify trackers in Android apps
  - ✓ https://exodus-privacy.eu.org

- Examples of Personal Data collection by Flurry in their sdk

https://www.flurry.com/blog/google-play-data-disclosure-requirements/



Data collected and shared automatically

The Flurry Analytics SDK collects and shares the following data types *automatically* for analytics, advertising, and fraud prevention purposes.

Data	By default, the Flurry Analytics SDK...
IP address	Collects the IP address to estimate the general location of a device
App lifecycle events	Collects screen views and sessions, background and foreground events, for use in reporting and analysis.
Country code	Collects country code in order to target parameters that are based on this data.
Language code	Collects language code for reporting and analysis.
Time zone	Collects time zone for reporting and analysis.
Platform version	Collects platform version for reporting and analysis.
OS version	Collects OS version for reporting and analysis.
Device Properties	Collects device brand, model, architecture, memory, CPU, Disk, battery, for reporting and analysis
Network Status	Collects wifi/cellular, carrier name, operator, band etc for reporting and analysis.
App Info	Collects app version, app bundle ID, orientation for reporting and analysis
Device Identifiers	Collects Android ID, Installation ID, and Android Ad ID (Android ad ID collection is optional. The ad ID can be reset or deleted by users using ad ID controls in the Android settings menu. As the app developer, you can prevent the collection of ad IDs by updating the app's manifest file.) Installation ID is generated by the SDK once when the app is initially installed on a device and is reset during app re-installation.
Location	Collects location if location permission for your app is granted by the user. Please make sure your end-user disclosure includes the use-cases consistent with Flurry Analytics SDK and with the Flurry Analytics Terms of Service.

Thank you… ☺

vincent.roca@inria.fr

Hey! What about my privacy??
They say that people who worry about their privacy have something to hide ...
Grea
sangrea.net