UNIVERSITÉ CÔTE D'AZUR

Inria INVENTEURS DU MONDE NUMÉRIQUE

07. Privacy and smartphones

(slides of Vincent Roca)

Nataliia Bielova

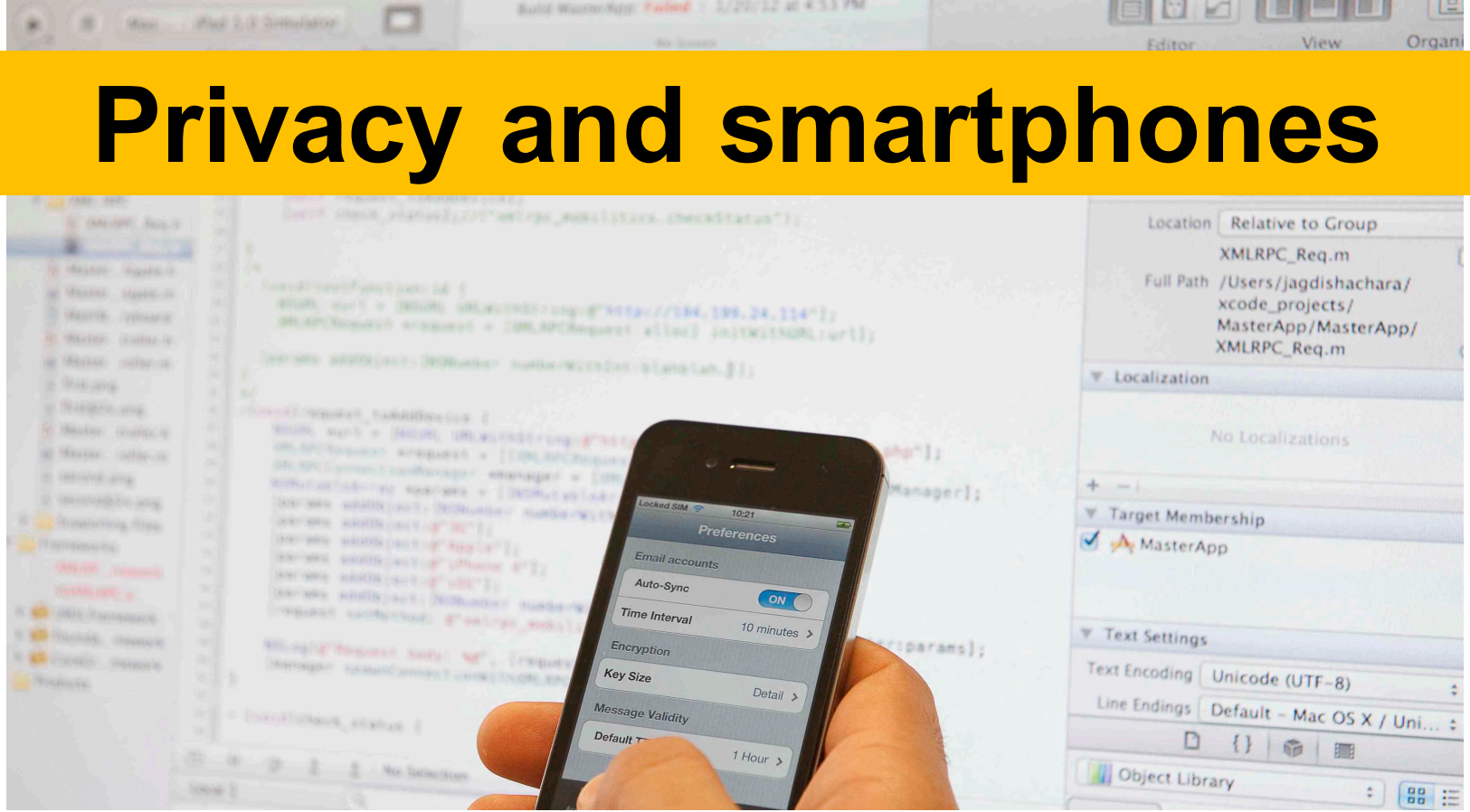
@nataliabielova

September 17th-21st, 2018

Web Privacy course

University of Trento

Privacy and smartphones



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

informatiques mathématiques
Inria

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
- 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
- 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!

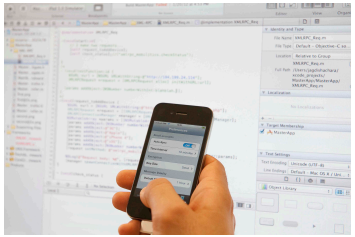
- As well as our centers of interest through the list of installed applications
- Many actors are interested by this wealth of PI
  - ✓ Our **“mouchard de poche”?**

Outline

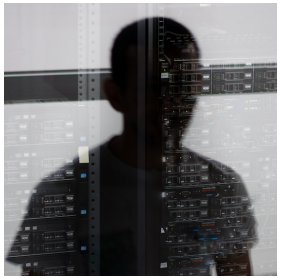
- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- **The ecosystem around applications for smartphones**
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- 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

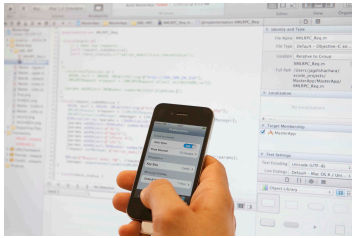
User

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.

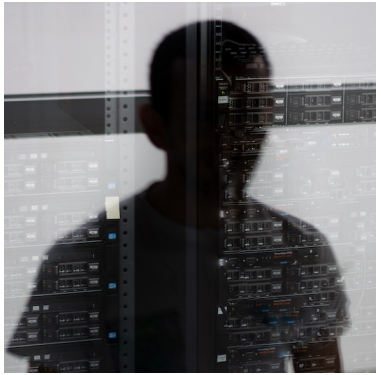
App. developer (or first party)



includes a library within the application

€

A&A company (third party)



builds and improves user profiles

develops and manages an application

Application Store

install an app.

User

the app. sends PI

targeted adv.

who's interested by a young and fashion user?

adv. +€€€

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…)

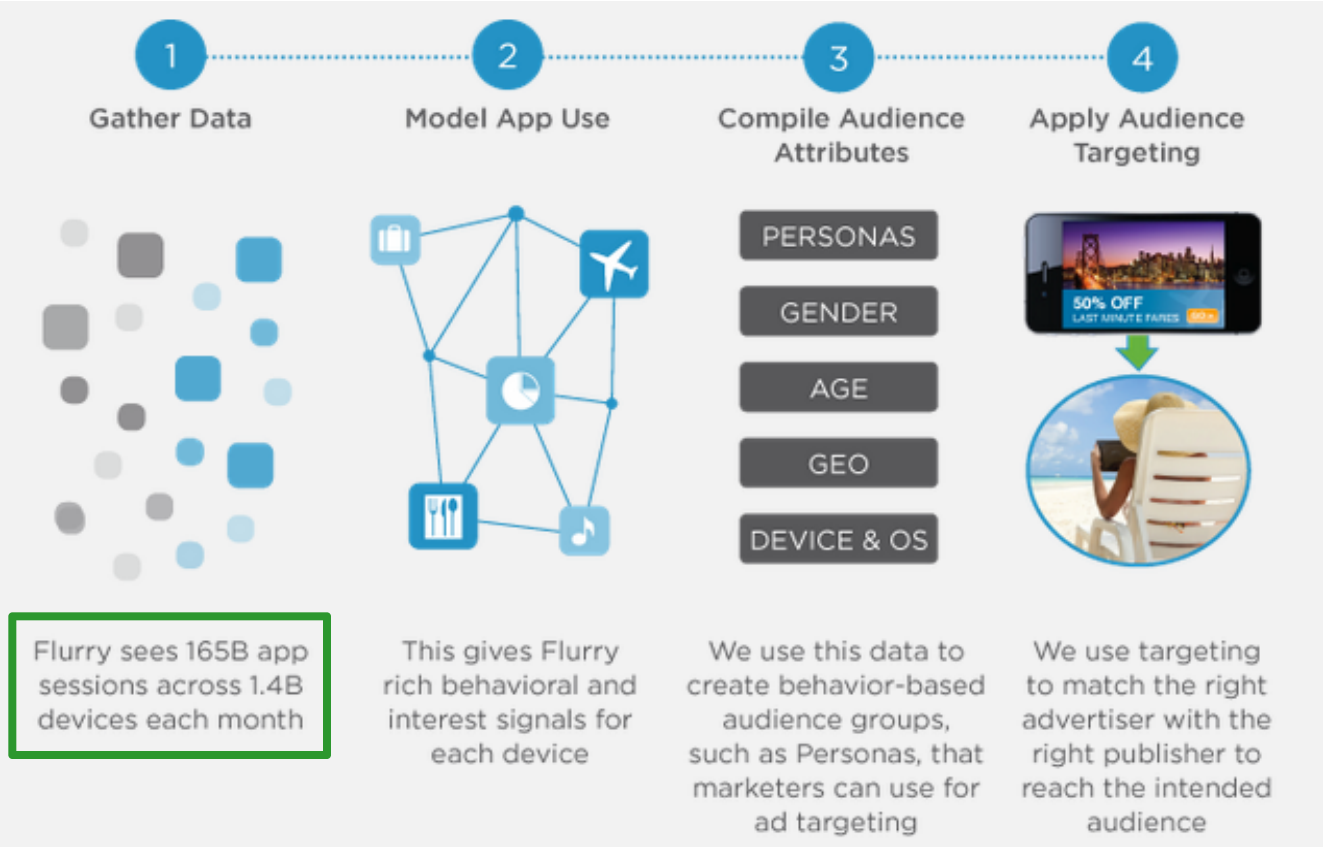
millennial media®

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!



FLURRY maintenant YAHOO! DEVELOPER NETWORK

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

Source: Flurry web site, February 2016.

… And gross revenues that are impressive too!

- **Alphabet** (owner of Google):
  - 22,7 Billion $ gross revenue for targeted advertising in April – June 2017 (3 months)
    - ✓ out of a total of 26 Billion $ of gross revenue ;
    - ✓ almost 100 Billion $ per year.

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/2017/Q2_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/

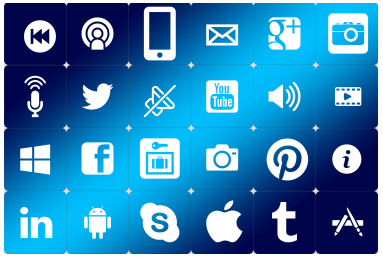
ZdNet : http://www.zdnet.fr/actualites/trimestriels-le-ca-d-alphabet-en-hausse-de-21-malgre-l-amende-de-l-ue-39855362.htm

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
- 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

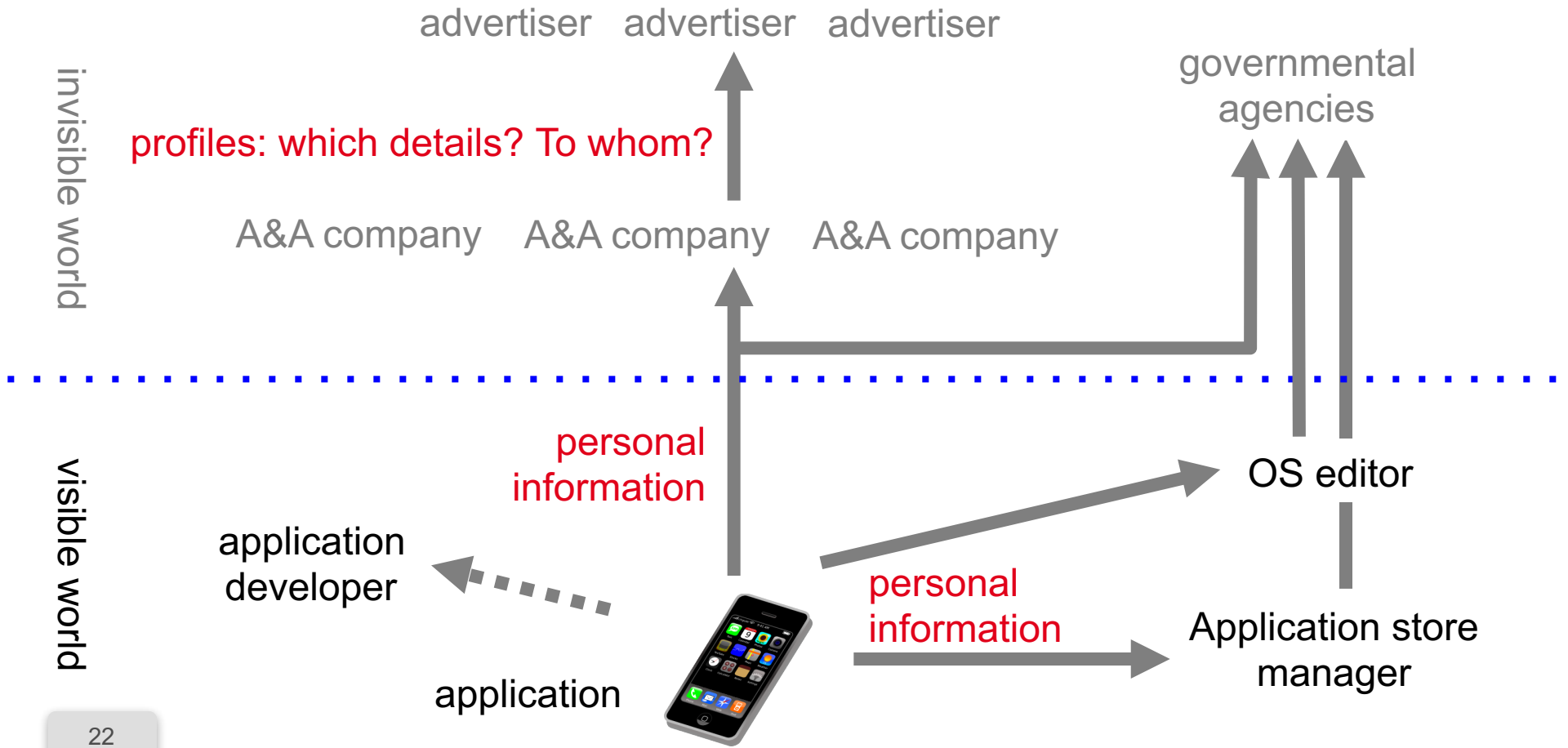
Fair business model or not?

- “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



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

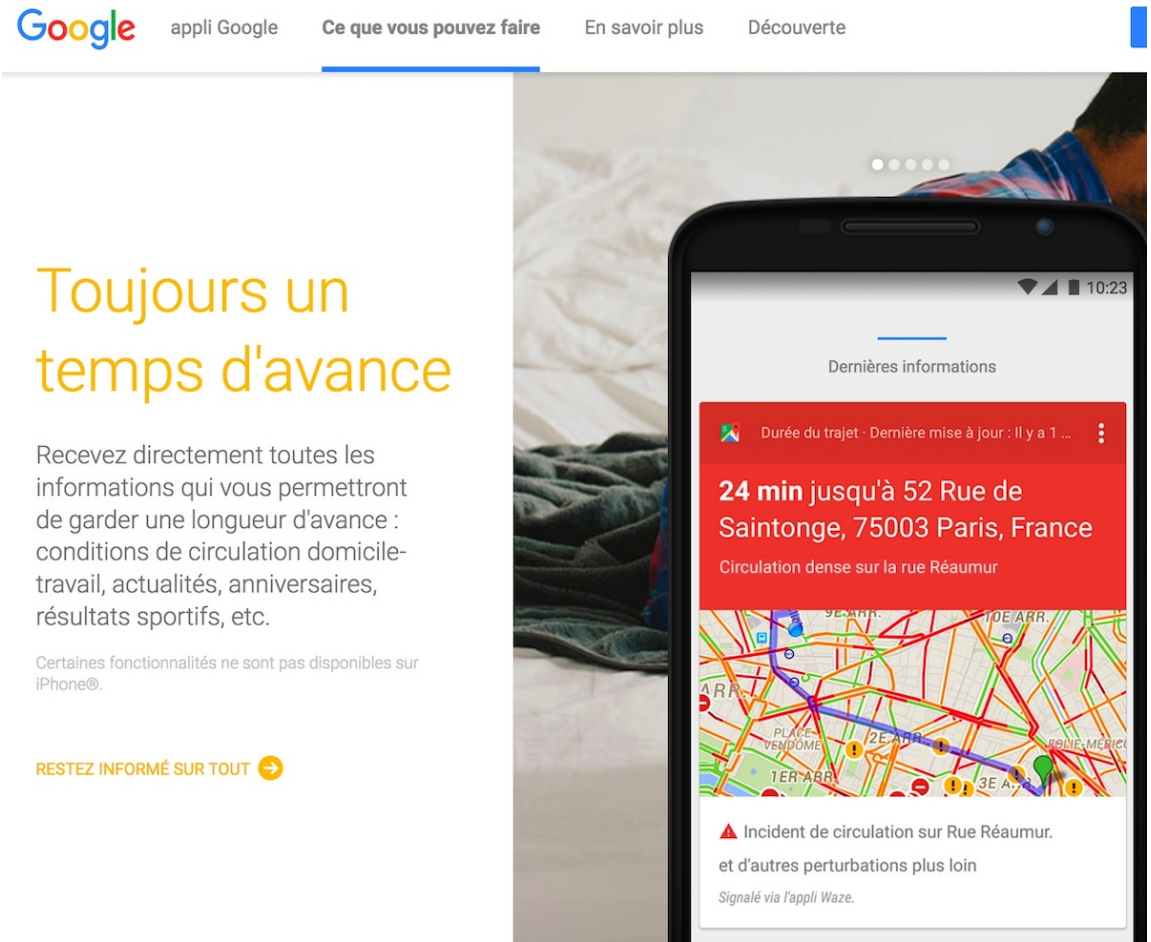
08:00 - 09:00
08:00 08:01 08:02 08:03 08:04 08:05
08:06 08:07 08:08 08:09 08:11:05
08:11:59 08:12 08:18 08:21 08:24
08:25 08:26 08:27 08:28 08:29 08:30
08:31 08:32 08:37 08:42 08:47 08:51
08:56

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)



- 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

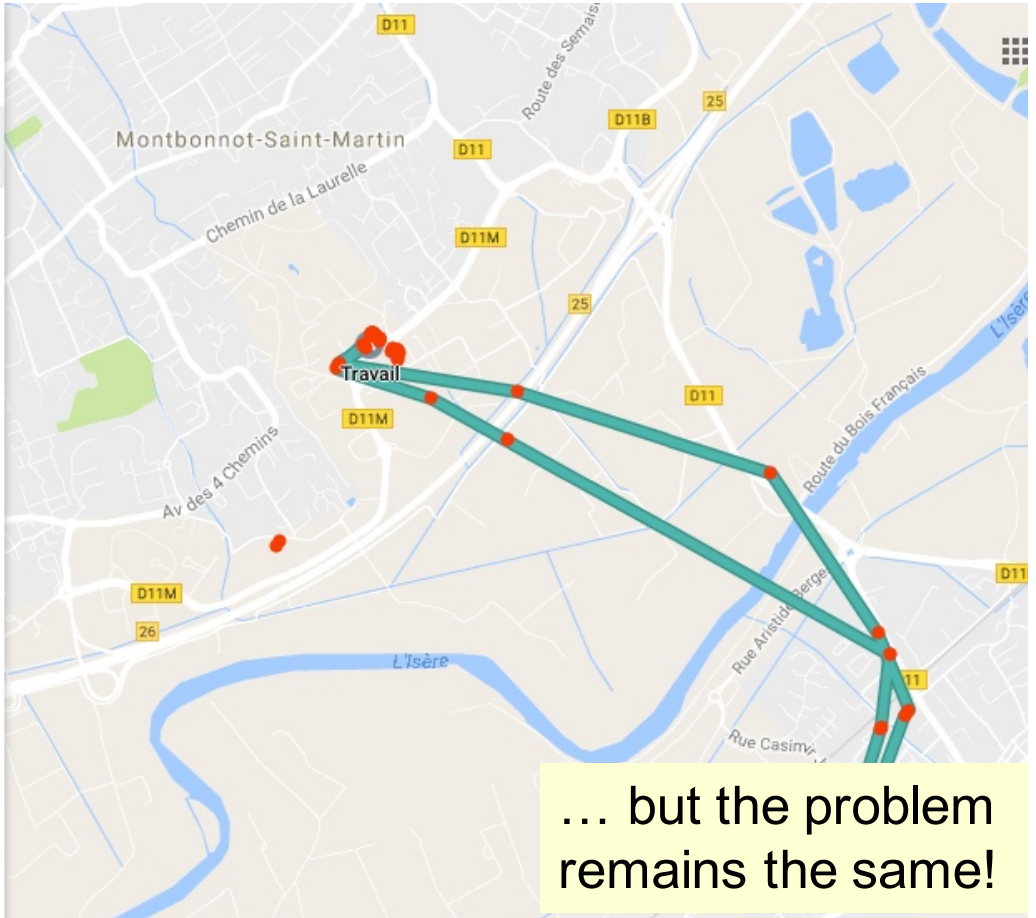
Domicile 07:55

It's less frightening…

26 min

Travail 08:21 – 18:33

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



2- A potential disproportion of data collection (5)

- Geolocation information are meaningful.
  - ✓ Google knows if I'm going to a church.
  - ✓ 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

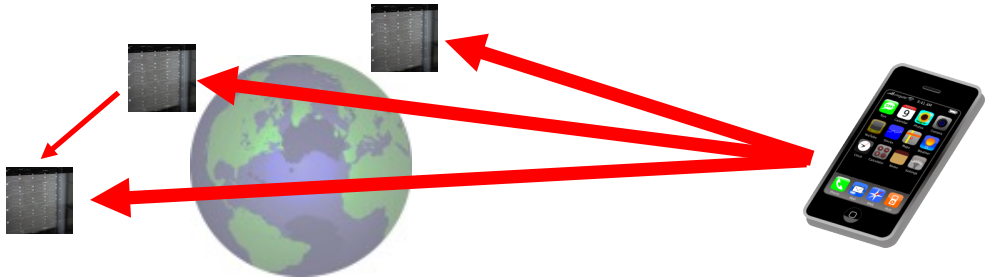
- We don’t know everything…
  - ✓ see the RATP application, 2013 version.
  - ✓ This RATP app. changed a lot since that version, but many others keep on leaking personal information without the user knowing.

- 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
  - ✓ FR and EU laws apply difficultly 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
  - ✓ wearable connected devices
  - ✓ home connected appliances
  - ✓ e.g., intelligent thermometer
  - ✓ “quantified self” trend
  - ✓ connected cars
  - ✓ 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
- 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 Wifi (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

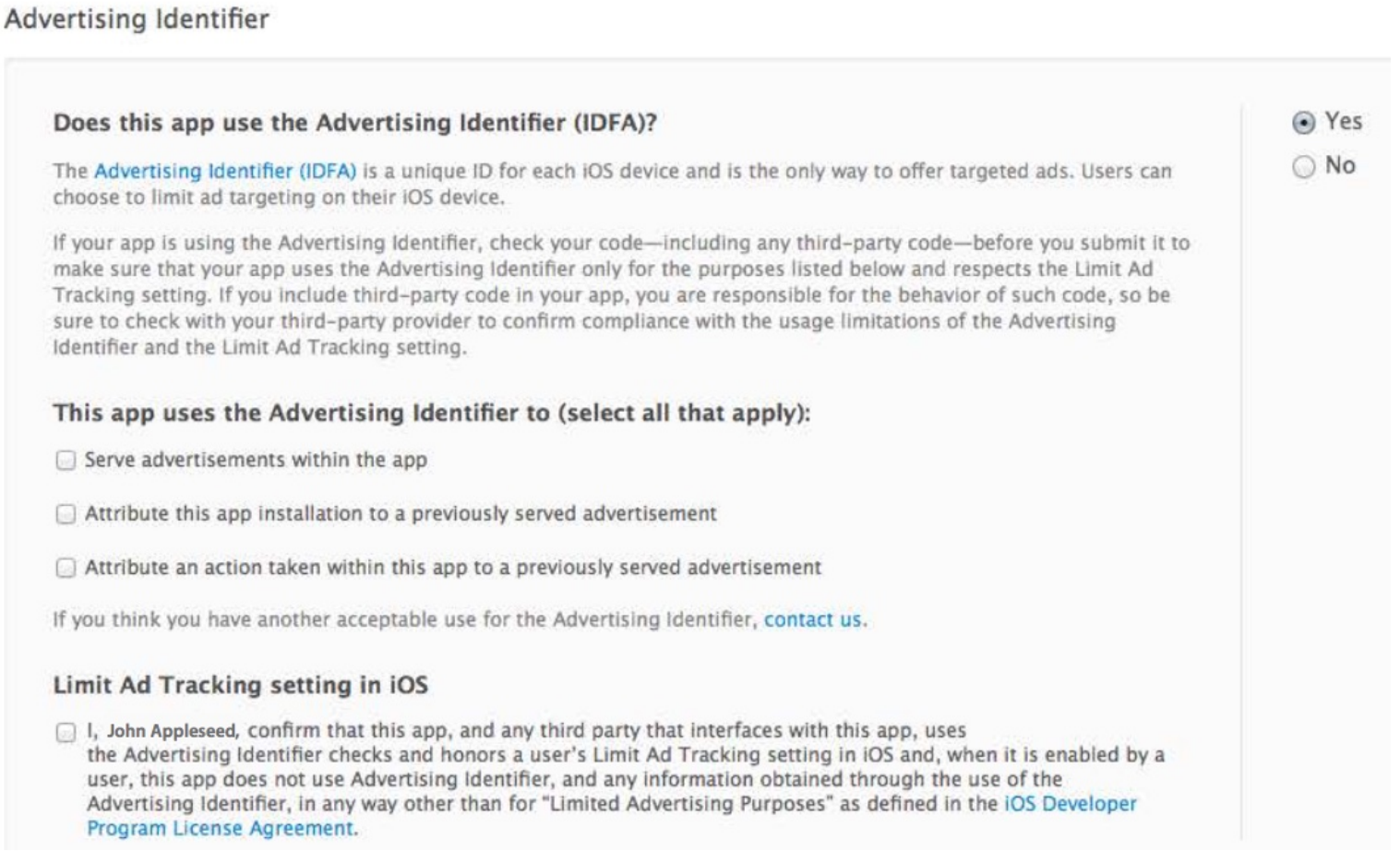
- and the AdID (Advertising Identifier)…

About the Advertising Identifier, or AdID (1)

- Quasi-unique identifier used explicitly for **targeted advertising.**
  - ✓ Historically created by Apple.
  - ✓ Recently added by Google.
  - The user can **reinitialize** the AdID at any time ☺.
  - Apple also enables the user to ask not to be tracked.

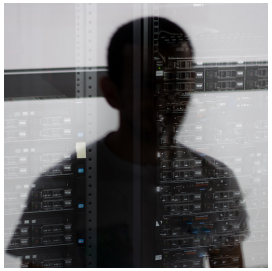
- Two benefits:
  - **Transparency**: it's designed for advertising only.
  - Gives back **control** to the user.

About the Advertising Identifier, or AdID (2)



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

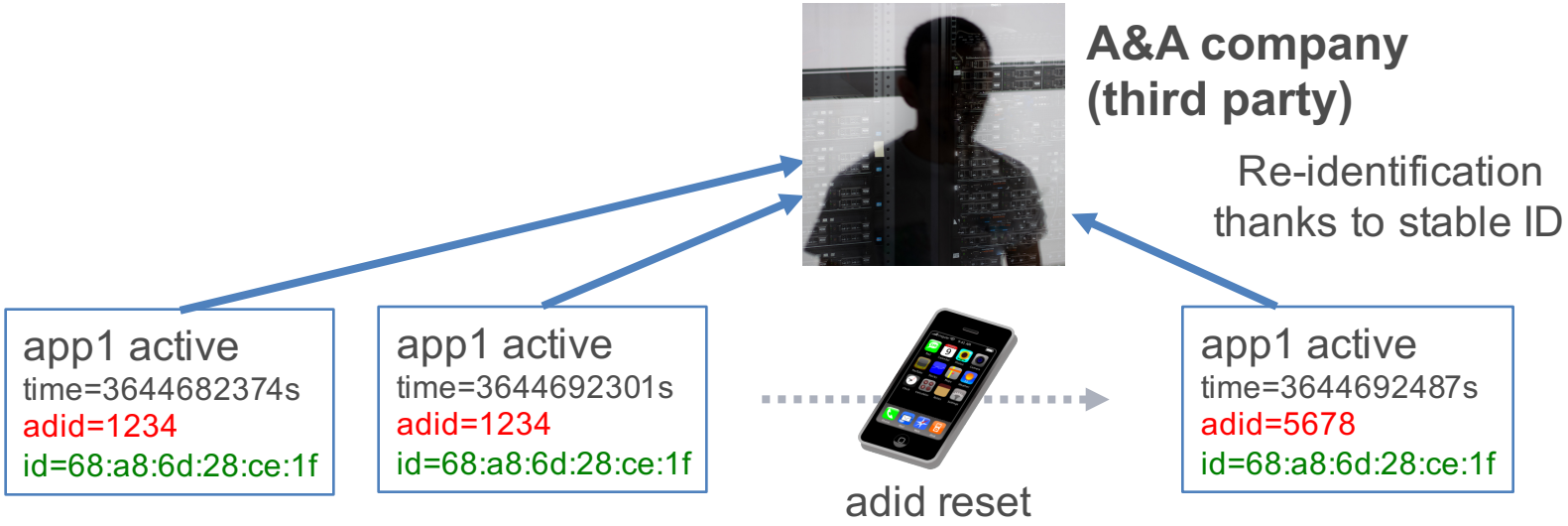
time

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!

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.



Major differences between Google - Apple

- **Google** chose not to fundamentally change the situation ☹
  - ✓ Many technical identifiers remain accessible, sometimes without the user explicit agreement
  - ✓ Google kindly asks A&A companies to use the AdID and not to cheat! https://developer.android.com/training/articles/user-data-ids.html

- **Apple** progressively banned access to stable identifiers ☺
  - ✓ The AdID is the only one authorized.
  - ✓ Greatly limits (but does not totally prevent) tracking possibilities.

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)** is a technology that brings transparency and control back to the user.
  - ✓ The user knows its purpose and can reset it at any time/.

- All of this assumes no other stable identifier be collected.
  - ✓ Apple is much more virtuous than Google from this point of view.

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
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

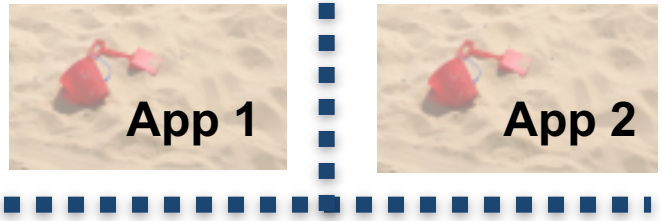
Notion of authorizations (1)

- An application can require authorizations to operate normally.
  - ✓ *Example : Internet access (transmission/reception).*
  - ✓ *Example : Contact access.*

- Goal of authorizations: get the **"free and informed consent"** of the user.
  - ✓ **"Free":** the user can refuse an authorization.
  - ✓ **"Informed":** the user knows the implications of the authorization.

  - ✓ This is an ideal that should be the goal… but it's not always 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.

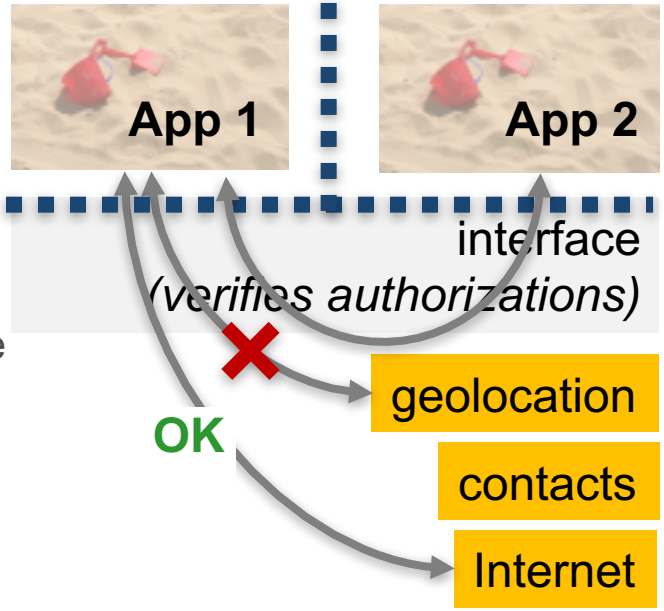
geolocation

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 priori or a posteriori authorizations?

- **Market centric:** the market owner checks the App before accepting it.
  - ✓ Checks the conformance of an application with Apple's rules.
  - ✓ Under the responsibility of Google (Play Store) et Apple (App Store).

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

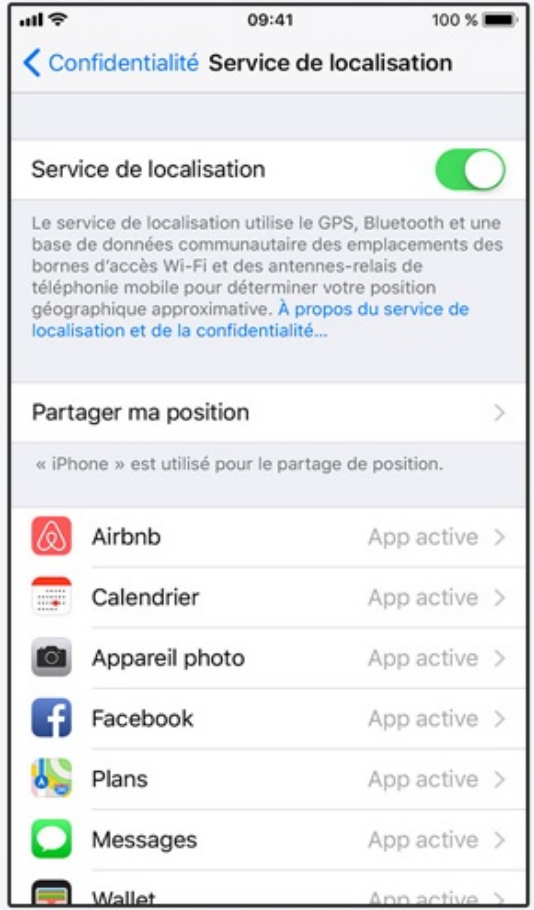
Dynamic Authorizations – iOS (1)

- 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/

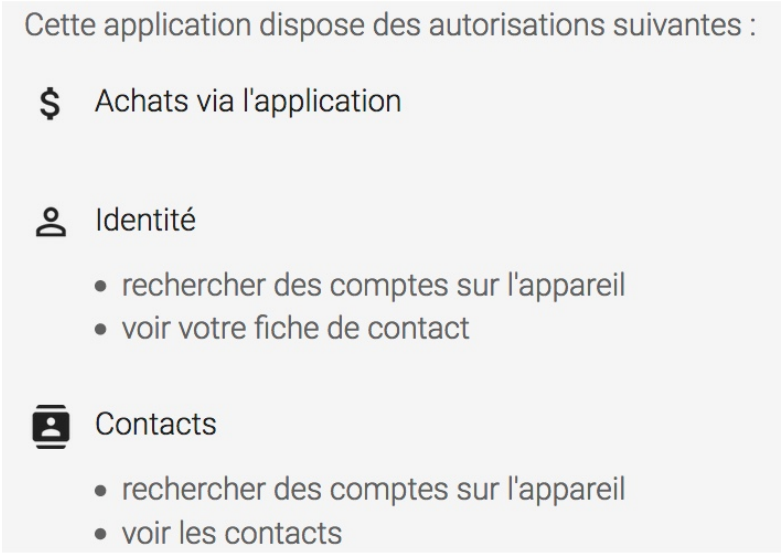
Dynamic Authorizations – iOS (2)

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



At installation time authorizations - Android

- Ask the user to grant authorizations **at installation time**.
  - ✓ The Android **“Permissions”**.
  - ✓ The only approach for Android until **Android 5.1**, and still the rule for many applications.
  - ✓ To accept all, otherwise no installation is possible.

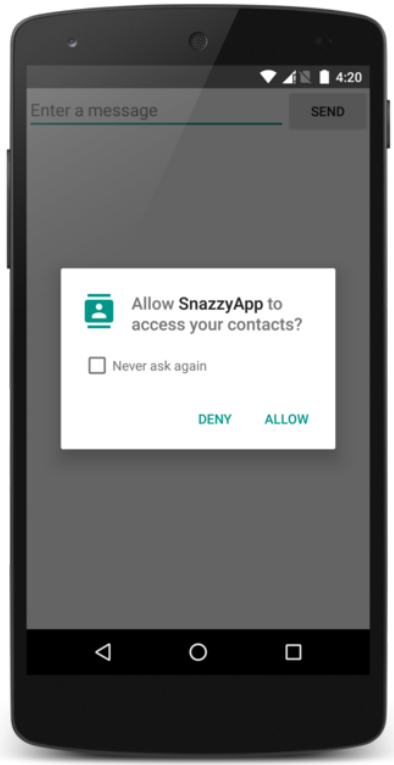


Dynamic Authorizations – Android (1)

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

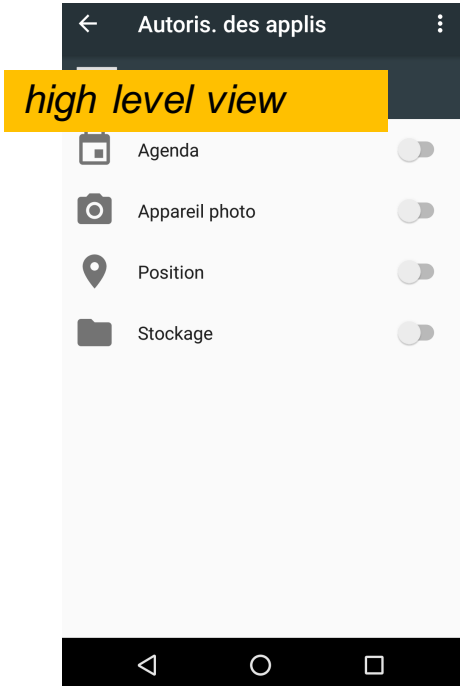
- The user has more control (idem Apple/iOS):
  - ✓ The user authorizes or refuses individually each authorization ☺.
  - ✓ The user can change his mind at any time ☺.

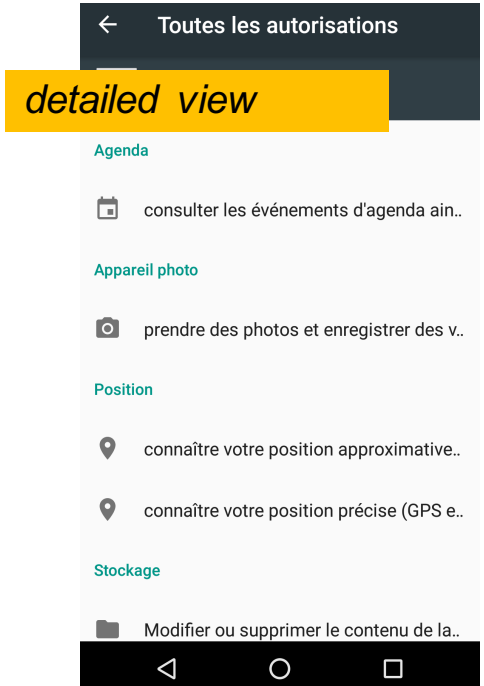
- Google talks about “fluid installation”…
  - ✓ Sure, but authorizations asked by a certain application are no longer displayed. The user needs to search them ☹.



Dynamic Authorizations – Android (2)

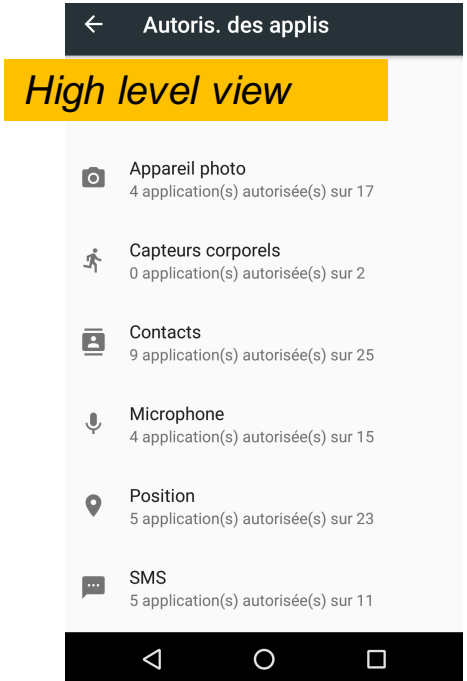
- List all authorizations **for a given application**.
  - ✓ High level view: Parameters > Applications > appli > Authorizations
  - ✓ Detailed view: “All authorizations”

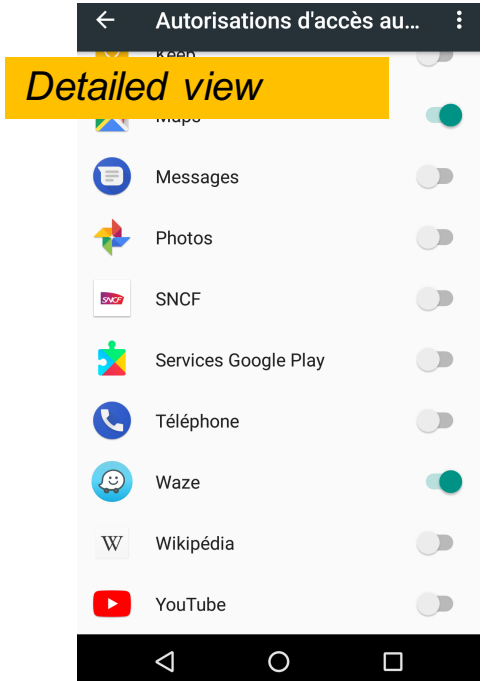




Dynamic Authorizations – Android (3)

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





In summary

- Authorizations have two goals:
  - ✓ the user can **determine the privileges** required by each application;
  - ✓ the user can **control** each application.

- Two different approaches:
  - ✓ at **installation time**: very limited;
  - ✓ and/or **dynamically**: much better control.

  - ✓ Fortunately, Android also tends to dynamic authorizations.

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**
- Two further examples: ACCESS_WIFI_STATE and physical world tracking
- Conclusion: towards a virtuous circle

Proposed authorizations approaches have limits

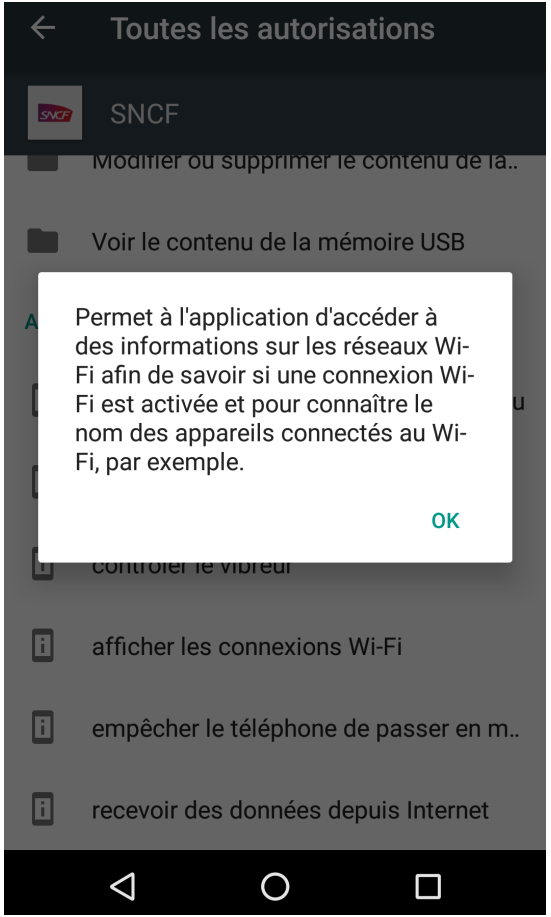
- Limits on the Android side.
- Limits on the iOS side.
- Limits common to Android and iOS :
  - ✓ lack of **behavioral** control of the application;
  - ✓ lack of control on the **composition** of authorizations.

Limits of Android authorization system (1)

- The installation based authorization system is **too basic** ☹
  - ✓ User needs to accept **all** authorizations.
  - ✓ If the user changes his mind, he has no other choice than uninstalling the application.
  - ✓ **The world is not binary, it's more complex.**
  - ✓ This approach is progressively abandoned, and users can change their mind later one with Android >= 6.

Limits of Android authorization system (2)

- The authorization system is **too complex** ☹
  - A total of **147 authorizations** (Oct. 2017).
  - The users **can not always appreciate all the implications of authorizations**…
    - ✓ … and sometimes specialists can't either!
  - Example :
    - ✓ ambiguous ("Name of connected devices"? All of them?)
    - ✓ non exhaustive list provided
    - ✓ also grants access to « *afficher les connections Wi-Fi* »
      Useful to track me but it's never said.



Limits of Android authorization system (3)

- The authorization system makes questionable assumptions.
  - ✓ Distinguishes “normal” and “dangerous” authorizations.
  - ✓ **No explicit information nor user solicitation is needed for “normal” authorizations!**
  - ✓ … it’s up to the user to go and look at all authorizations in the Play Store or in the smartphone’s Parameters.

Limits of Android authorization system (4)

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."

- 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 of Android authorization system (5)

- A simple yet strong message towards A&A companies:
  - ✓ « […] utiliser l'identifiant publicitaire […] au lieu de tout autre identifiant d'appareil pour l'ensemble des aspects publicitaires. »
- But:
  - ✓ this relies on the good will of A&A companies (access to other stable identifiers is trivial and does not necessarily require to ask the user);
  - ✓ **only concerns** targeted advertising. Are you concerned if you want to track somebody for another purpose?

https://support.google.com/googleplay/android-developer/answer/6048248?hl=fr
https://developer.android.com/training/articles/user-data-ids.html

What about iOS?

- The **advertising identifier** is the only one that can be collected…
  - ✓ … and only by applications that display targeted advertising.
  - ✓ Any other usage is strictly forbidden.

- Stable identifiers have been soon **banned**.
  - ✓ UDID : May 2013.
  - ✓ Wi-Fi MAC address: iOS7, September 2013.

Using Identifiers in Your Apps

March 21, 2013

Starting May 1, the App Store will no longer accept new apps or app updates that access UDIDs. Please update your apps and servers to associate users with the Vendor or Advertising identifiers introduced in iOS 6. You can find more details in the UIDevice Class Reference.

Limits common to Android and iOS (1)

- No **behavioral control** of the application ☹

  - ✓ 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)!

Limits common to Android and iOS (2)

- 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**.
  - ✓ A deliberate choice of Apple to favor privacy in his commercial offer.
  - ✓ Visible in iOS for long.

- 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
- **Two further examples: ACCESS_WIFI_STATE and physical world tracking**
- Conclusion: towards a virtuous circle

ACCESS_WIFI_STATE: an Android authorization with unexpected implications (1)

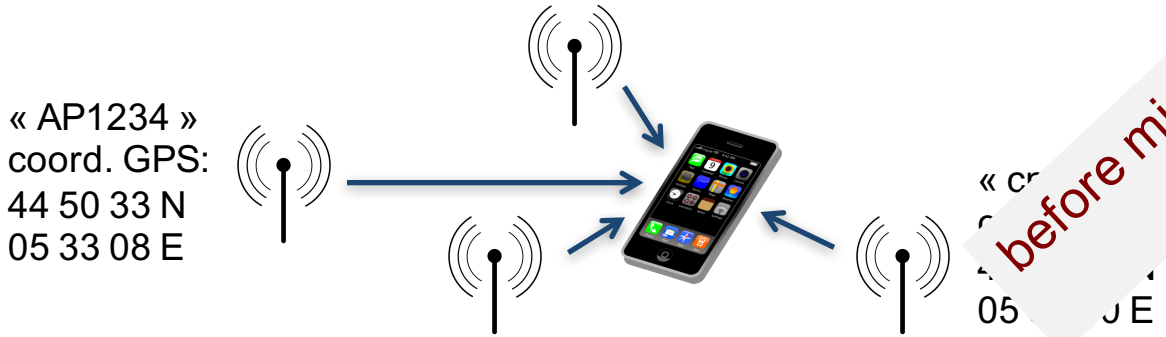
- Imagine an App, that without asking the user explicit authorization

- … can **track** the user thanks to a stable identifier.
  - ✓ it's the Wifi MAC address
  - ✓ e.g., 68:a8:6d:28:ce:1f
  - ✓ guaranteed to be unique in the world
  - ✓ impossible to re-initialize

ACCESS_WIFI_STATE: an Android authorization with unexpected implications (2)

- Imagine an App, that without asking the user explicit authorization…

- … knows your **location**.
  - ✓ Listen to Wi-Fi networks in range, then thanks to a broad database giving the geolocation of all AP can locate the smartphone by triangulation
  - ✓ in urban environments, can be very accurate



before mid-2016 (things have changed since)

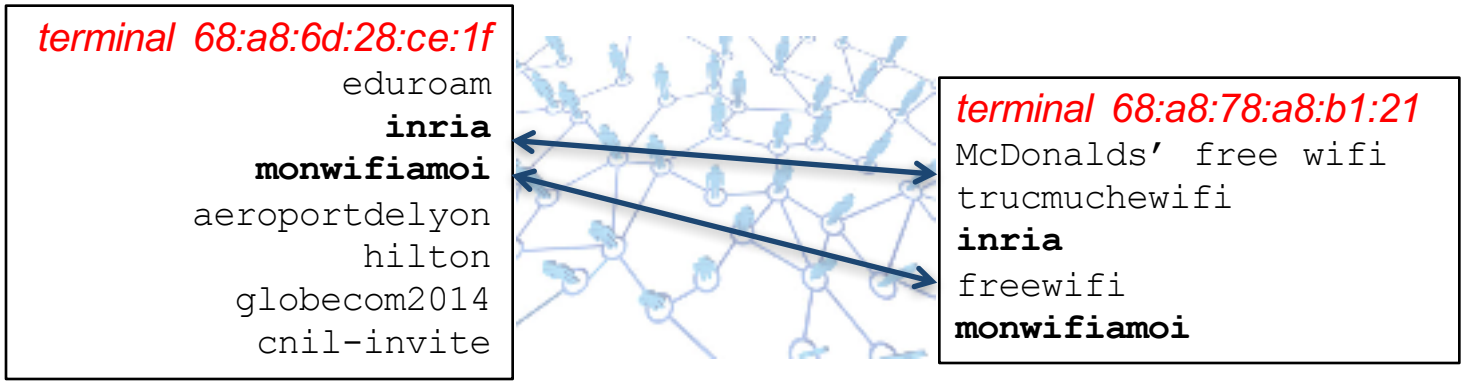
ACCESS_WIFI_STATE: an Android authorization with unexpected implications (3)

- Imagine an App, that without asking the user explicit authorization…
- … knows a part of your **travels history** and your **profile**.
  - ✓ via the list of Wifi AP to which you connected, which is automatically registered in your smartphone

terminal 68:a8:6d:28:ce:1f
```
eduroam
Inria
monwifiamoi
aeroportdelyon
hilton
globecom2014
cnil-invite
```

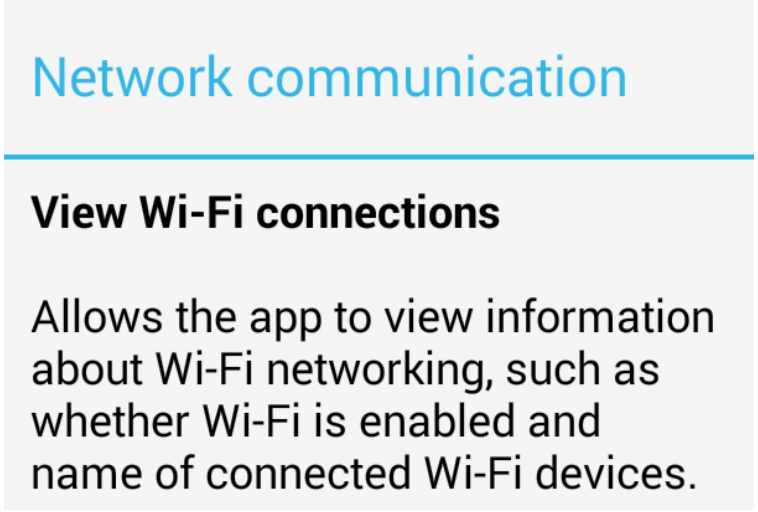
ACCESS_WIFI_STATE: an Android authorization with unexpected implications (4)

- Imagine an App, that without asking the user explicit authorization…
- … can infer **social links** between users.
  - ✓ by calculating the distance between their Wi-Fi connection list, after creating a large dedicated database



ACCESS_WIFI_STATE: an Android authorization with unexpected implications (5)

- **Till 2016**, it was sufficient to request the **ACCESS_WIFI_STATE** and **INTERNET** authorizations…
  - ✓ No user could imagine this is possible.
  - ✓ And the authorization descriptions gives no clue…



ACCESS_WIFI_STATE: is it in use?

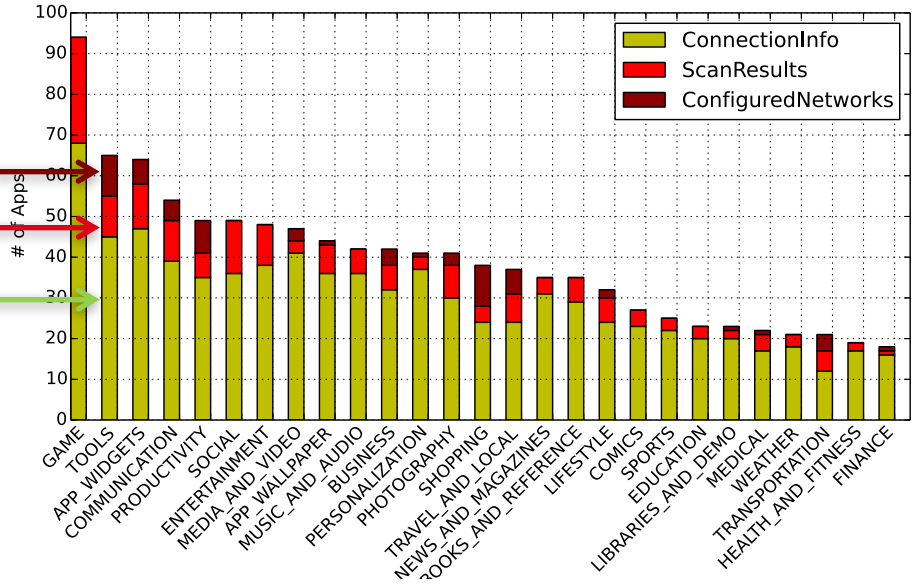
- Yes… In 2014, out of the 2700 most popular Apps, 41% ask both permissions and many of them use them.

number of applications concerned

wifi connection list

in rage Wifi AP list

Wifi address + other info



Application types in Play Store

J. Achara, M. Cunche, V. Roca, A. Francillon, **"Short paper: WifiLeaks: Underestimated Privacy Implications of the ACCESS WIFI STATE Android Permission"**, IEEE WiSec'14, juillet 2014. http://hal.inria.fr/hal-00997716/en/

ACCESS_WIFI_STATE: two outcomes (1)

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Co

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE

News & Events » Press Releases » Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions c

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

FOR RELEASE

June 22, 2016

our work triggered this enquiry ☺

ACCESS_WIFI_STATE: two outcomes (2)

- mid-2016 Google changed the ACCESS_WIFI_STATE authorization
  - ✓ listening to Wi-Fi network is now protected by the "geolocation" permission

Did our work triggered this enquiry? No confirmation.

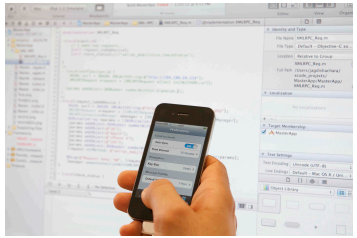
Outline

- 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
- 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!**
  - ✓ Major 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

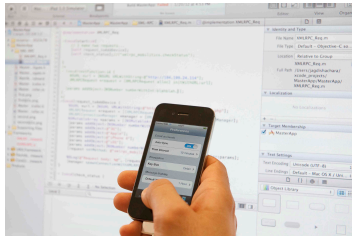
Users

anonymized user profile

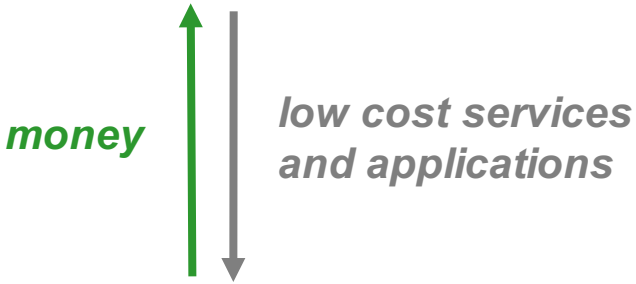
A&A company

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

Virtuous Circle: the paying model



Application developer



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.

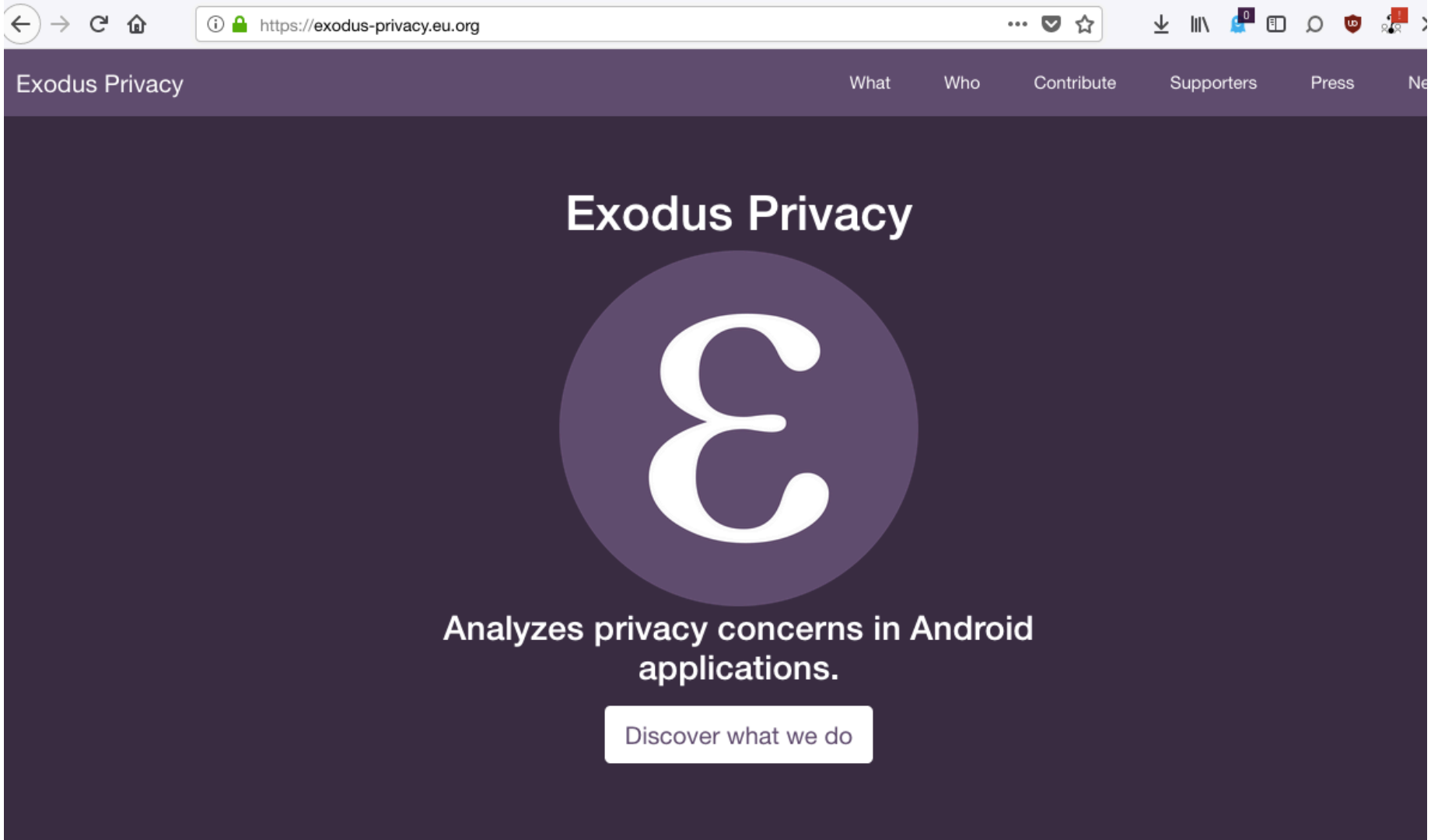
An utopia?

- 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.**

TOOLS TO CHECK YOUR APPS


https://exodus-privacy.eu.org
Exodus Privacy
What
Who
Contribute
Supporters
Press
Exodus Privacy
Analyzes privacy concerns in Android applications.
Discover what we do

https://recon.meddle.mobi

ReCon | Home | About | Reports | Code and Data | Contact | Meddle (parent project)

USING RECON

- Android Install
- iOS Install
- Tutorial
- FAQ

DETAILS

- Overview
- Technical details

CASE STUDIES

- Panoptispy
- App Versions
- App vs Web
- Pokemon Go

Are you already using ReCon? If so, check out the ReCon Monitoring and Configuration page.

Why run ReCon?

Have you ever wondered who or what is tracking you and/or stealing your personal information? Unfortunately, your mobile devices currently give you little or no way to tell if this is the case. Even if they did, they don't give you any way to control it except to decline to install an app. With ReCon, we give you a way to see how your personal information is transmitted to other parties, and allow you to block or modify it with fine granularity. A demo is shown in the video and you can learn more details in this tutorial.

Jingjing Ren, David Choffnes,
Northeastern University
Ashwin Rao, University of Helsinki
Martina Lindorfer, SBA Research

Google Play

Search

Apps

Categories

Home

Top Charts

New Releases

My apps

Shop

Games

Family

Editors' Choice

Account

My subscriptions

Redeem

Buy gift card

My wishlist

My Play activity

Parent Guide

Lumen Privacy Monitor

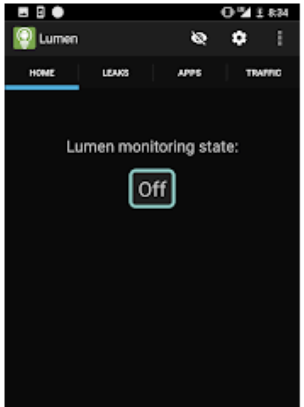
Int. Computer Science Institute-UC Berkeley Tools

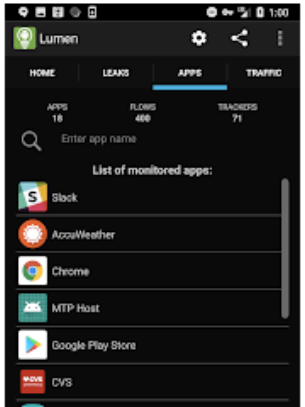
127

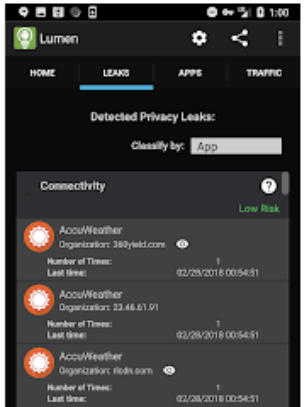
PEGI 3

Add to Wishlist

Install







Thank you… ☺

vincent.roca@inria.fr