



# The Mobilitics Inria-CNIL project: privacy and smartphones

*Claude Castelluccia*

*[Claude.castelluccia@inria.fr](mailto:Claude.castelluccia@inria.fr)*

*June 2013*

# ***DATAVEILLANCE = DATA + SURVEILLANCE***

- **Systematic** monitoring of people's actions or communications through the application of information technology.
- We leak data, leave traces when we are browsing the web or using our smart phone...
  - On the **visible** web
  - On the **invisible** web
- For economical or security reasons

# ***Dataveillance on the « Visible » Web***

- Foursquare knows **where you are**
- Flickr knows **what you see**
- Facebook knows **what you do**
- LinkedIn knows **what you've done**
- Twitter knows **what you say**
- Amazon knows **what you buy**
- Google knows **what you think**

*\*Courtesy of F. Bancihlon*

# Dataveillance on the “Invisible” Web

- “Meta-data”
- Tags, Web bugs, pixels and beacons that appear on Websites to track and profile users
- Allows trackers to build profiles of users



The screenshot shows a web browser displaying the New York Times homepage. A Ghostery extension is active, showing a notification that 7 trackers were found. The extension's interface is overlaid on the right side of the page, listing the following trackers with their categories and status (on/off):

- Facebook Connect (Widget) - On
- Google-AdSense (Advertising) - On
- Krux Digital (Tracker) - On
- New York Times (Tracker) - Off
- Typekit by Adobe (Widget) - Off
- WebTrends (Tracker) - On

At the bottom of the extension interface, there are buttons for "Pause Blocking", "Whitelist Site", and a help icon. The background shows the New York Times website with a main article titled "Justices Allow Police to Take D.N.A. Samples After Arrests" and a sidebar with various news categories.

# Dataveillance on the “Invisible” Web



The screenshot shows the Ghostery browser extension interface. At the top, a blue banner displays the Ghostery logo (a blue smiley face), the text "Ghostery found 3 trackers", and the URL "cfspart.impots.gouv.fr". A gear icon for settings is in the top right of the banner. Below the banner, three trackers are listed, each with a chevron icon on the left, the tracker name, a sub-label, and a toggle switch with a red 'X' icon and a circular icon with a checkmark on the right.

Tracker Name	Sub-label	Toggle Status
AT-Internet	Analytics	Off
Facebook-Connect	Widget	Off
Twitter-Button	Widget	Off

# A Example of Abuse: NSA PRISM



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection  
(Surveillance and Stored Comms)?  
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:  
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

# TRACKING THE TRACKERS

- It is important to understand how much info are collected about us and by whom?
- « tracking the trackers » projects
- Imho this is an **important task (even duty)** of a **public** research institute like Inria
- The main motivation of the Cnil-Inria **Mobilitics** projects:  
understand how much and how data is leaked by our smartphones!

# *Cnil-Inria Convention*

- Signée début 2012
- 2 objectifs principaux
  - Sensibiliser les chercheurs à la problématique “protection de la vie privée” + aider à définir un cadre légal
  - Apporter une expertise scientifique et technique a la CNIL (nouveau service “des études, de l'innovation et de la prospective” de la Cnil).



# MOBILITICS

- Why smartphones?
  - smartphones have become our companions
    - useful and user-friendly, always connected
    - easy to customize to match everybody expectations
    - ~20% of mobile phones are smartphones

but smartphones know a lot of our cyber-activities

- they **gather** private information
  - while we're using them
- they **generate** private information
  - GPS, NFC, WiFi, camera

**Apps/OS servers (first party)**



**May send personal information to**

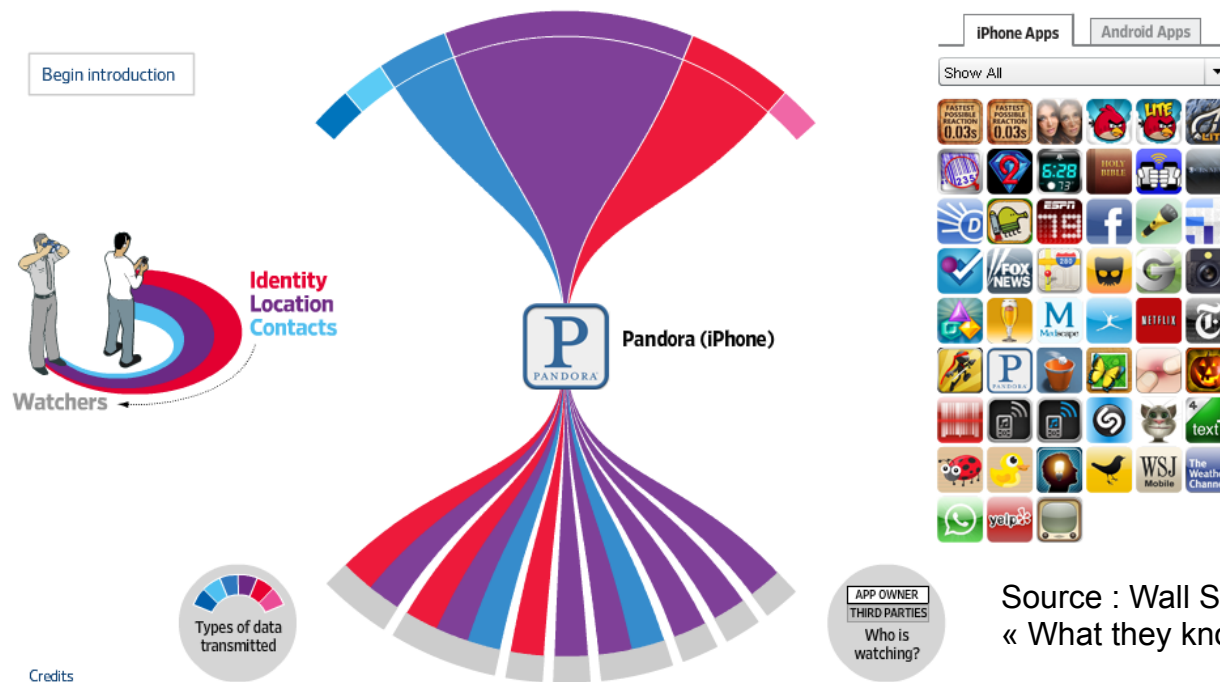


**Can access personal information (location, contacts, device name, photos, notes, etc.)**



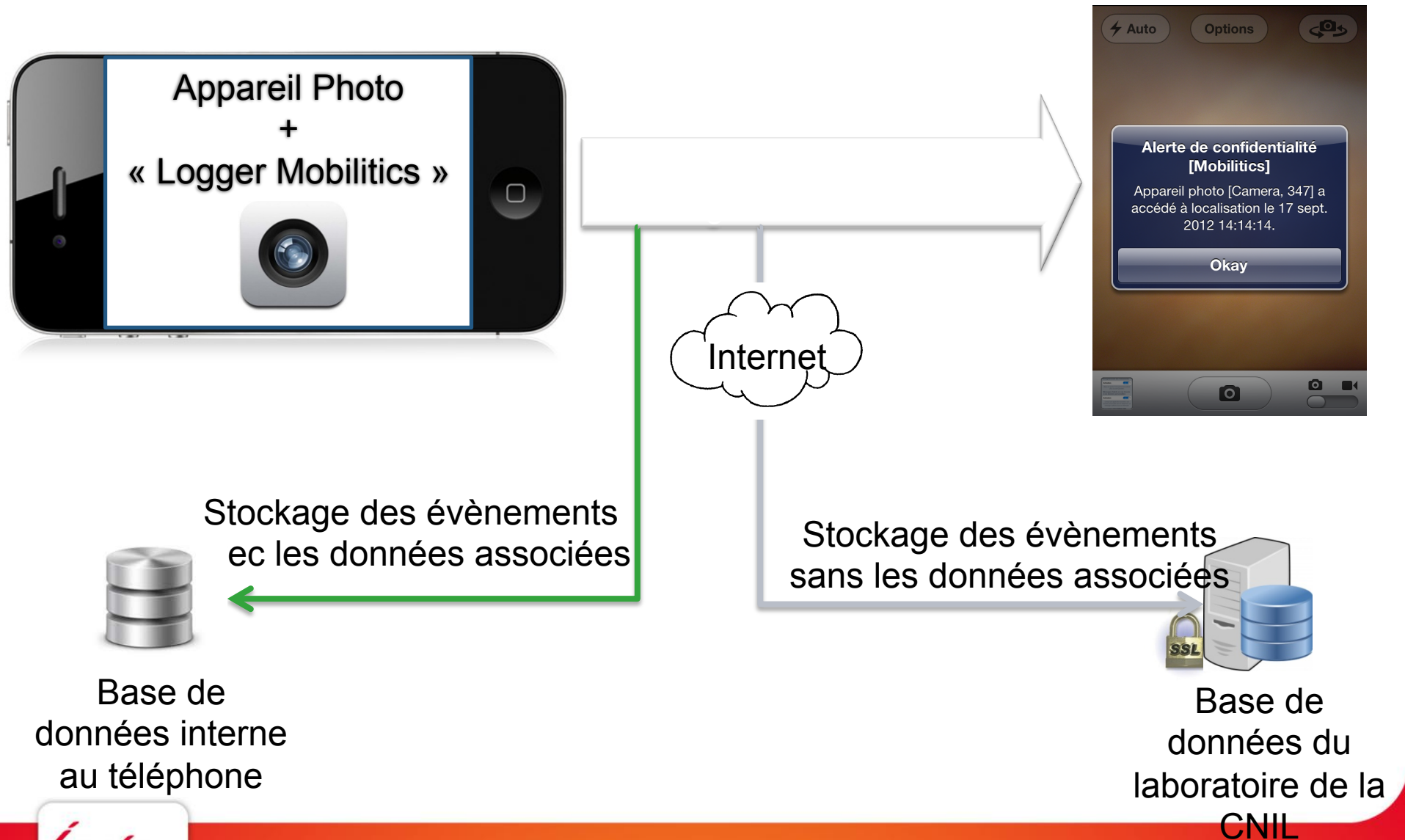
# Objectif de MOBILITICS

- De nombreuses études "in vitro"



➔ Mobilitics complète ses résultats par des éléments "in vivo »

# Comment Ca Marche?



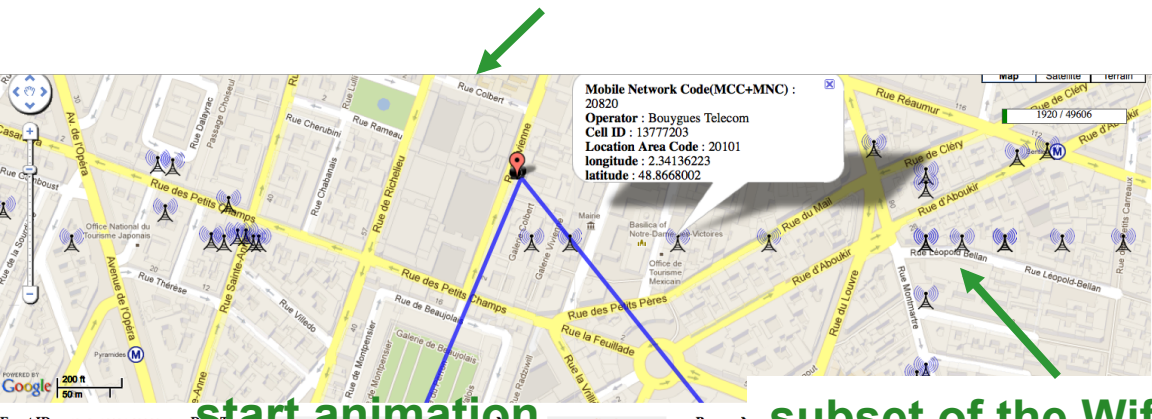
# Data being collected

we capture

- Access to personal data
  - contacts
  - geographic location
  - various device and user accounts
  - calendar
  - photos and videos
  - UDID and device name
  - voice memos, etc.
- Various user related activities and events
  - phone calls and incoming calls
  - sending and receiving SMS, iMessage or emails
  - Internet navigation using safari/youtube apps
  - taking a picture, etc.

# Mobilitics, c'est aussi des outils de Visualisation!

map showing phone location and movements for that day

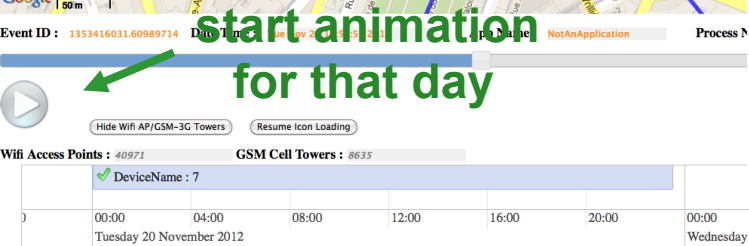


current events

Other Events happening during Geolocation (Before, Between and After)

Event ID	Date Time	App Name	Process Name	Event Type
1353416031.60989714	Tue Nov 20 13:53:51 2012	NotAnApplication	SpringBoard	LocationRetrievedThroughDelegate
1353416031.45530510	Tue Nov 20 13:53:51 2012	Téléphone	MobilePhone	BSDSockets_read
1353416031.45094109	Tue Nov 20 13:53:51 2012	NotAnApplication	locationd	BSDSockets_write
1353416031.39290905	Tue Nov 20 13:53:51 2012	NotAnApplication	dataaccessd	AccountsAccess

Showing 1 to 4 of 4 entries



subset of the Wifi AP and GSM/3G towers collected automatically

time line (lists all the days of the field test to select the one of interest)

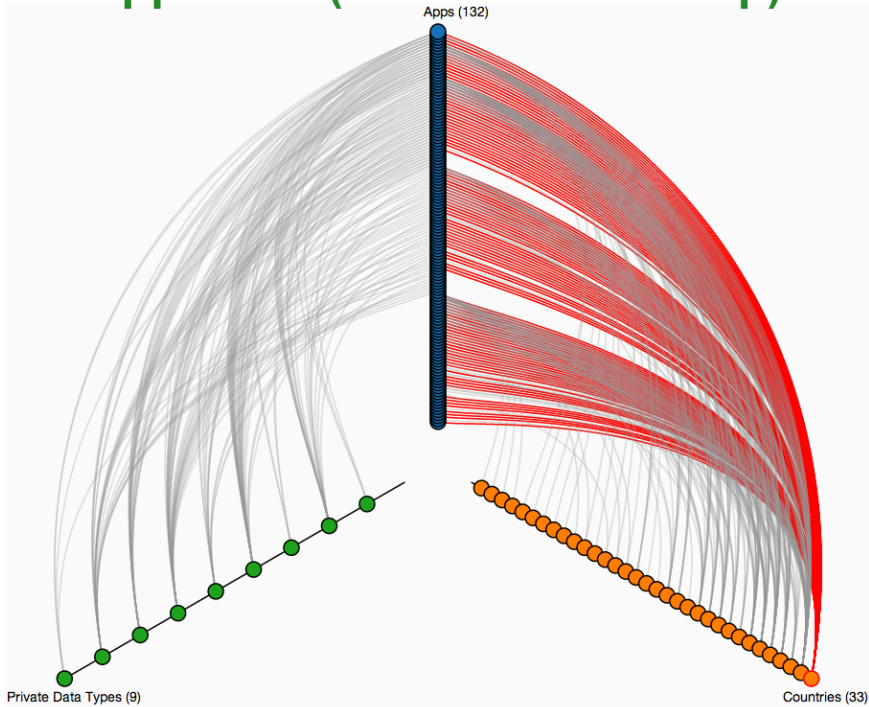
Event ID	Date Time	App Name	Process Name	Type
1353366000.38906407	Tue Nov 20 00:00:00 2012	NotAnApplication	SpringBoard	CalendarEvents
1353366000.41469002	Tue Nov 20 00:00:00 2012	NotAnApplication	SpringBoard	CalendarEvents
135337937.10008693	Tue Nov 20 03:18:57 2012	NotAnApplication	mobiliticslogcollector	DeviceName
135339794.96525097	Tue Nov 20 07:59:54 2012	NotAnApplication	SpringBoard	AppleAccountAccess
135339476.29934406	Tue Nov 20 07:59:56 2012	NotAnApplication	SpringBoard	CalendarEvents
1353394796.11381202	Tue Nov 20 07:59:56 2012	NotAnApplication	SpringBoard	CalendarEvents

show global stats

DB entries for that day (here sorted by their event time)

# Visualization per Country

## Apps axis (most active on top)



## Private data axis

## Country axis (most active on the right)

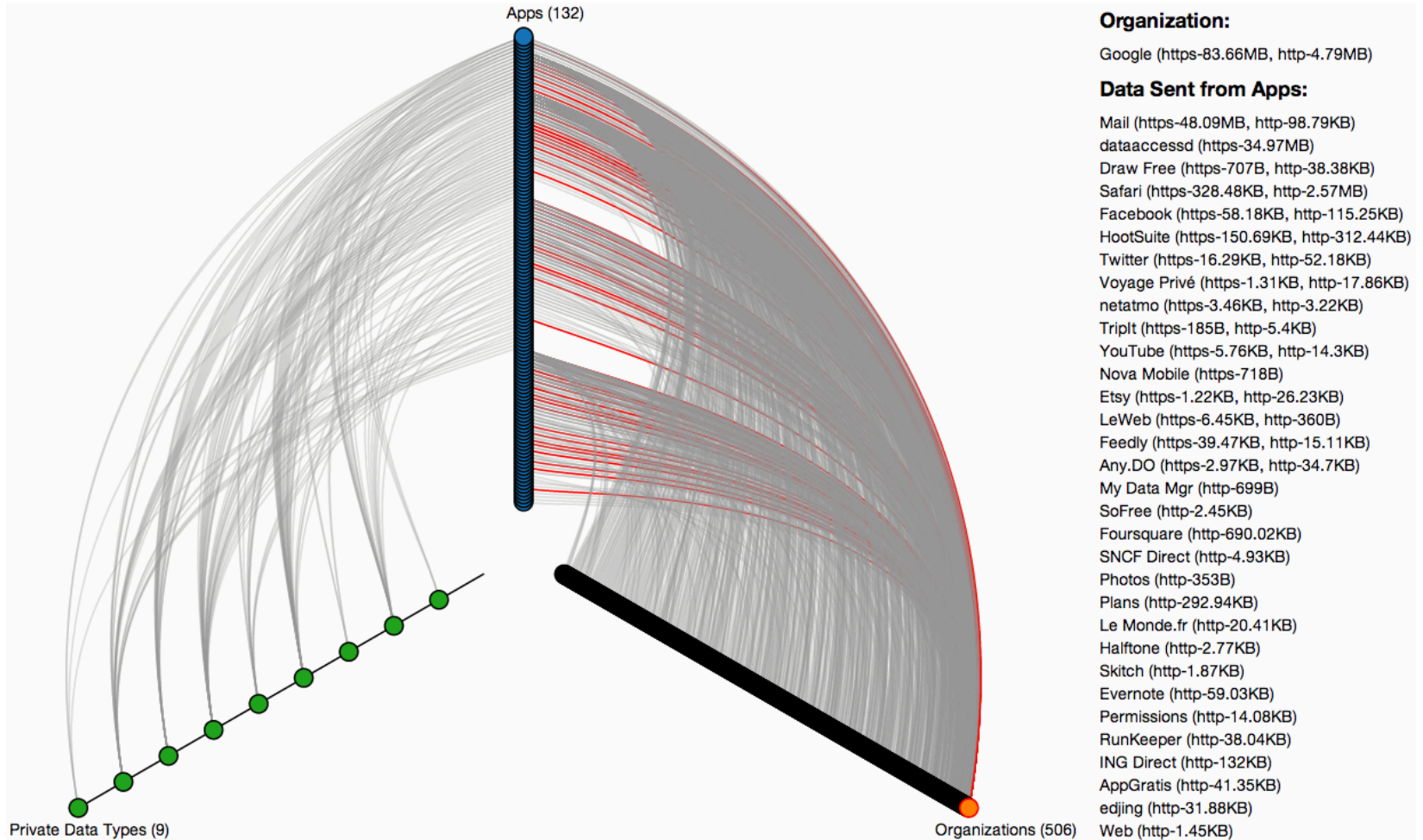
### Country:

United States (5122-4.27KB, 5223-6.23MB, 13392-3.23KB, 33033-2.42KB, 40002-275B, 40003-165B, 40004-203B, 40005-539B, 40006-73B, 40007-344B, 40010-80B, 40011-363B, 40012-1.29KB, 40013-3.28KB, 40014-176B, 40016-9.99KB, 40017-450B, 40019-233B, 40020-458B, 40021-71B, 40022-290B, 40023-12.42KB, 40024-110B, 40025-145B, 40026-122B, 40027-409B, 40028-4.19KB, 40029-285B, 40030-516B, 40031-1.84KB, 40032-1.94KB, 40033-290B, 40034-10.6KB, 40036-2KB, 40038-1.72KB, 40039-175B, 40040-423B, 40041-129B, 40042-285B, 40043-1.16KB, 40044-1.6KB, 40046-169B, 40047-354B, 52775-205B, https-144.74MB, http-25.05MB, http-alt-593B, jabber-client-182B)

### Data Sent from Apps:

Urban Pulse (5122-4.27KB, http-8.97KB)  
apsd (5223-6.23MB, https-513.08KB)  
Skype (13392-3.23KB, 33033-2.42KB, 40002-275B, 40003-165B, 40004-203B, 40005-539B, 40006-73B, 40007-344B, 40010-80B, 40011-363B, 40012-1.29KB, 40013-3.28KB, 40014-176B, 40016-9.99KB, 40017-450B, 40019-233B, 40020-458B, 40021-71B, 40022-290B, 40023-12.42KB, 40024-110B, 40025-145B, 40026-122B, 40027-409B, 40028-4.19KB, 40029-285B, 40030-516B, 40031-1.84KB, 40032-1.94KB, 40033-290B, 40034-10.6KB, 40036-2KB, 40038-1.72KB, 40039-175B, 40040-423B, 40041-129B, 40042-285B, 40043-1.16KB, 40044-1.6KB, 40046-169B, 40047-354B, 52775-205B, https-186.86KB, http-1.81KB)  
ubd (https-355.88KB)  
backupd (https-21.54KB)  
SpringBoard (https-6.77KB, http-749.92KB)  
Mail (https-48.55MB, http-1.08MB)  
aosnotifyd (https-368.27KB)  
PMP (https-14.48MB)  
itunesstored (https-3.28MB, http-419KB)  
dataaccessed (https-40.88MB, http-154.08KB)  
My Data Mgr (https-5.88KB, http-699B)  
12 jours (https-2.17KB)  
Météo (https-185B, http-32.03KB)  
syncdefaultsd (https-280.33KB)  
Draw Free (https-211.83KB, http-1003.84KB)  
configd (https-10.97KB, http-4.35KB)  
locationd (https-2.51MB)  
Shazam (https-17.06KB, http-37.16KB)  
Réglages (https-17.69KB)  
imagent (https-990.3KB, http-30.3KB)  
Safari (https-1.54MB, http-6.7MB)  
Facebook (https-9.99MB, http-801.14KB, http-alt-593B)  
HootSuite (https-4.75MB, http-3.19MB)  
- (https-1.01MB, http-898.57KB)  
0.46KB)  
92.94KB)  
http-17.86KB)  
p-241.46KB)  
1.87KB)  
Apple Store (https-15.13KB, http-3.15KB)  
RATP (https-9.1KB, http-18.65KB)  
Yammer (https-64.11KB)  
Evernote (https-5.89MB, http-82.49KB)  
Résultats foot (https-750B)  
Instagram (https-82.36KB, http-5.08MB)  
SoundCloud (https-837.38KB, http-637.85KB)  
netatmo (https-3.46KB, http-3.22KB)  
RunKeeper (https-444.41KB, http-38.4KB)  
iTunes (https-29.85KB, http-7.6KB)  
vente-privee (https-71.58KB, http-624B)  
Shopwise (https-122.09KB, http-34.35KB)  
Triplt (https-30.1KB, http-98.19KB)  
L'CEil by LaSer (https-7.13KB, http-308B)

# Visualization per Organization



## Organization:

Google (<https>-83.66MB, <http>-4.79MB)

## Data Sent from Apps:

Mail (<https>-48.09MB, <http>-98.79KB)

dataaccesssd (<https>-34.97MB)

Draw Free (<https>-707B, <http>-38.38KB)

Safari (<https>-328.48KB, <http>-2.57MB)

Facebook (<https>-58.18KB, <http>-115.25KB)

HootSuite (<https>-150.69KB, <http>-312.44KB)

Twitter (<https>-16.29KB, <http>-52.18KB)

Voyage Privé (<https>-1.31KB, <http>-17.86KB)

netatmo (<https>-3.46KB, <http>-3.22KB)

Triplt (<https>-185B, <http>-5.4KB)

YouTube (<https>-5.76KB, <http>-14.3KB)

Nova Mobile (<https>-718B)

Etsy (<https>-1.22KB, <http>-26.23KB)

LeWeb (<https>-6.45KB, <http>-360B)

Feedly (<https>-39.47KB, <http>-15.11KB)

Any.DO (<https>-2.97KB, <http>-34.7KB)

My Data Mgr (<http>-699B)

SoFree (<http>-2.45KB)

Foursquare (<http>-690.02KB)

SNCF Direct (<http>-4.93KB)

Photos (<http>-353B)

Plans (<http>-292.94KB)

Le Monde.fr (<http>-20.41KB)

Halftone (<http>-2.77KB)

Skitch (<http>-1.87KB)

Evernote (<http>-59.03KB)

Permissions (<http>-14.08KB)

RunKeeper (<http>-38.04KB)

ING Direct (<http>-132KB)

AppGratis (<http>-41.35KB)

edjing (<http>-31.88KB)

Web (<http>-1.45KB)

Paf le Chien + (<http>-10.3KB)

MyLittleParis (<http>-13.76KB)

McDo France (<http>-38.2KB)

Maniacs (<http>-65.36KB)

WSJ (<http>-501B)

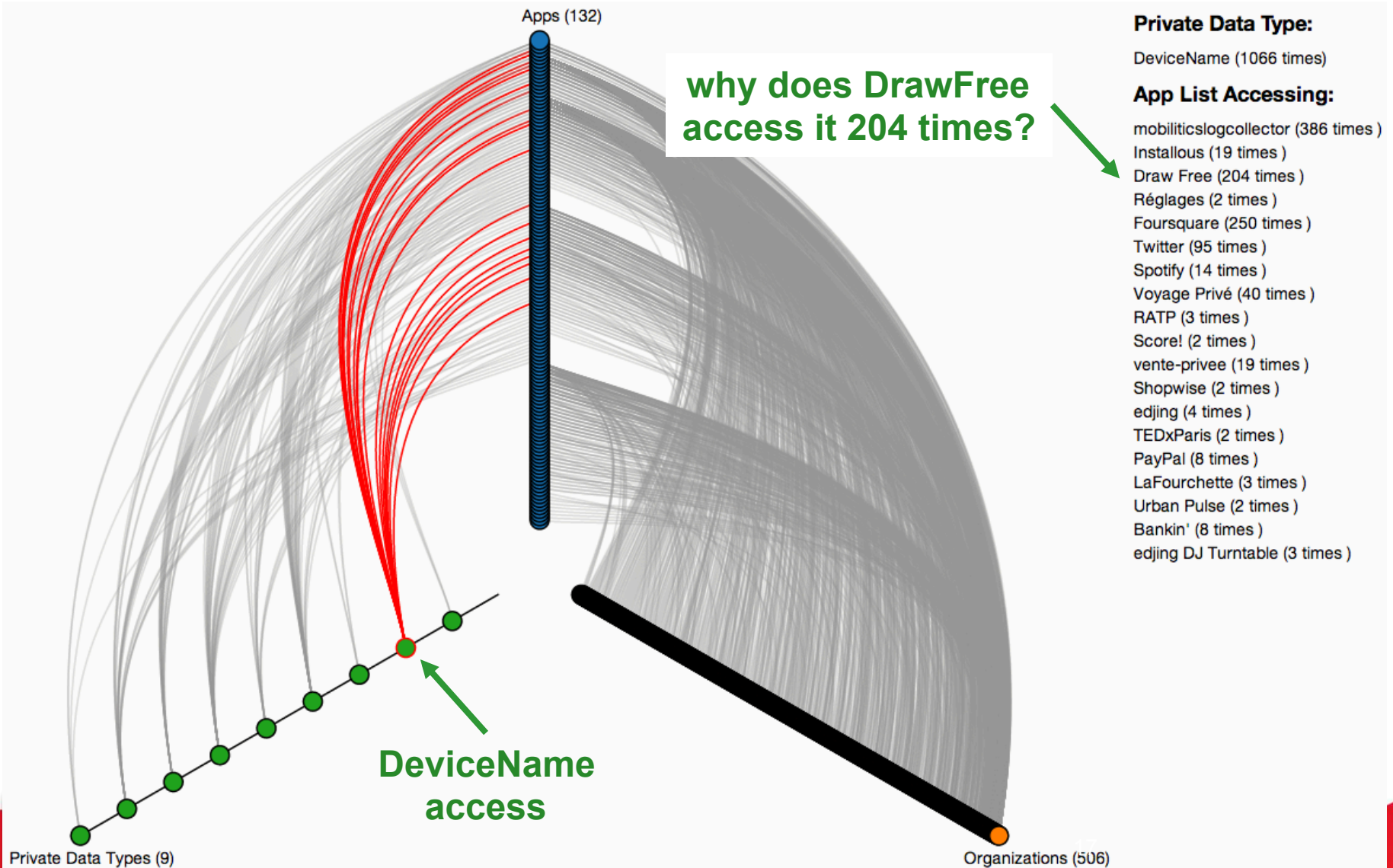
Traduction (<http>-6.57KB)

22racks (<http>-22.63KB)

Organization axis  
(most active on the right)



# An Example: DeviceName Access



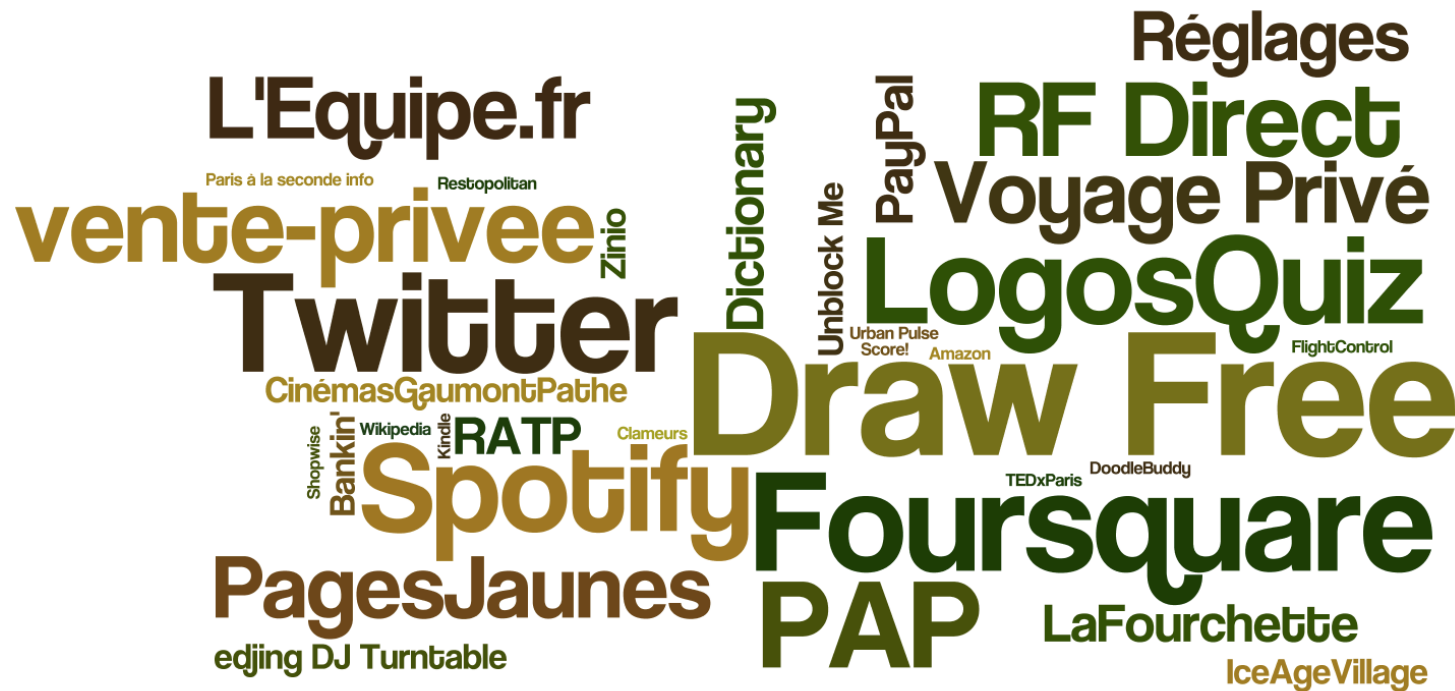
# Quelques Résultats...

- 6 volontaires de la CNIL pendant 3 mois
- 9 Go de données récoltées
- 7 millions d'événements à analyser dans la base de données
- 189 applications utilisées



# Pourquoi accéder au nom de l'appareil?

- 36 applications, soit un peu plus de 15% ont accédé à cette info.
- L'usage qui peut être fait de cette donnée est peu clair.



A screenshot of an iPhone's 'Informations' page. The status bar at the top shows 'SFR 3G', '14:29', and '80%'. The page title is 'Informations' with a 'Général' tab selected. The 'Nom' field shows 'iPhone de GDX'. Below are various system information fields:

Nom	iPhone de GDX >
Réseau	F SFR
Morceaux	506
Vidéos	0
Photos	78
Applications	151
Capacité	13,7 Go
Disponible	3,5 Go
Version	6.1.3 (10B329)

Outil : Wordle.net

Courtesy CNIL



# De nombreux acteurs économiques, invisibles pour les utilisateurs

- Des « acteurs tiers » très présents au sein des applications.
  - ❑ Ces acteurs fournissent des solutions techniques ou de monétisation au développeur (outils de statistiques, publicité, ...).
  - ❑ on retrouve des acteurs classiques du « *tracking* » : Google, **Criteo**, Xiti, ...
  - ❑ mais également des acteurs émergents, spécialisés dans le mobile (Flurry)
- Les moyens d'information et de contrôle par les utilisateurs, déjà limités dans le web « classique » sont inexistants dans le « in app ».

# La Suite?

- **Poursuivre les travaux**, notamment autour des **autres systèmes d'exploitation** pour smartphones (Android, WindowsPhone, ...);
- **Publier** - dans le cadre de publications scientifiques et plus « grand public » - des résultats;
- **Dialoguer avec tous les acteurs** : identifier et mettre en œuvre avec eux des bonnes pratiques (notamment dialoguer avec Apple autour des paramètres de vie privée disponibles);
- **Utiliser l'outil *Mobilitics* pour analyser en profondeur le « comportement » de certaines applications**

# Mobilitics: Next?



Google Glass

## Self-Tracking Devices





# Plus d'info.?

<https://team.inria.fr/privatics/mobilitics/>

[claude.castelluccia@inria.fr](mailto:claude.castelluccia@inria.fr)



[www.inria.fr](http://www.inria.fr)