Why Mobilitics ?
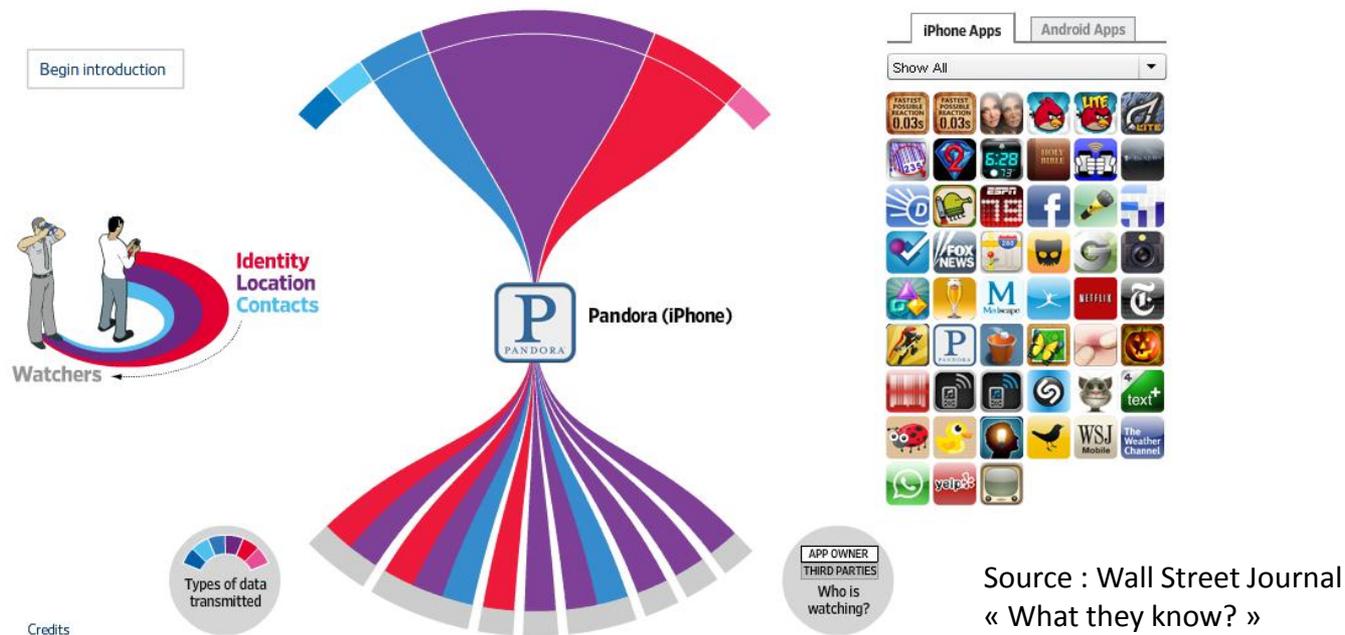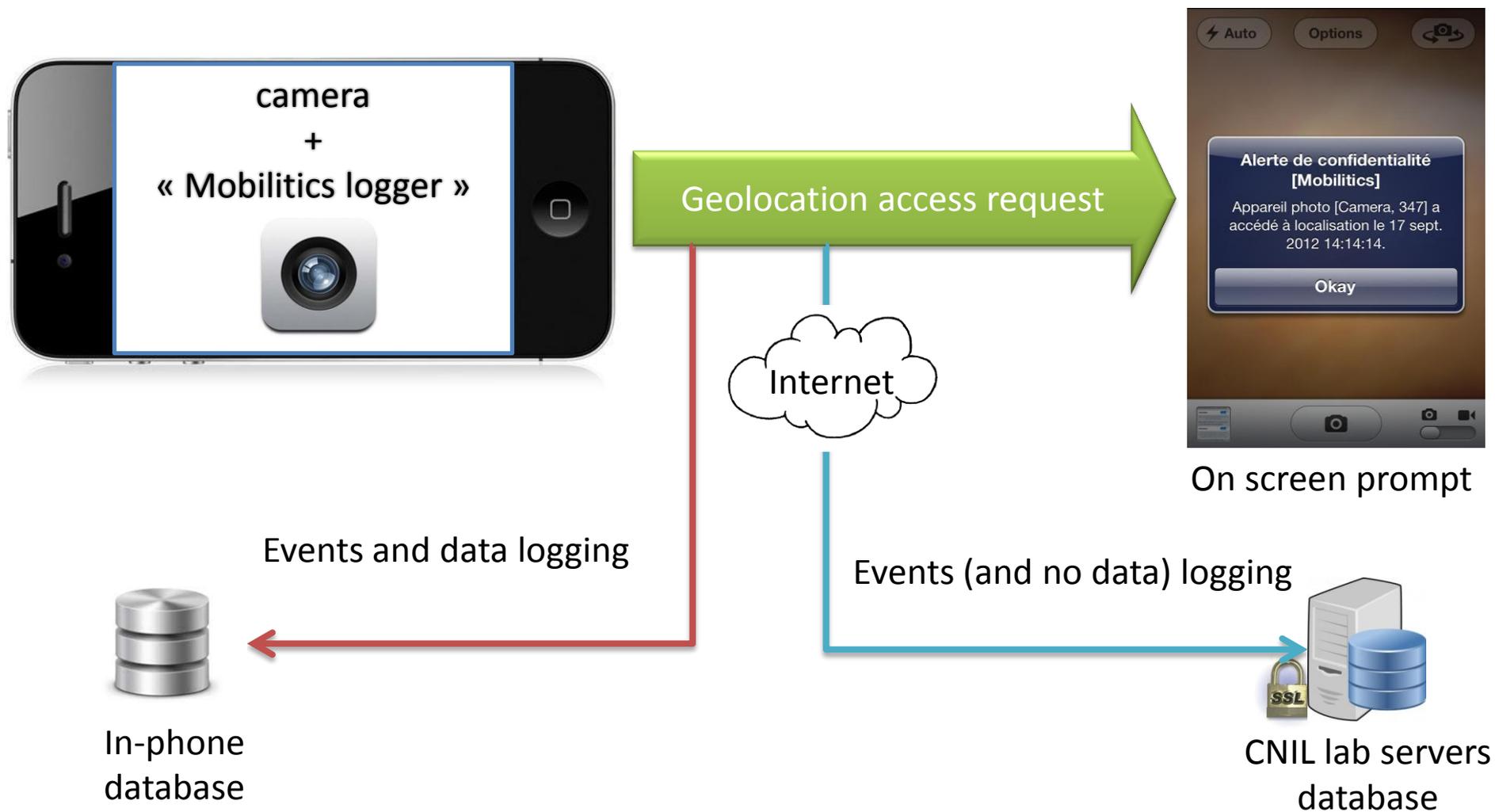
- Smartphones are black boxes for users… and regulators !
- Existing studies: in a « lab mode »

Source : Wall Street Journal
« What they know? »

➡ Mobilitics aim to give additional insights from « real life »
users perspective

Mobilitics, How does it work?

camera
+
« Mobilitics logger »

Geolocation access request

Alerte de confidentialité
[Mobilitics]

Appareil photo [Camera, 347] a
accédé à localisation le 17 sept.
2012 14:14:14.

Okay

On screen prompt

Internet

Events and data logging

Events (and no data) logging

In-phone
database

CNIL lab servers
database

Key results

Number of apps used during the 3-months experiment…	Total : 189	
- **Accessing network and communicating**	176	93%
- **Accessing the UDID**	87	46%
- **Accessing geolocation**	58	31%
- **Accessing « device name » info**	30	16%
- **Accessing user accounts data**	19	10%
- **Accessing to contacts list / address book**	15	8%
- **Accessing Apple account data**	4	2%
- **Accessing calendar data**	3	2%

Almost 50% sent it in clear text. Now : AD id? Fingerprint (MAC adress, …)? some others industry standard (openUDID, …)

76 events per day per user

No specific purpose

- Several (and in fact almost permanent) network accesses without a clear user information.
  - 9 out of 10 apps connect to the internet, even if the user doesn't see the direct result of this access (for example for games) ;
- A few applications generate the vast majority of accesses to data (with an intensity that seems to go beyond the simple needs related to obvious functions of these apps) ;
- Several apps access data not directly related to a user action or an obvious service provided by the application (recovery of unique identifier, of the device name, or very intense access to location data).

localhost:81/cookie_viz/

Ouvrir menu