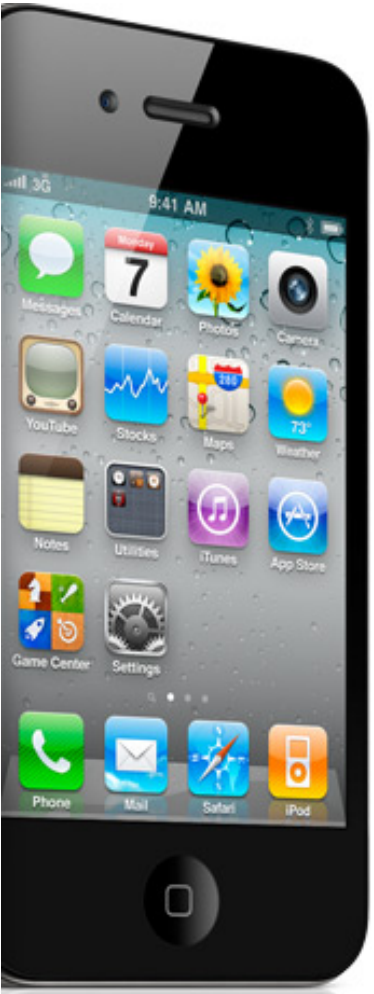
Mobilitics :
Saison 1 : résultats iPhone



CNIL. Labo d'innovation + Inria INVENTEURS DU MONDE NUMÉRIQUE

Conférence de presse du
9 avril 2013

Smartphone, un ami qui vous veut du bien...

- 24 millions de smartphones en France (médiamétrie, Septembre 2012)
- Près d'1 milliard de smartphones dans le monde (IDC, 2012)

2 grands univers concurrents :

Apple iOS

- 775 000 applications disponibles sur l'app store d'Apple
- Apple annonce 20 milliards de téléchargements en 2012

Google Android

- 700 000 applications disponibles sur le magasin "Play"
- 25 milliards de téléchargements depuis la création du magasin

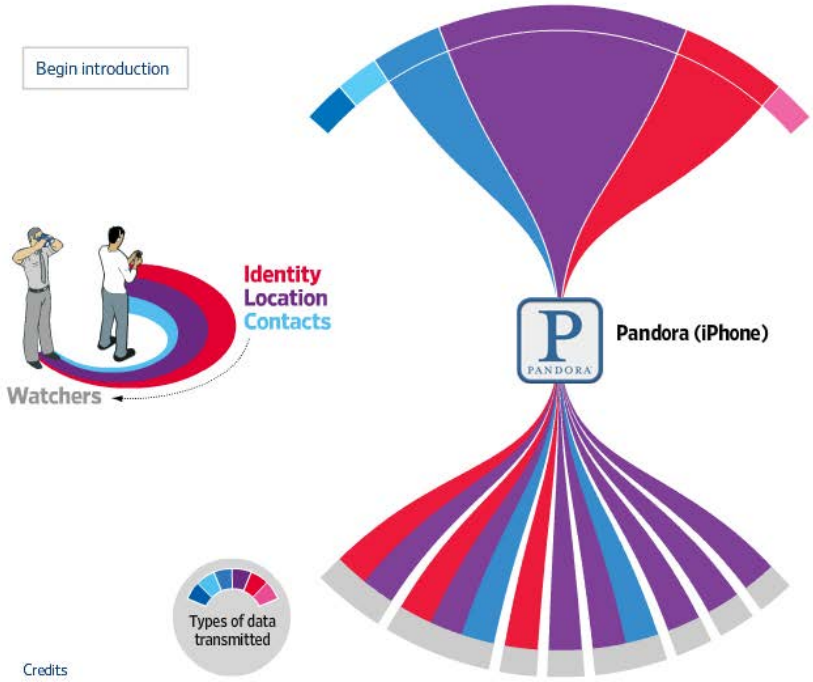
Et des concurrents qui suivent une voie similaire (magasins d'applications, ...) : RIM BlackBerry, Microsoft WindowsPhone, ...

Pourquoi Mobilitics ?

- Les smartphones sont des boites "noires" pour l'utilisateur...

et le régulateur !

- De nombreuses études "in vitro"



Source : Wall Street Journal
« What they know? »

Mobilitics complète ses résultats par des éléments "in vivo »

Mobilitics, comment ça marche ?

Demande d'accès à la géolocalisation

Internet

Stockage des évènements avec les données associées

Base de données interne au téléphone

Stockage des évènements sans les données associées

Base de données du laboratoire de la CNIL

Mobilitics, du *big data* à la CNIL?

- 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

Des résultats qui ne se veulent pas "représentatifs" des centaines de milliers d'applications, mais permettent :

- d'étudier dans le temps l'évolution des accès aux données personnelles ;

- de dresser un état des lieux des pratiques de collecte des différents acteurs.

Résultats globaux

Nombre d'applications utilisées durant l'expérimentation :	Total : 189	
- Qui accèdent au réseau	176	93%
- Qui accèdent à l'UDID (identifiant unique Apple)	87	46%
- Qui accèdent à la géolocalisation	58	31%
- Qui accèdent au nom de l'appareil	30	16%
- Qui accèdent à des comptes	19	10%
- Qui accèdent au carnet d'adresses	15	8%
- Qui accèdent au compte Apple	4	2%
- Qui accèdent au calendrier	3	2%

• Accès réseaux nombreux et quasi permanents sans une information claire des utilisateurs
• quelques applications sont responsables de la majorité des accès aux données, avec une intensité qui semble dépasser le seul besoin des fonctions de ces applications
• Certaines applications accèdent à des données sans lien direct avec une action de l'utilisateur ou un service offert par l'application (récupération de l'identifiant unique, du nom de l'appareil, de la localisation).

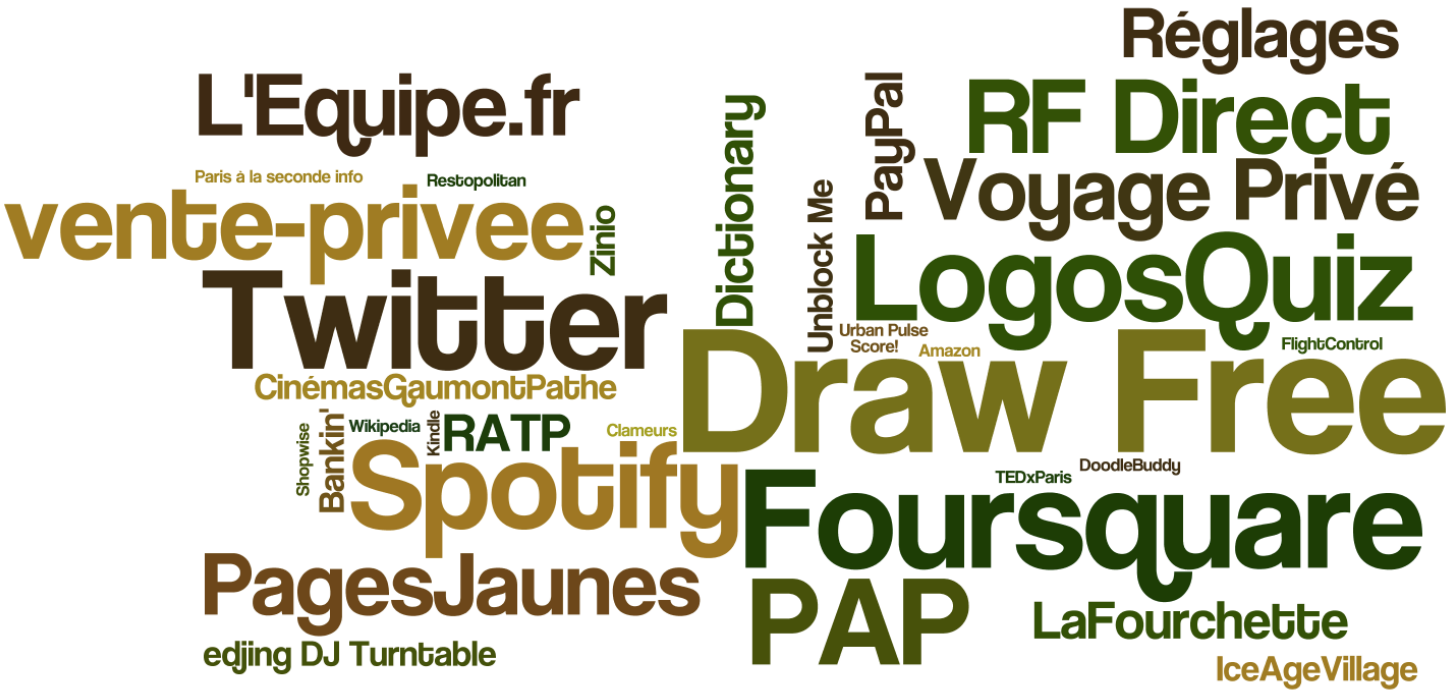
La géolocalisation, reine des données

- 31% des applications utilisées ont cherché à accéder à la localisation
- 41 000 « événements » de géolocalisation au total,
- soit une moyenne de 76 événements par jour et par volontaire
- L'intensité de ces accès surprend.

Outil : Wordle.net

Pourquoi accéder au nom de l'appareil?

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



Outil : Wordle.net

Identifiants et tracking envahissent les smartphones

• UDID : identifiant intégré à l'appareil par Apple et qui ne peut être ni modifié ni effacé par l'utilisateur.

• bientôt plus accessible, remplacé par un identifiant de publicité et un identifiant par vendeur

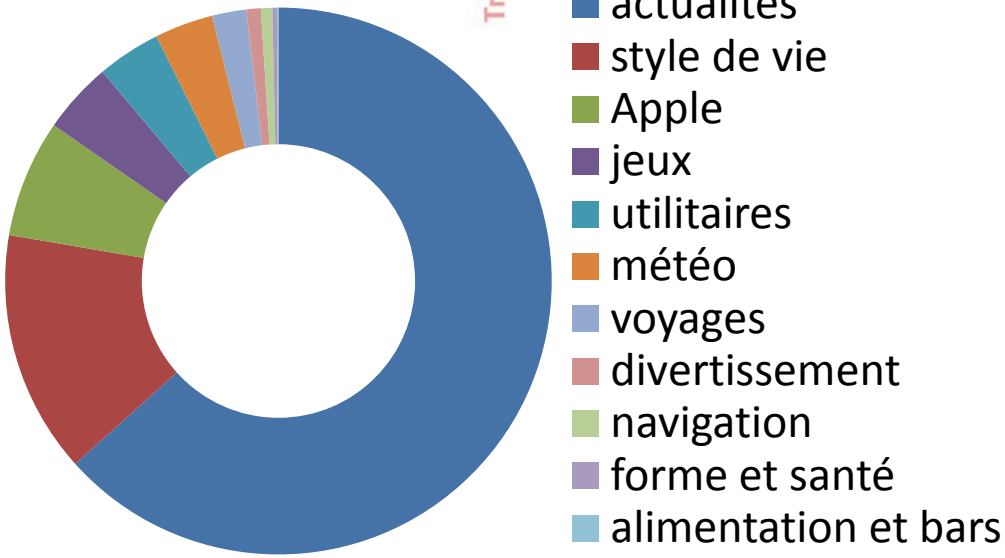
Identifiants et tracking envahissent les smartphones

• Cet UDID est très « demandé » : **87 applications sur les 189 ont accédé à l'UDID, soit presque 50% ;**

• il est souvent récupéré par l'éditeur de l'application : **33 applications l'ont transmis en clair**, la plupart du temps plusieurs fois durant l'expérimentation ;

• et demain? Quelles méthodes ?

Outil : Wordle.net



(Applications ayant transmis l'UDID en clair, regroupées par catégories de l'App store)

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)

- L'extension de la problématique des cookies à l'intérieur des applications est en cours.

- Les moyens d'information et de contrôle par les utilisateurs, déjà limités dans le web « classique » sont inexistants dans le « in app ».

La responsabilité partagée de tous les acteurs de la chaine

• **Développeurs d'application** : « privacy by design » et besoin d'accompagnement

• **Magasins d'application** : inventer des modes innovants d'information des utilisateurs et de recueil du consentement au-delà du « à prendre ou à laisser » actuel

• **Editeurs de systèmes d'exploitation** : proposer un contrôle plus fin et contextualisé. La CNIL et Inria ont à cet égard développé à titre expérimental un « démonstrateur » de ce que pourraient être ses réglages.

• **Les acteurs tiers** doivent adopter une approche de minimisation des données collectées et être clairs avec les développeurs sur les conséquences vis-à-vis de l'utilisateur final

Et demain?

• **Poursuivre les travaux**, notamment autour des **autres systèmes d'exploitation** pour smartphones (Android, WindowsPhone, …);

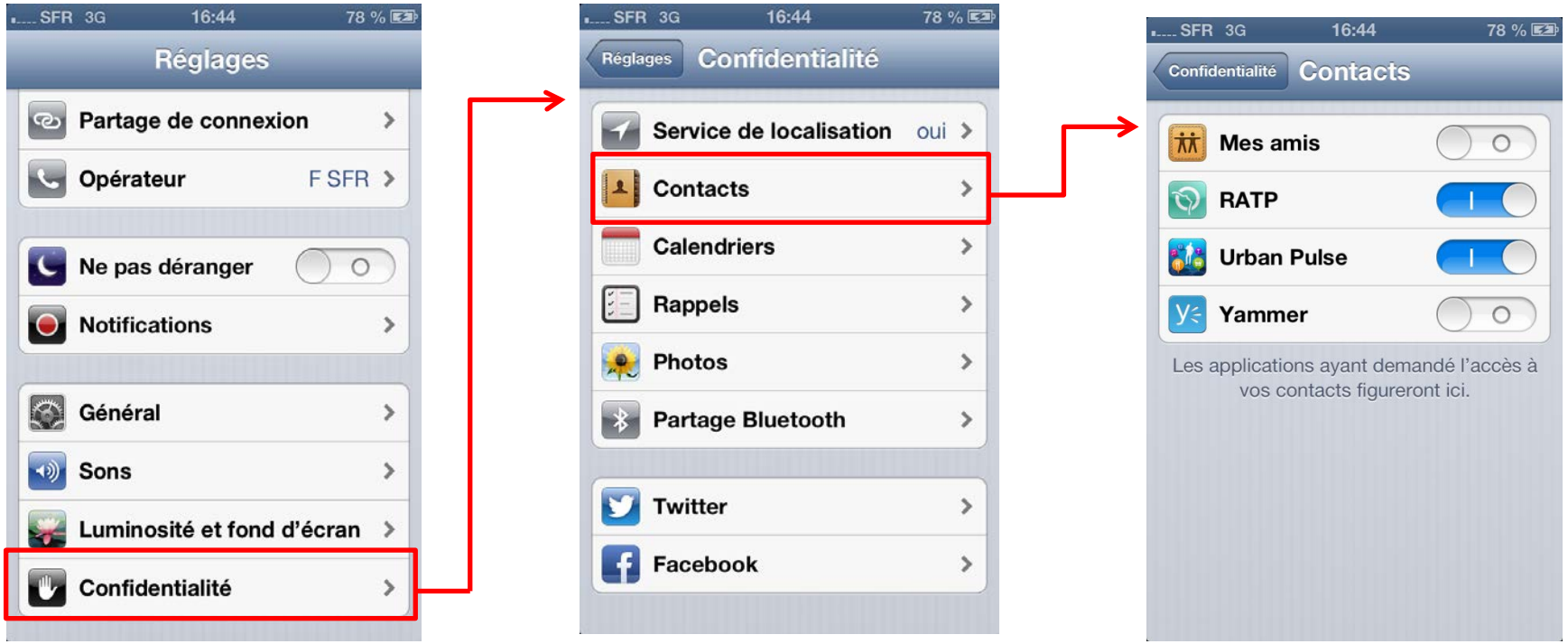
• **Publier** - dans le cadre de publication scientifiques et plus « grand public » - des résultats;

• **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**.

Démonstrateur « privacy extension »

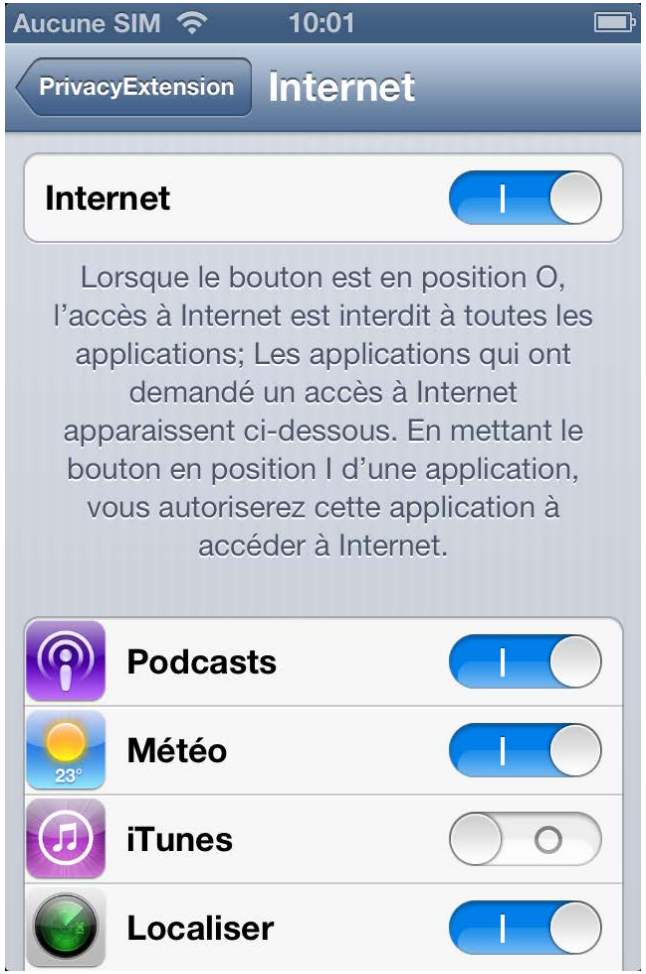
1. Ce que propose pour le moment Apple (iOS6)



2. Les résultats *mobilitics* montrent que des catégories de données sont à la fois très exploitées et en dehors du champ de ces options :
    - **Le nom de l'appareil (Device Name)**
    - **L'identifiant unique (UDID)**
    - **L'identifiant de publicité**
    - **Les accès au réseau**

[Retour]

Pour répondre à ce problème : Mobilitics Privacy extension (démo)



[Retour]