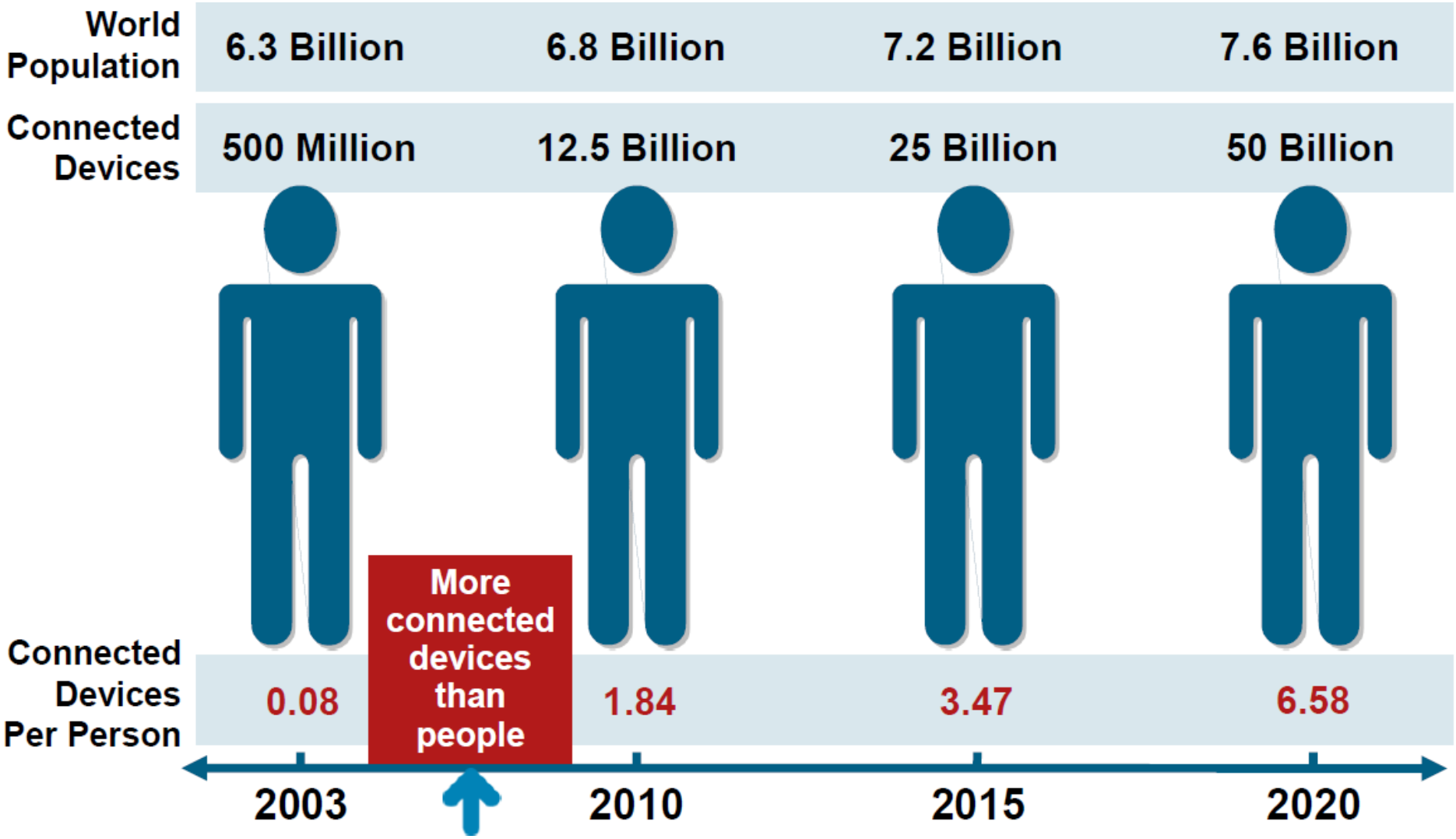
Stéphane Petitcolas– Ingénieur Expert à la CNIL

DE L'INFORMATIQUE NOMADE À L'INFORMATIQUE AMBIANTE : LES ENJEUX EN TERME DE VIE PRIVÉE

Nombre de dispositifs “connectés” selon CISCO



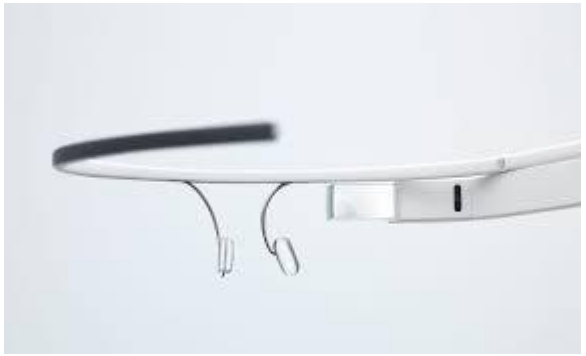
Observons les objets intelligents d'aujourd'hui…
…pour deviner vers où va l'intelligence ambiante promise demain.

Quels risques de traçage des personnes ?


optile
RATP
SNCF
NAVIGO
STIF
AUTORITÉ ORGANISATRICE DES TRANSPORTS D'ILE-DE-FRANCE


android


4000 1234 5678 9010
12/09
B. PARKER



Le pass navigo

1975

- Anonyme
- Rachat en cas de perte
- Pas de fichier clients
- Statistiques pauvres

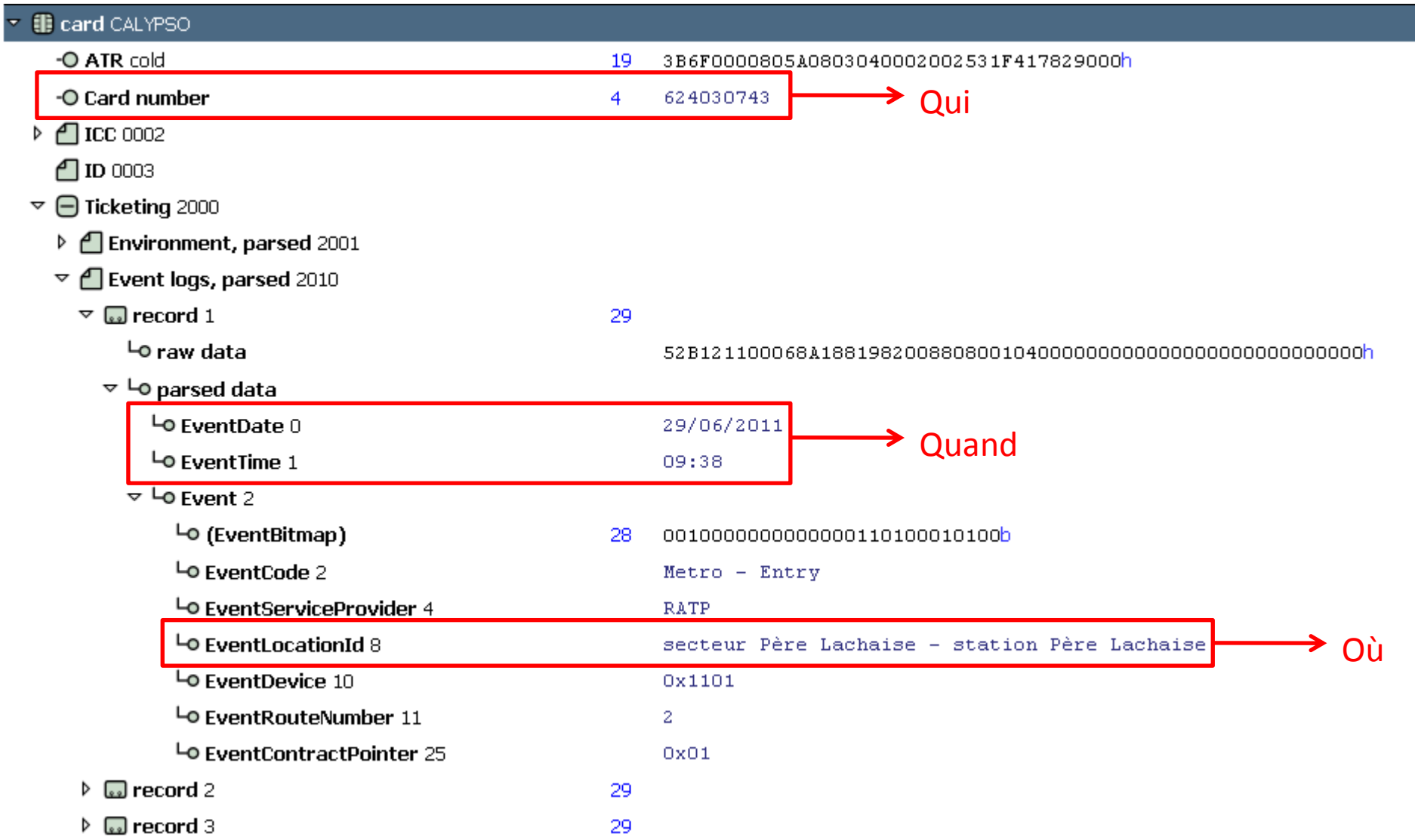
2009

- Un numéro unique
- Personelle et infalsifiable
- Remplacée en cas de perte
- Un fichier clients
- Des statistiques réseaux fines

? ? ?

100 % 2 % 40 %

Dans la puce du pass navigo



Les leçons du pass navigo

- Les actions de la CNIL
  - Imposer une anonymisation des données collectées.
  - Imposer l'existence d'un « pass anonyme »
    - Mais il coûte 5 euros…

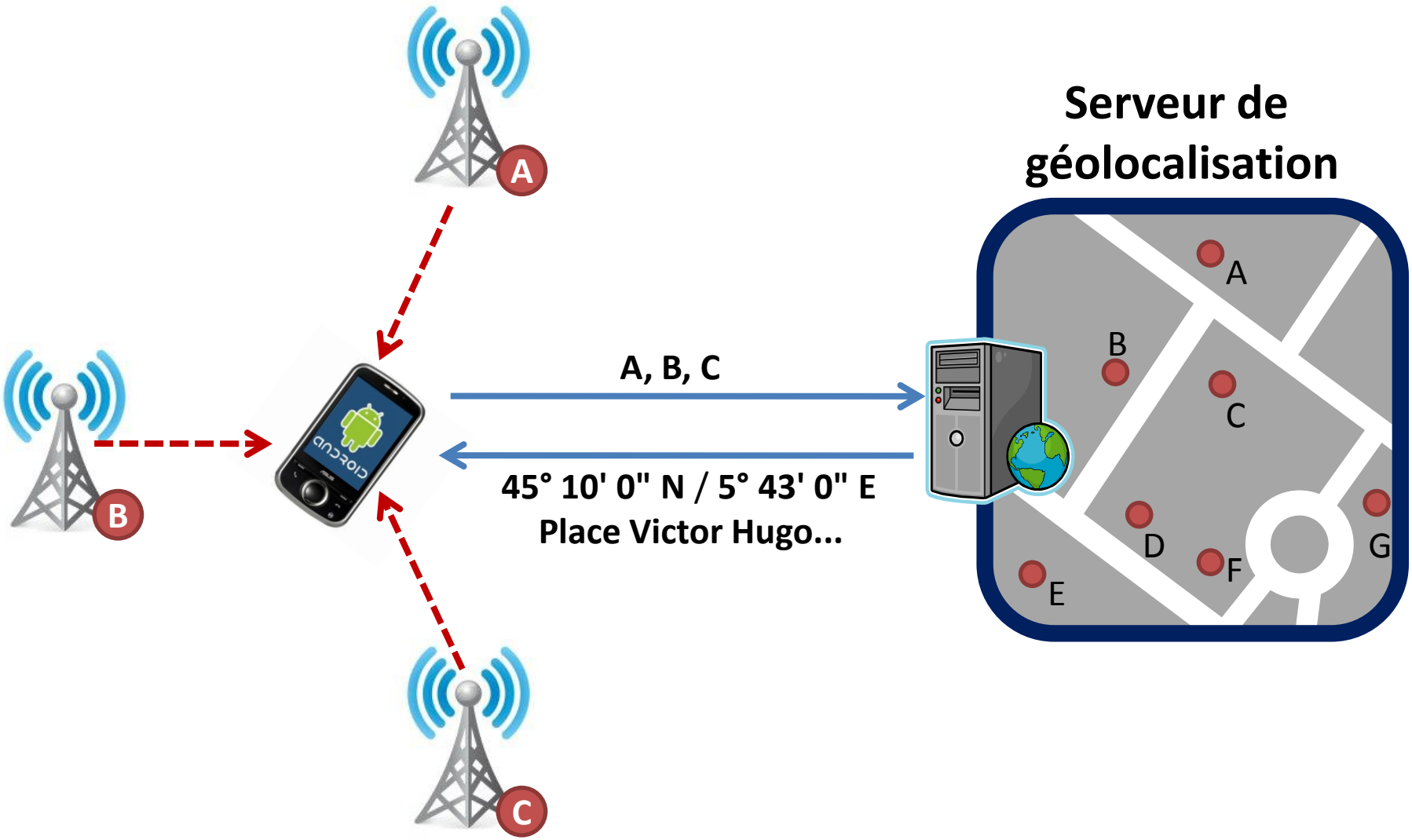
- Ce n'est pas de l'intelligence ambiante mais déjà de l'intelligence dans les objets + des capteurs.
- **Demain la reconnaissance faciale pour remplacer le pass navigo ?**
- **Confort = traçabilité des personnes?**

Les cartes bancaires sans contact

Les actions de la CNIL

- Participation aux groupes de travail autour des cartes bancaires sans contact
- Demande de suppression du nom et de la date de validité en lecture sur l'interface sans contact
- Mise en application de cette recommandation depuis septembre 2012
- Suppression de la liste des transactions depuis mi 2013

La géolocalisation mobile WiFi



Comment constituter une base de géolocalistion?

Méthode « ancienne »: faire travailler des employés

Comment constituter une base de géolocalistion?

Méthode « crowdsourcing »: faire travailler les utilisateurs

Les leçons des mécanismes de géolocalisation

- Des capteurs et des réseaux:
  - Des usages impossibles à deviner à l'avance.
  - Un boom du « crowdsourcing » à prévoir

- Que fait-on des données collectées:
  - Transferts à des partenaires?
  - Publicité?
  - Quels droits (réels) pour les personnes?

Mobilitics : un projet de recherche pour mieux comprendre les smartphones

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).

Mobilitics : un projet pour comprendre l'utilisation des données à caractère personnel dans un téléphone

- 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.

Les objets connectés de demain

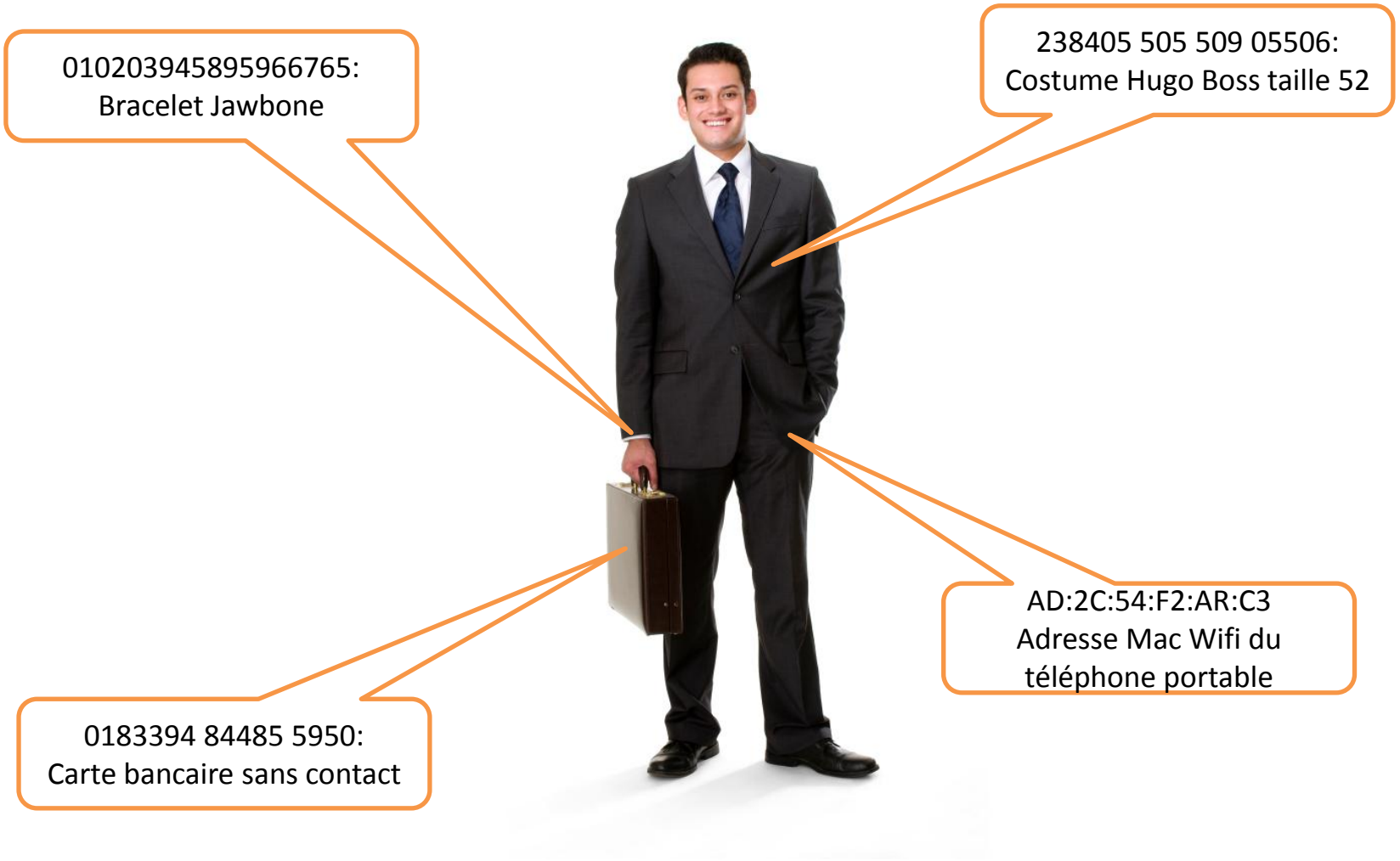
- Les compteurs intelligents
  - Réflexion des groupes de travail Européen

  sur la définition du périmètre des études d'impacts

- Le mouvement du « quantified self »

- Les Google Glass

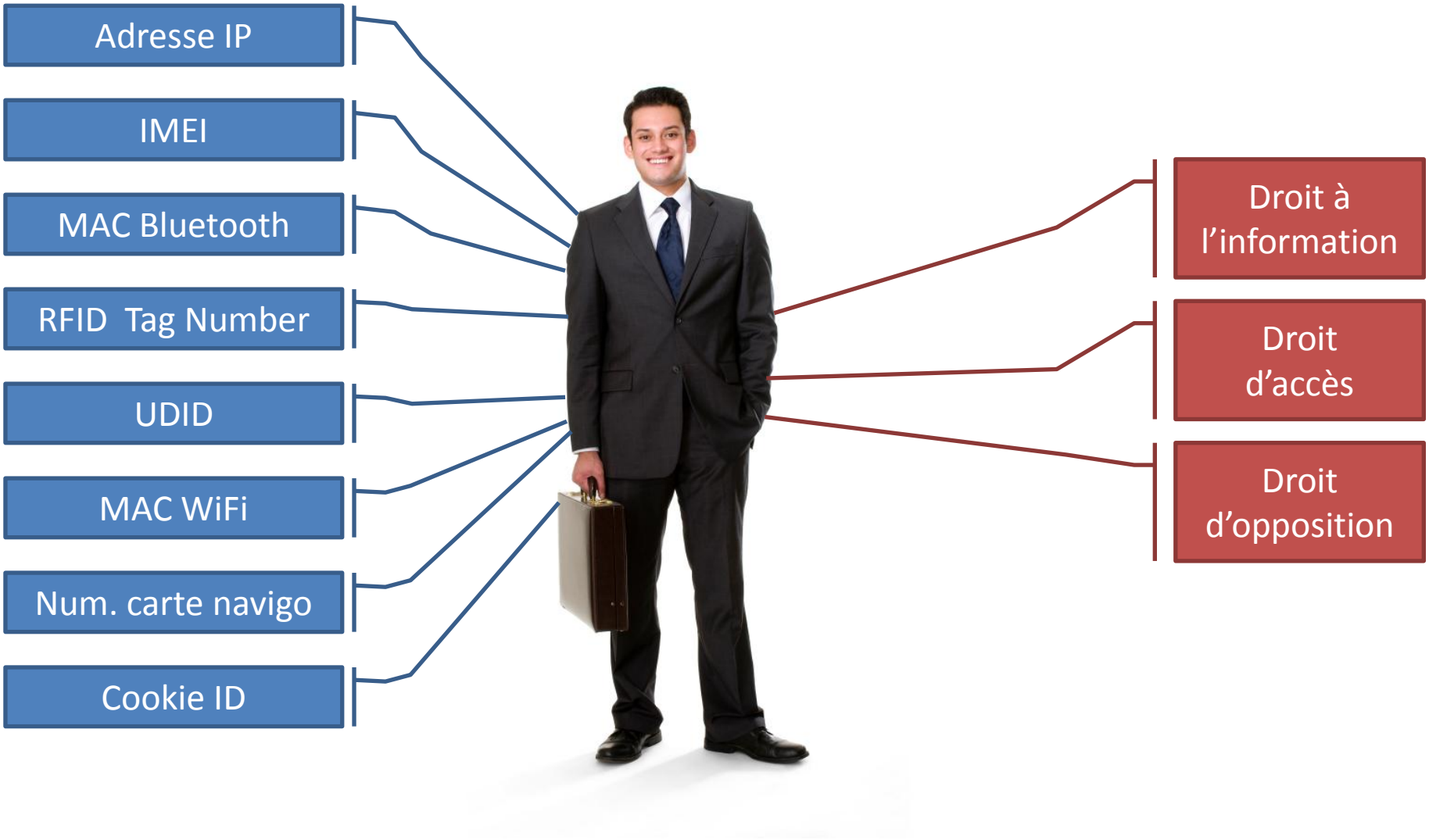
Quels risques pour la vie privée?



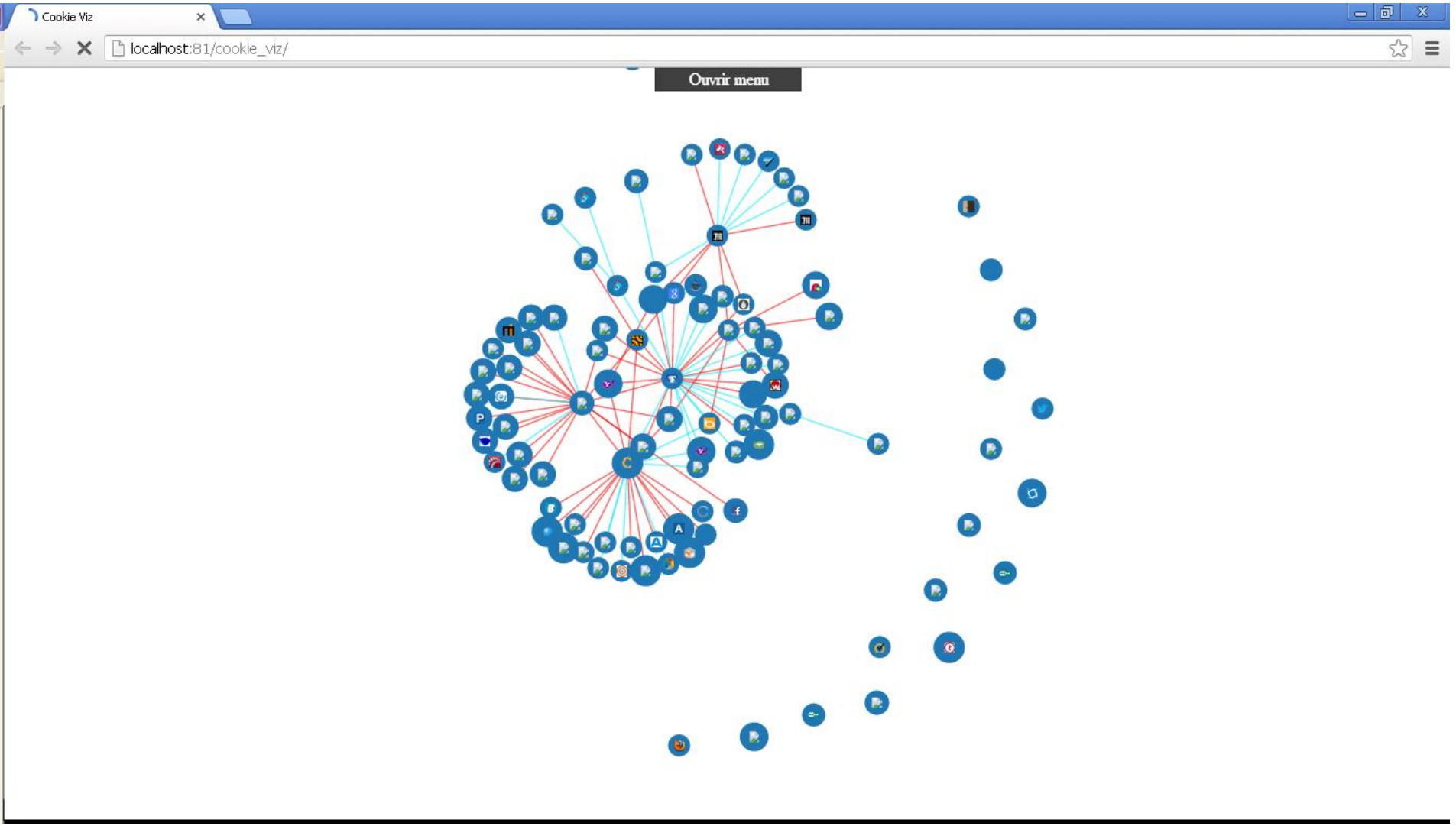
Un cadre européen pour les RFID

- Une recommandation de mai 2009 de la Commission Européenne sur les RFID. Principes:
  - Conduire des études d'impact sur les produits RFID.
  - La désactivation des puces au point de vente dans la grande distribution.
    - Sauf exception si l'étude d'impact montre une absence de danger.
- Les études d'impact RFID: un instrument utile?

D’une identification ubiquitaire… vers un déséquilibre?



Un exemple de traitement invisible : Les cookies



Quelles solutions ?

L'approche actuelle

- **Déploiement produit / service**
- Déclaration / contrôle CNIL
- Problème / Sanctions
- Correction des problèmes
- Approche « pansement »

Des solutions pour demain ?

- Analyse d'impact / de risque
- Correction des problèmes
- **Déploiement produit /service**
- Contrôle CNIL
- Approche « privacy by design »

Demain

ALORS?

Des tendances

- Chaque être humain aura des dizaines ou des centaines de puces.

- La donnée personnelle va changer de nature:
  - 1978: Nom, prénom, numéro de sécurité sociale, …
  - 2013: Adresse IP, MAC, IMEI, Numéro de série, …

- Des traitements invisibles par milliers.
  - un coût de stockage des données proche de zéro.
  - sans frontières.

Enjeux

- Pour le monde de la recherche
  - Sécurité des systèmes
  - Anonymisation / pseudonymisation
  - Minimisation des données

- Pour les industriels
  - Sécurité des systèmes
  - Le « Privacy by design »
  - L'exercice effectif des droits des personnes

- Pour le monde du droit
  - Une jungle d'expertise technologique?