Links between wearable devices, identity concept and privacy by design

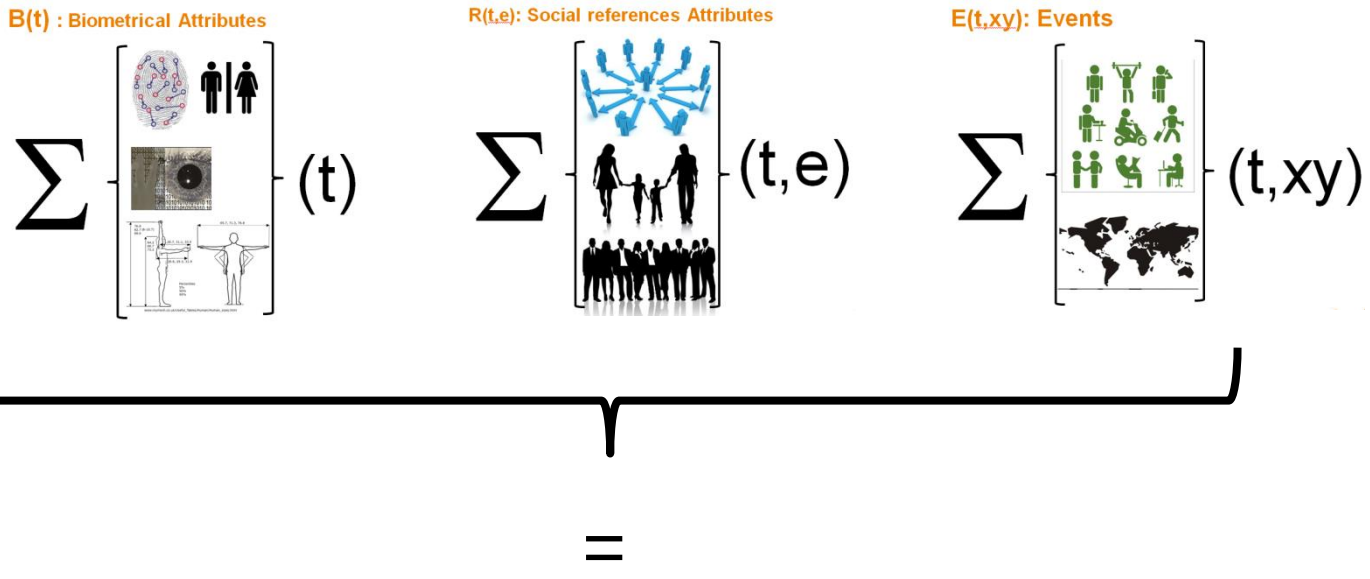
Alain RHELIMI

June 2014

Journée sur l'Internet des Objets et la Cybersécurité/Cyberdéfense

IDENTITY: What is it?

- Collection of Attributes(*)



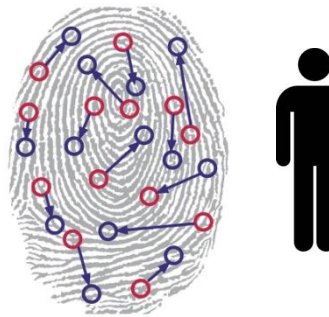
=

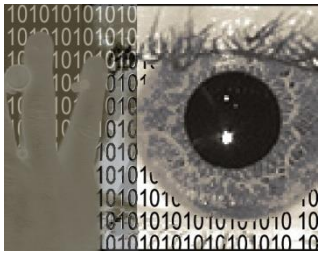
Identity Signature footprint (a virtual DNA)

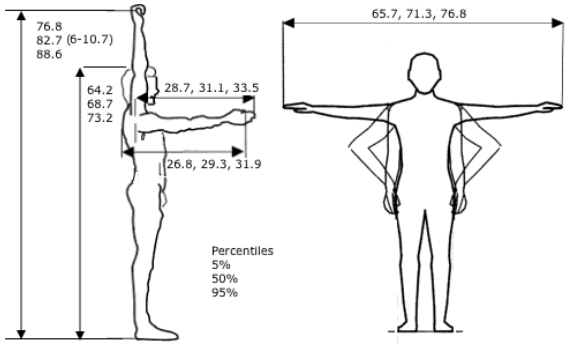
* Most of them are referenced to the time (and the space)

B(t) : Biometrical Attributes

$$\sum \left\{ \right\} (t)$$







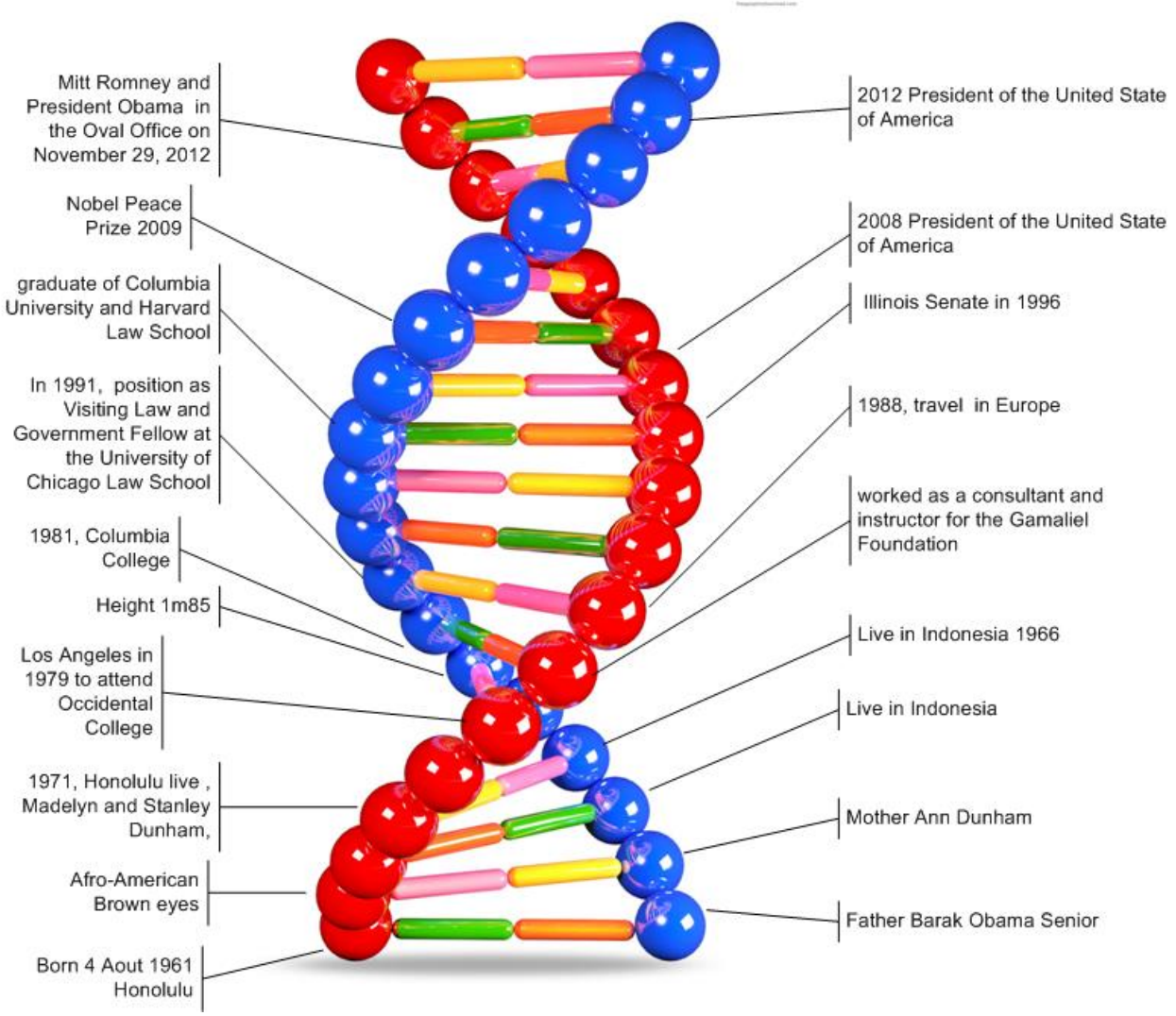
R(t,e): Social reference Attributes

$$\sum \left\{ \right. \quad \left. \right\} (t,e)$$

E(t,xy): Events

$$\sum \left\{ \text{  } \right\} (t,xy)$$

Identity: a virtual DNA

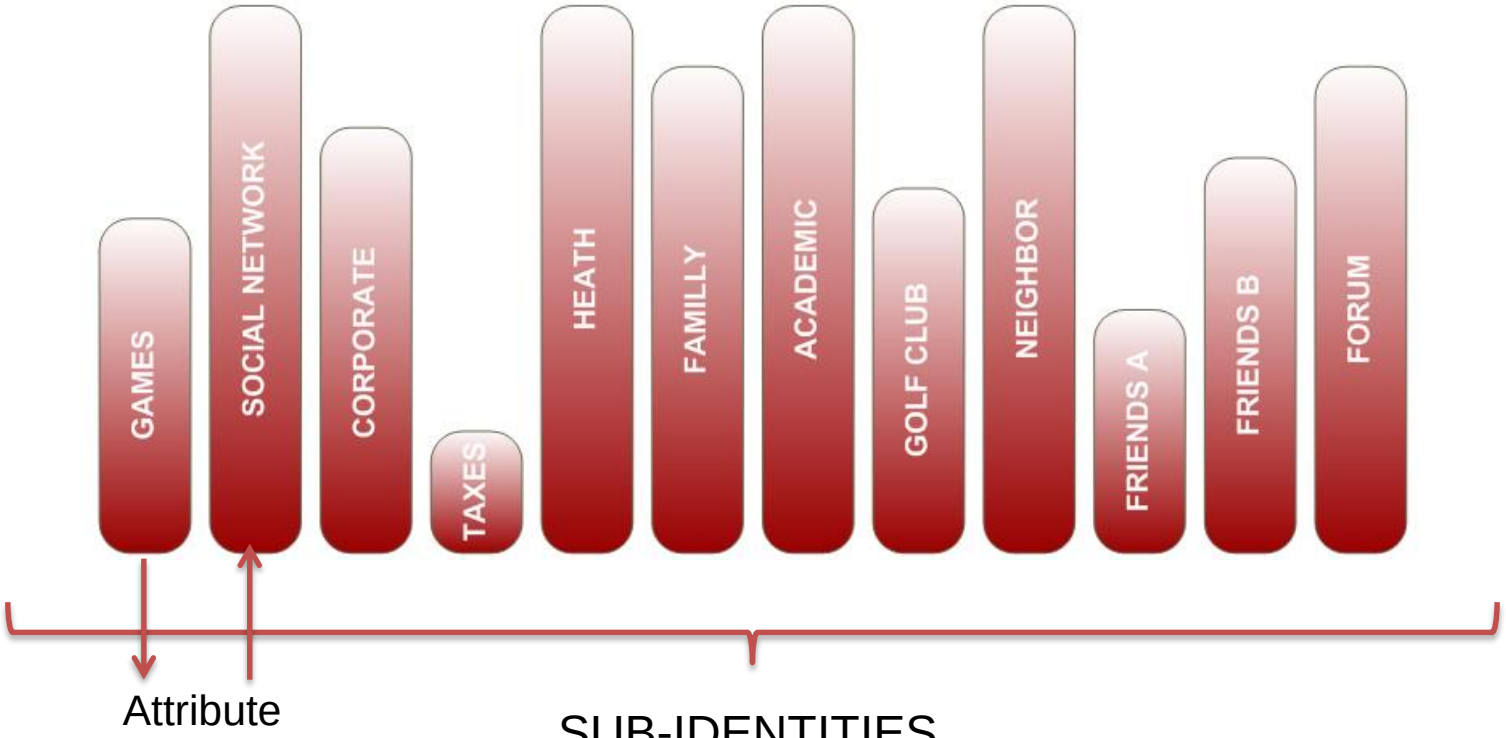


- Redundant
- Traceable
- Cross-checkable
- Recordable
  - Partially
- Authentic
  - Cannot be faked globally

$$DNA(t)=\begin{pmatrix} B(t) \\ R(t,e) \\ E\,(t,xy) \end{pmatrix}$$

Privacy Protection

- Attributes of the identity are grouped according to contexts



- The privacy protection is a set of means which aims at preventing the disclosing of the attributes of a sub-identity group to another without the user's agreement

We have an overview about what the identity and the privacy are….

but ...

WEARABLE & PORTABLE DEVICES

What does this means?

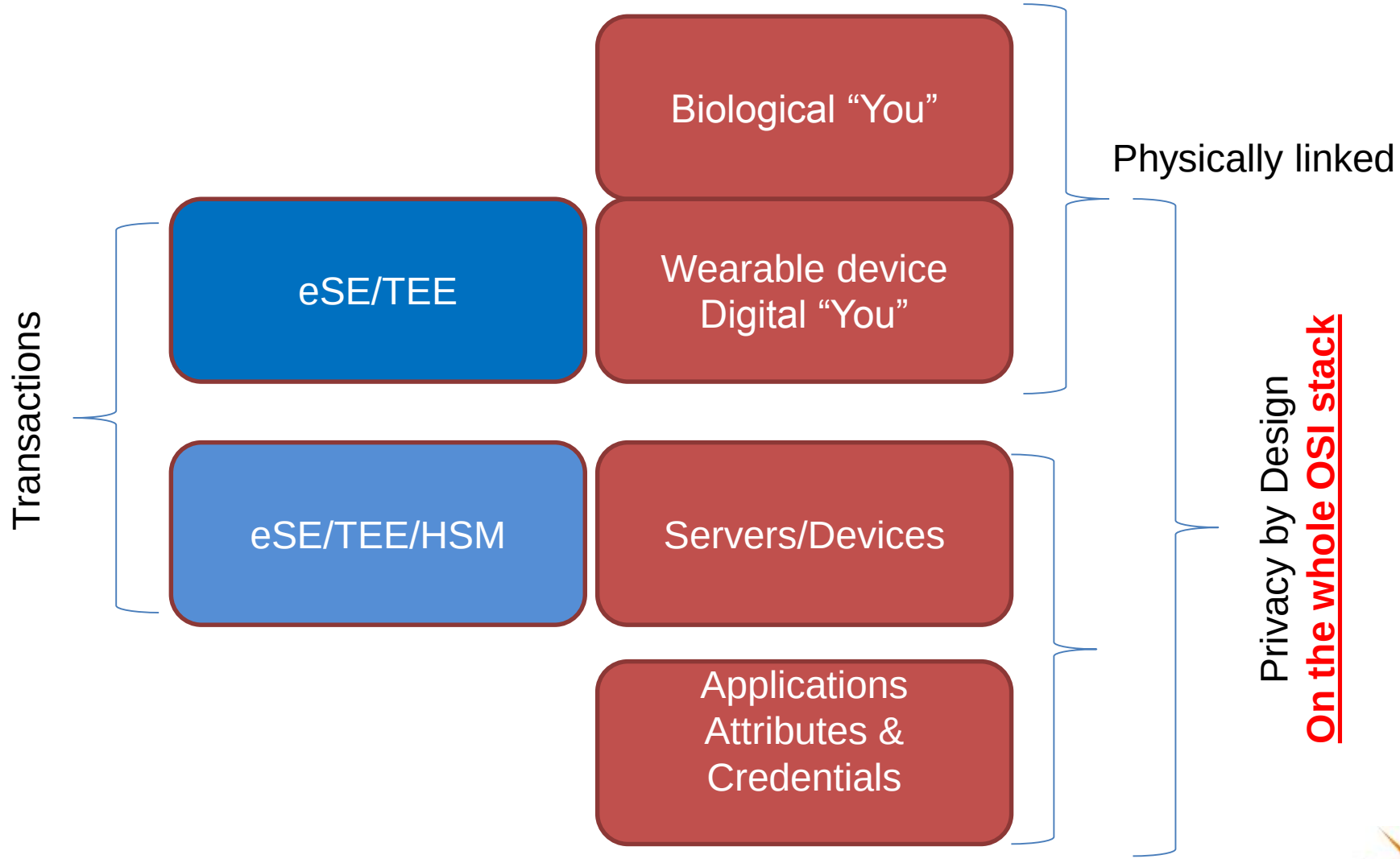
Wearable versus Portable

- Portable
  - Device on the user's body but not attached to the body
  - No single sign-on possible

- Wearable
  - Device attached to the user's body
  - Single sign-on possible
  - 2FA* with the user's experience of 1FA
  - Aim at being YOU in the digital world

*2FA: Two Factors of Authentication

Where are the links ?



Wearable devices: new threats against Privacy?

- Identity = collection of independent sub-identities
- Sub-identity = collection of attributes
  - B(t): Biometrical
  - R(t,e): Social references: sharing your events
  - E(t,xy): Events (time/space dependent)
- Privacy = user's control to disclose attributes from a sub-identity to another

- Wearable devices = the digital "YOU"
- Wearable device = mobility = E(t,xy): Events (time/space dependent)

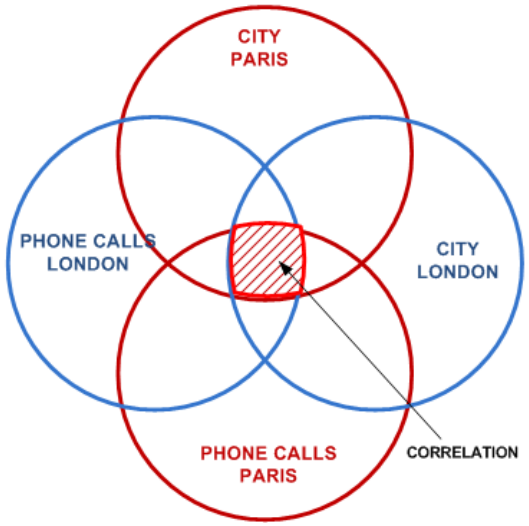
- From Correlation between E(t,xy) events we may deduce all other attributes = NO PRIVACY!

The Privacy by Design : 7 Principles

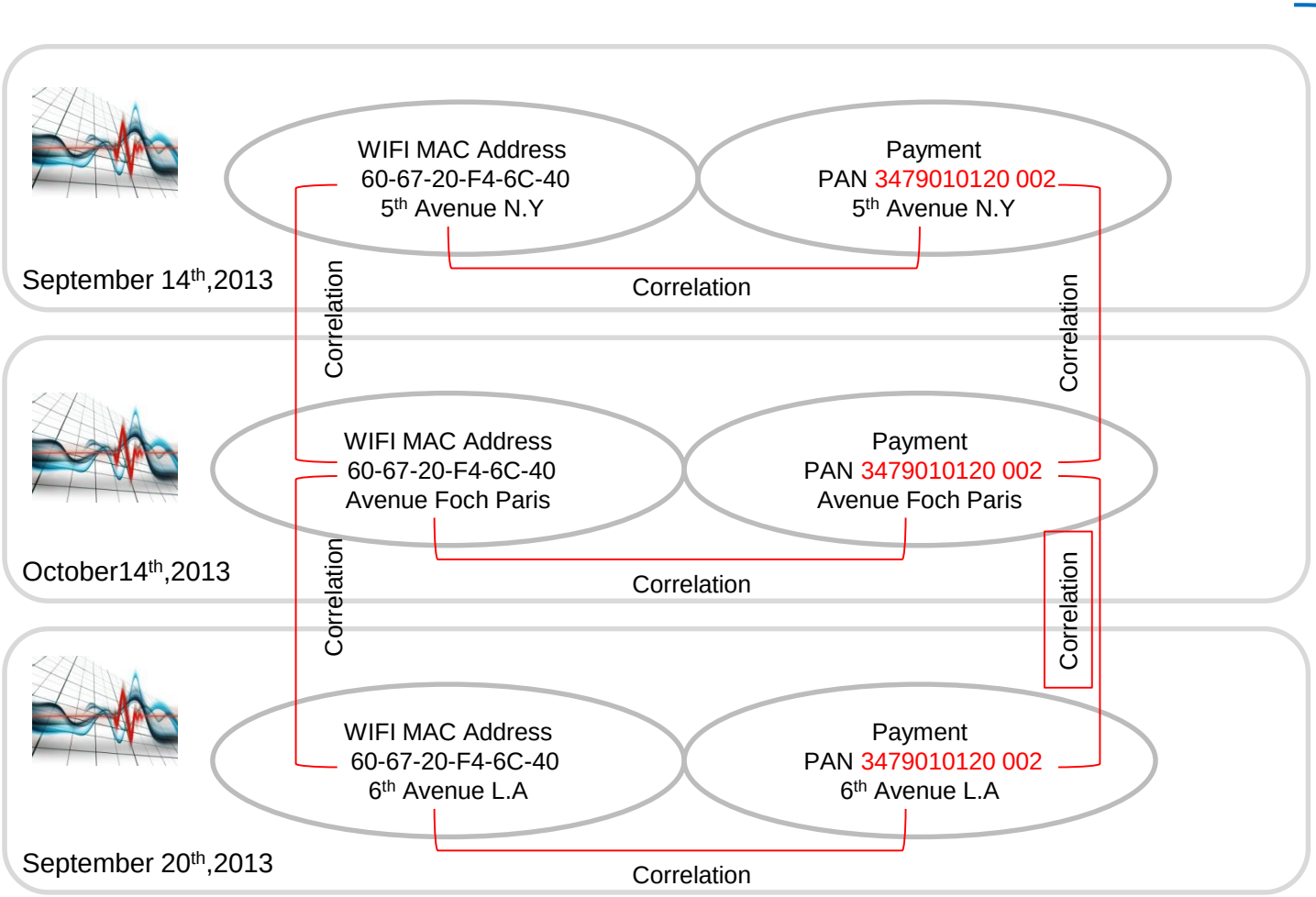
- 1. Proactive not Reactive; Preventative not Remedial
- 2. Privacy as the Default Setting
- 3. Privacy Embedded into Design
- 4. Full Functionality — Positive-Sum, not Zero-Sum
- 5. End-to-End Security — Full Lifecycle Protection
- 6. Visibility and Transparency — Keep it Open
- 7. Respect for User Privacy — Keep it User-Centric

Design impacts about Data Correlation

- The No Traceability property: The hardest property to support for data exchanges with:
  - No large constant data
  - No large identifier
  - No diversified Public key
  - No UUID
  - No static combination of small constants (fingerprinting)



Data Correlation & scoring example



Scoring

60-67-20-F4-6C-40 = 3479010120 002 = John Does

New challenge to support about wearable devices

- Data correlation prevention involving new protocols
  - fast authentication protocol, **non traceable** and supporting open systems
  - Data exchanges on the whole data path appearing as random for an observer outside an application (e.g. no static wireless MAC address)
- On device generic facilities
  - Secure synchronization between multiple devices related to a single user
  - User's data disaster recovery on a blank device without specific equipments
  - Cloning of applications and credentials to blank devices
  - User's checking for the detection of fake devices without specific equipments
  - Easy Initial enrolment
- But supporting constraints asking for antagonist technical solutions such as:
  - Fast responsiveness and short transactions (e.g < 100 ms for conditional physical access)
  - Long autonomy (several days even weeks)
  - Small form factors (eg. a watch) and small battery
  - Low cost for matching the expectations of the consumer mass markets
  - Easy manufacturing within standard and non secure promesses
- And shall support
  - National and international legal regulations

What did we?

eGo

What you touch is yours

The eGo project

- Started in 2004
  - eGo Catrene program in 2010 to 2014 (www.ego-project.eu)
  - H20 Catrene program in 2015 to 2018
- Minimal technology for a wearable device and the user's credentials support
  - Easy pairing (BCC) of any eGo compliant devices touched by the user
  - Long autonomy on several weeks
  - Harsh Environment support
  - Credentials recovery
  - Multi-tenants and multi-TSM
- Privacy by Design
  - authenticity, anonymity, non traceability.
  - Non relay attack possibility (UWB), Lost detection
  - Common criteria capable
- User's interface Friendly
  - Education/age independence (natural user's interface)
  - Single sign-on and strong authentication (2FA)
  - Automatic and programmed application termination (UWB)
  - On the go transaction and long transaction support
  - Fast (<200 ms) application setup
  - Implicit (pre-agreement) and explicit (post-agreement) eGo pairing
- Side effect capability
  - Accurate RTLS

Questions?

THANK YOU