

# *Privacy by design in embedded system*



Harald Kosch

18.03.2022

- 1. Privacy by Design*
  - 2. Embedded Systems and IoT*
  - 3. Privacy by Design in Embedded Systems*
-

**Privacy  $\neq$  Secrecy**

**Privacy is *not* about having something  
to hide**

---

- **Information privacy** refers to the right or ability of individuals to exercise control over the collection, use and disclosure by others of their personal information
  - **Personally-identifiable information (“PII”)** can be biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, and is the stuff that makes up our modern identity
  - **Personal information** must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded.
-

<ul style="list-style-type: none"><li>• Safeguards</li></ul>	<b>Safeguards</b>
<ul style="list-style-type: none"><li>• Purpose Specification</li><li>• Collection Limitation</li><li>• Use, Retention and Disclosure Limitation</li></ul>	<b>Data Minimization</b>
<ul style="list-style-type: none"><li>• Consent</li><li>• Accuracy</li><li>• Access</li><li>• Redress</li></ul>	<b>User Participation</b>
<ul style="list-style-type: none"><li>• Accountability</li><li>• Openness</li><li>• Compliance</li></ul>	<b>Accountability (beyond data subject)</b>

# Privacy by Design: The 7 Foundational 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**.



## Privacy by Design

### The 7 Foundational Principles

Ann Cavoukian, Ph.D.  
Information & Privacy Commissioner  
Ontario, Canada

*Privacy by Design* is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

*Privacy by Design* advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

*Privacy by Design* extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

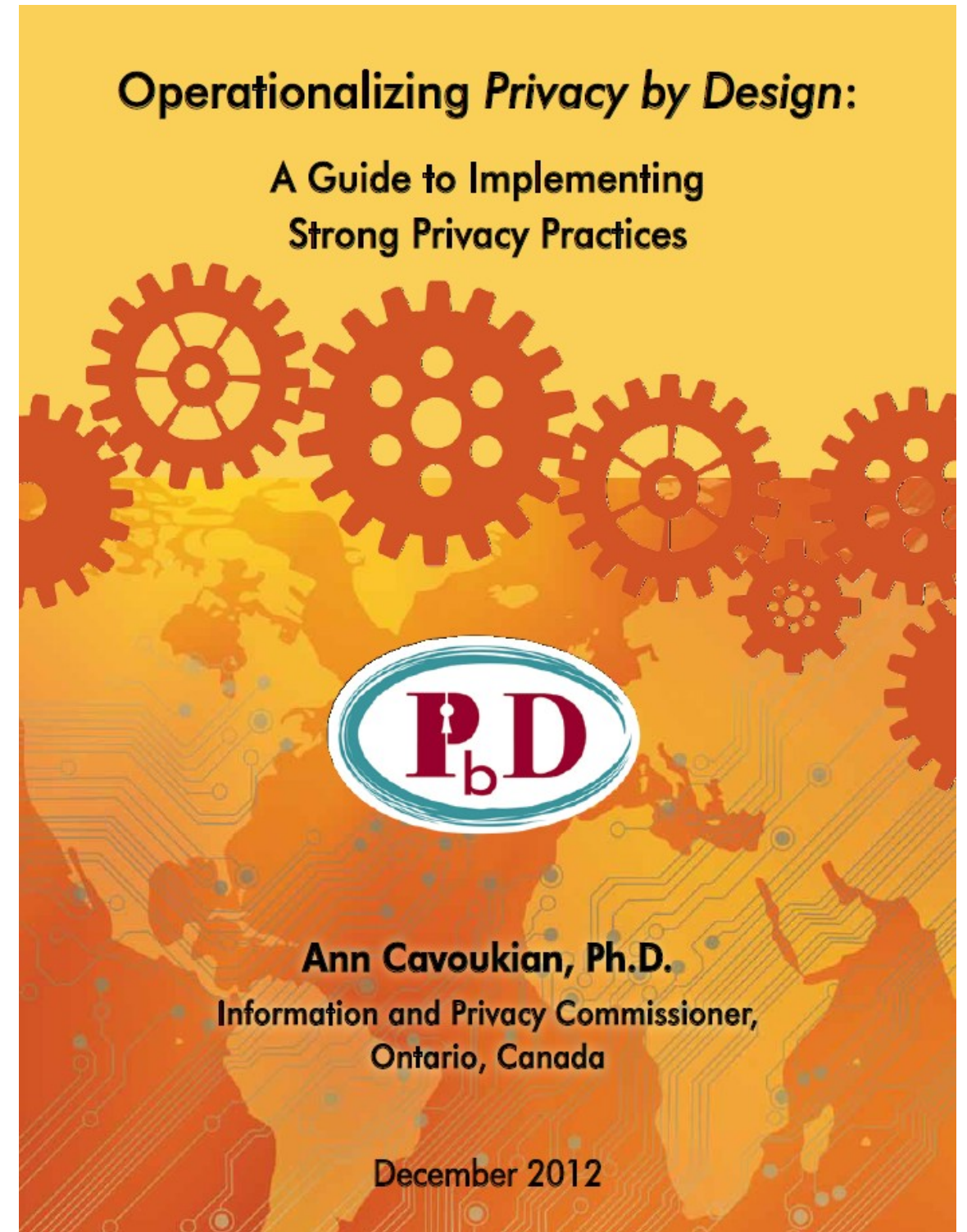
Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (*see over page*):



## 11 *PbD* Application Areas

- CCTV/Surveillance cameras in mass transit systems;
- Biometrics used in casinos and gaming facilities;
- Smart Meters and the Smart Grid;
- Mobile Communications;
- Near Field Communications;
- RFIDs and sensor technologies;
- Redesigning IP Geolocation;
- Remote Home Health Care;
- Big Data and Data Analytics;
- Privacy Protective Surveillance;
- SmartData.



## *General Data Protection Regulation*

Strengthens and unifies data protection for individuals within the European Union

Gives citizens control over their personal data and simplifies regulations across the EU by unifying regulations

Enforcement – Spring 2018

---



## Regulation

- The language of “Privacy/Data Protection by Design” and “Privacy as the Default” is appearing for the first time in a privacy statute, that was passed in the E.U.
    - Privacy by Design
    - Data Protection by Design
    - Privacy as the Default
-

---

*The Similarities Between  
PbD and the GDPR*

“Developed by former Ont. Information & Privacy Commissioner, Ann Cavoukian, Privacy by Design has had a large influence on security experts, policy makers, and regulators ... The EU likes PbD ... it’s referenced heavily in Article 25, and in many other places in the new regulation. **It’s not too much of a stretch to say that if you implement PbD, you’ve mastered the GDPR.**”

---

- 1. Big Data and privacy are *not* mutually exclusive:**
  - Data is one of the most valuable assets of any organization ;
  - Privacy is about *personal* information;
  - Consumer demands are creating additional pressures;
- 2. Proactive privacy drives innovation:**
  - It is entirely possible to achieve privacy in the Big Data era, while also using data analytics to unlock new insights and innovations to move an organization forward;
- 3. Innovation and privacy: One *can* have it all:**
  - Organizations will continue to apply data analytics to Big Data in order to advance their strategic goals and better serve their customers.

- **Public Perceptions of Privacy and Security in the Post-Snowden Era**
  - There is widespread concern about surveillance by both government and business:
    - **91% of adults agree that consumers have lost control over their personal information;**
    - 80% of social network users are concerned about third parties accessing their data;
    - 80% of adults agree that Americans should be concerned about government surveillance;

## *Embedded Systems and IoT*

The network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to enables services by exchanging data with the manufacturer, operator and/or other connected devices.

---



## 1) Wearable Computing:

- Everyday objects
  - i.e. Apple watch, Nymi Band

## 2) Quantified Self:

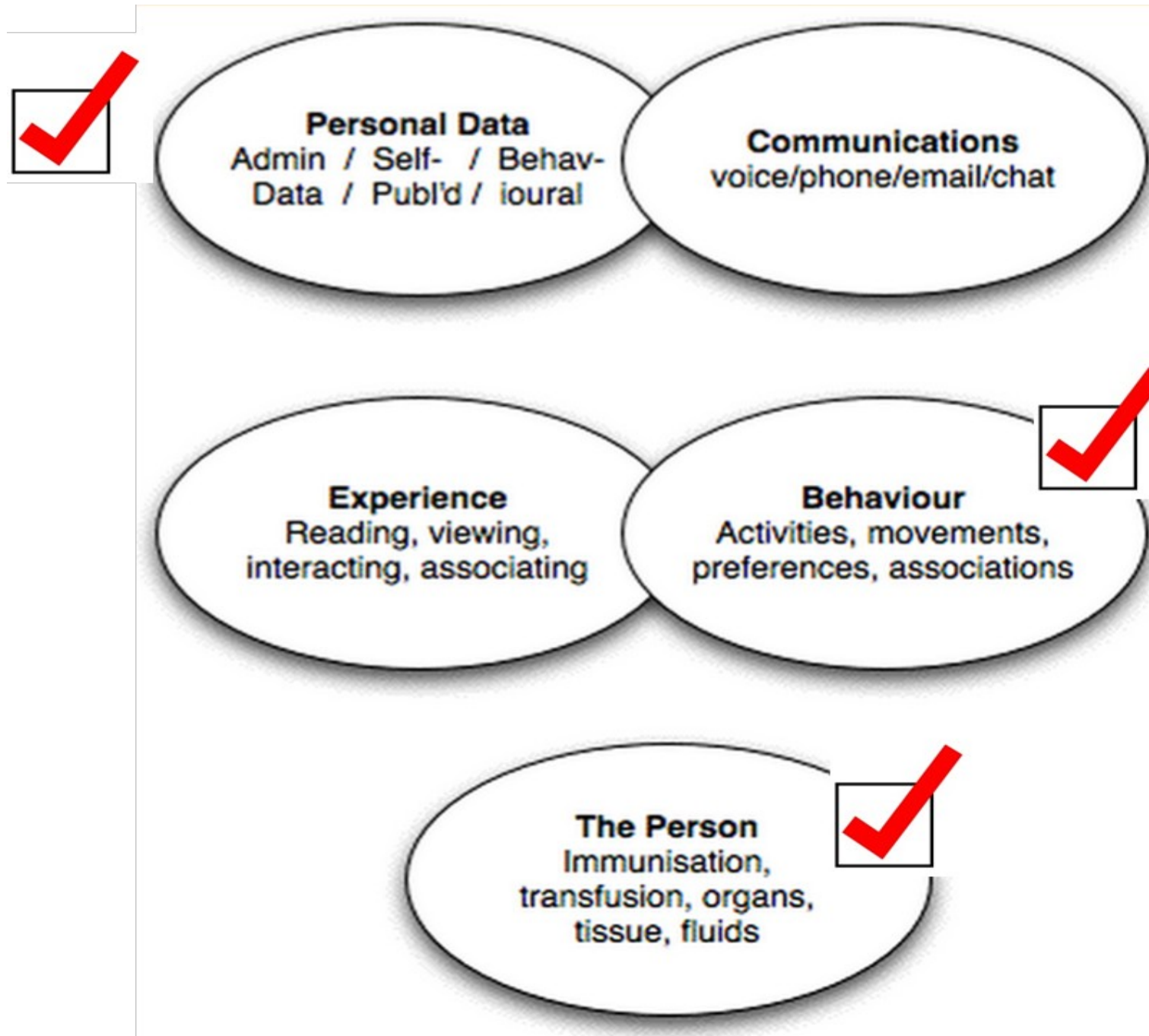
- Record information about one's habits, lifestyle and activities (Health, Fitness and sleep trackers)

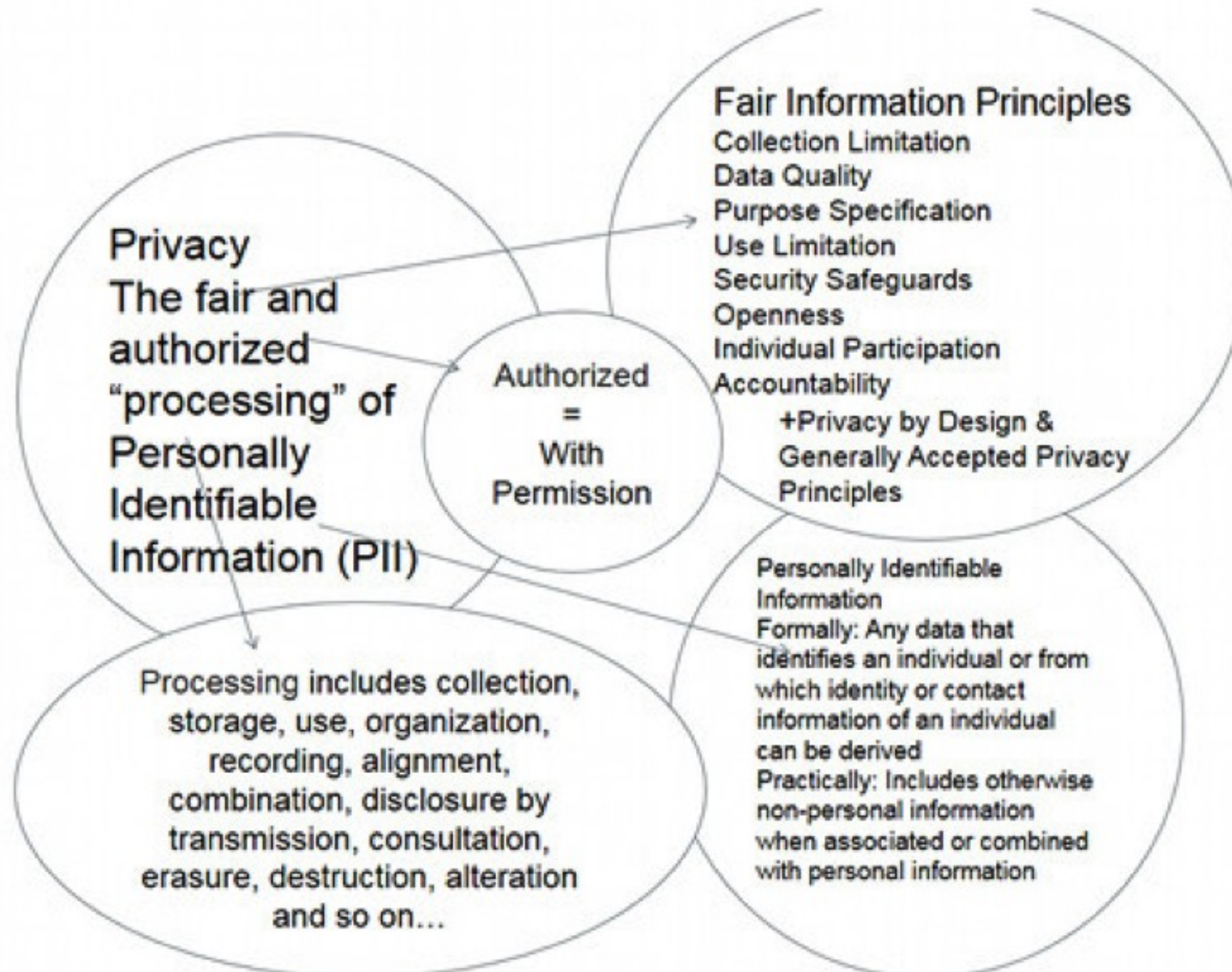
## 3) Home Automation:

- Computer controlled thermostats, light bulbs, smart meters, the smart grid, etc.
-

- The U.S. Federal Trade Commission (FTC) has expressed concerns with the risks associated with the Health Information collected by the Apple Watch and HealthKit platform;
- **FTC found that 12 mobile health and fitness app developers were sharing user information with 76 different parties;**
- The FTC would like to ensure that developers have the necessary safeguards to protect personal health information.

- **Third party monitoring removes control of one's information from the individual involved;**
  - The nature of the devices may make it more difficult to obtain consent before data collection begins;
  - Specific instances of data collection may not seem important on their own, but when aggregated, they can create a comprehensive picture of a person that may be extremely harmful to the individuals involved, especially in the hands of unauthorized third parties.
-







# *A Much-Needed Privacy Standard for the Internet of Things*

---

Suggestion:

Creating a common privacy standard will  
earn user trust in privacy and security;

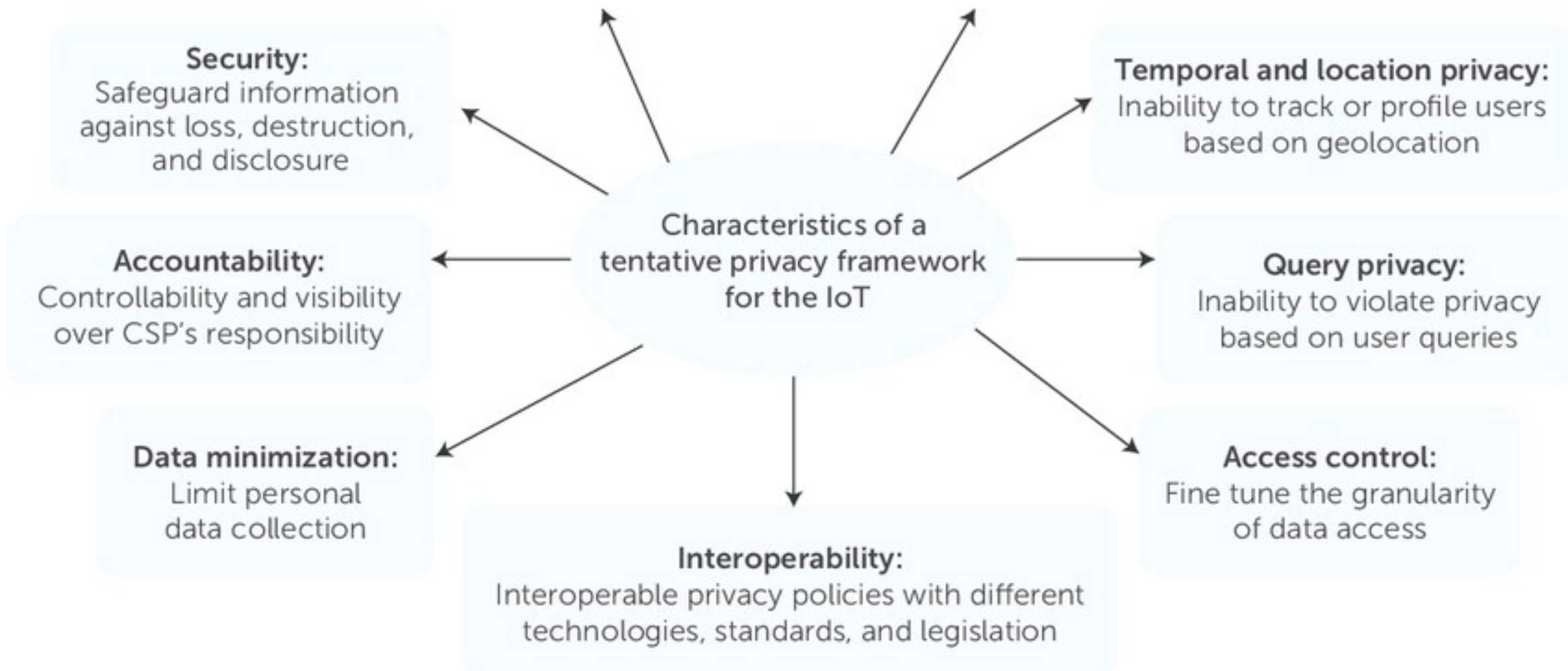
24 billion IoT devices before the decade is  
up;

---

- **Recommendations on the Internet of Things:**
    - **Make privacy the default setting ... follow Privacy by Design;**
    - Delete all raw data after processing;
    - Respect a user's self-determination over their own data, and seek consent in a user-friendly way;
    - Be transparent about how a user's data is being used;
    - When sensors are continuously collecting one's personal data, remind users of this surveillance activity;
    - Ensure that data published to social platforms remain private, by default;
    - Users should not be penalized for failing to consent;
    - Data should be De-Identified, except when necessary.
-

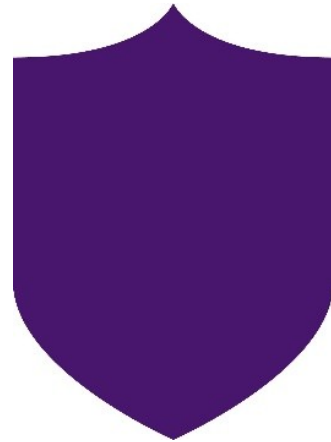
## Conference of Data Protection and Privacy Commissioners (2014):

- The value of Internet of Things (IoT) is not only in the devices, but in the services that arise from their use;
  - Connectivity is ubiquitous: it is the joint responsibility of all actors to ensure trust in connected systems : Transparency is Key;
  - Protection should begin from the moment the data is collected:  
**“Privacy by Design should be the key selling point of innovative technologies”**
  - Strong, active and constructive debate is necessary to overcome the huge challenges presented by the developers of IoT.
-



Porambage, Pawani & Schmitt, Corinna & Kumar, Pardeep & Gurto, Andrei & Ylianttila, Mika & Vasilakos, Athanasios. (2016). The Quest for Privacy in the Internet of Things. IEEE Cloud Computing. 3. 10.1109/MCC.2016.28.

## **Privacy and Security top of mind for both Design and Development of IoT Application**



**Authentication  
Access Restrictions  
Data Encryption and  
Secure Storage**



**User Transparency &  
Control  
Explicit User  
Consent  
Data Containment**



# Privacy and Security as the Default

## Wellness Data Read from Paired Peripherals

## User Authorization and Control

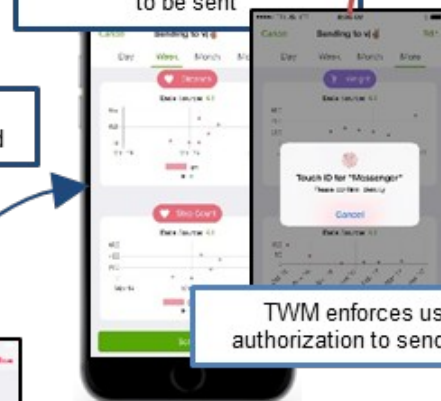
## File and Message Transfer

## Data Retention



Full visualization of all data to be sent

Read by TWM only when needed



TWM enforces user authorization to send data



End-to-end user-specific encryption: AES256

User relationships must be mutual for communication



7 day server lifetime

14 day device lifetime

TWM also purges all shared data if the relationship ends

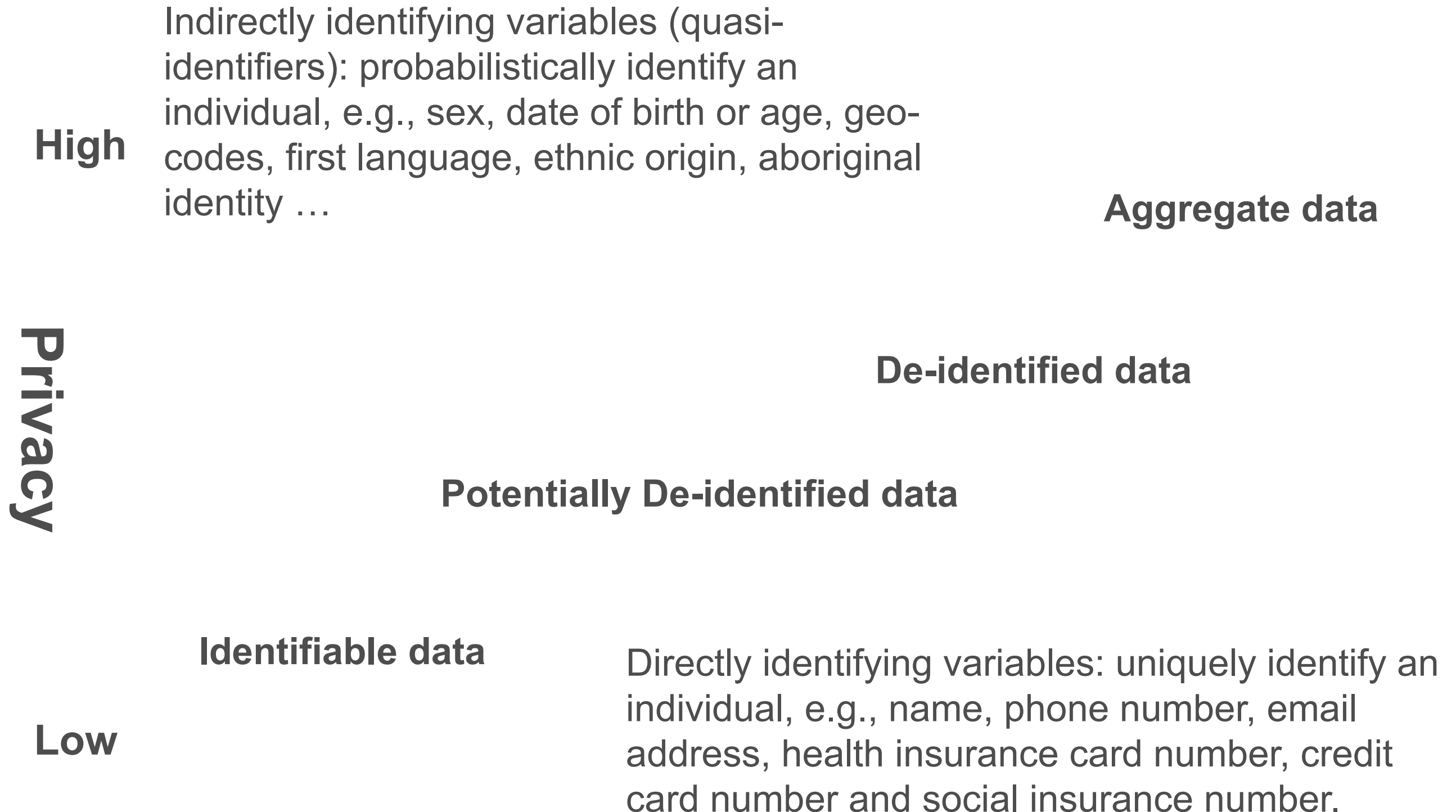
Privacy

Security

iOS enforces user authorization to access data

All data is encrypted in transit and at rest: it is only accessible when being read for display to the authorized user alone

- Data minimization is the most important safeguard in protecting personally identifiable information, including for a variety of research purposes and data analysis;
  - The use of strong de-identification techniques, data aggregation and encryption techniques, are absolutely critical.
-



- If proper de-identification techniques and re-identification risk management procedures are used, re-identification becomes a very difficult task;
  - While there may be a residual risk of re-identification, in the vast majority of cases, de-identification will strongly protect the privacy of individuals when additional safeguards are in place.
  - Personally identifiable data must be rendered non-identifiable;
  - Strong de-identification protocols must be used in conjunction with a risk of re-identification framework.
-

- De-Identification and data minimization are among the most important safeguards in protecting personal information;
  - You should not collect, use or disclose personal information if other data (i.e., de-identified, encrypted or obfuscated) will serve the purpose;
  - The use of strong de-identification, aggregation, and encryption techniques are absolutely critical, and readily available.
-



- Internet of Vehicule
- Non Intrusive Load Monitors (NILM)

- Refers to the vehicles to vehicles, vehicles to roads, vehicles to people, vehicles to sensing equipment interaction, implement dynamic mobile communication system of the vehicles with the **public network**.

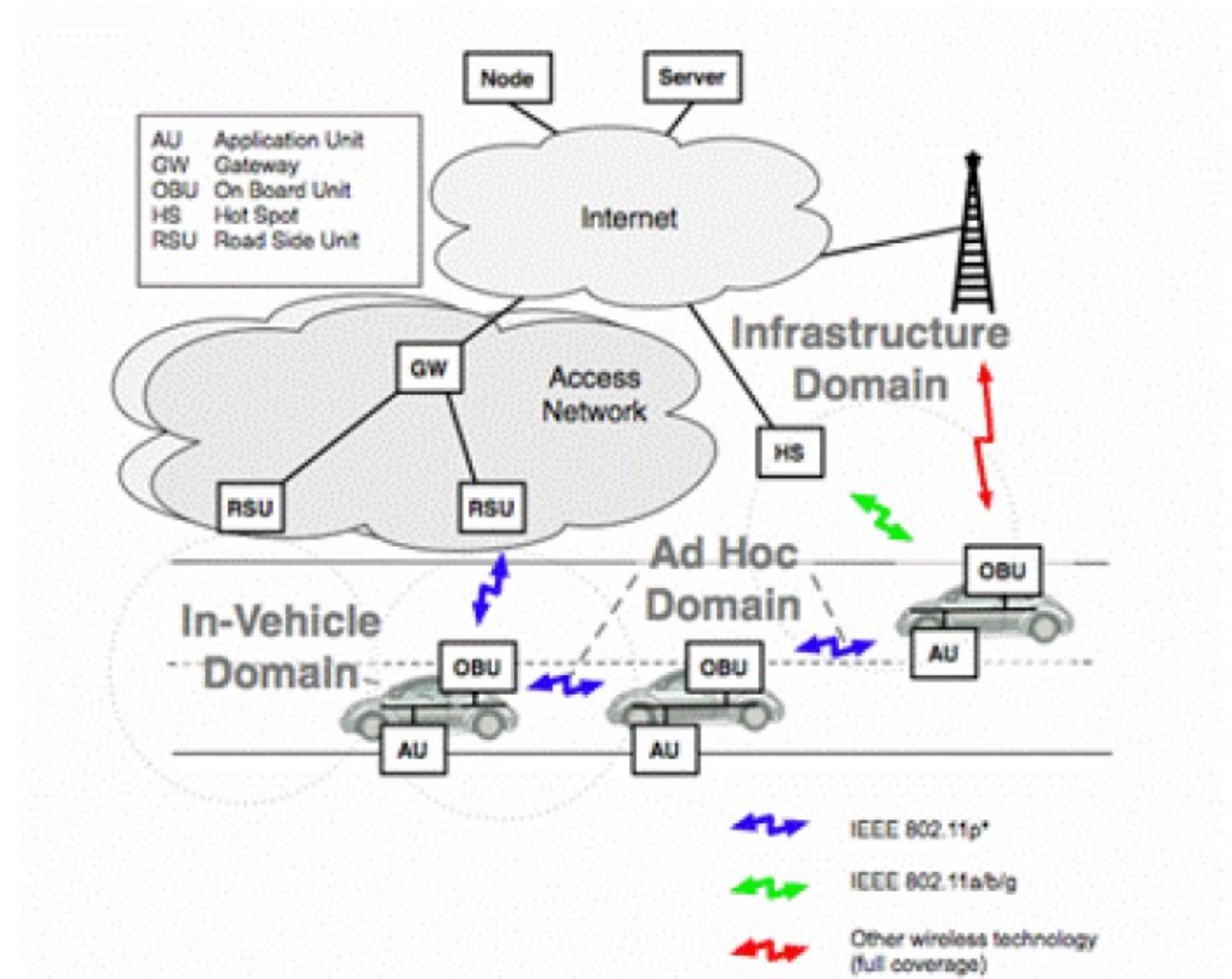
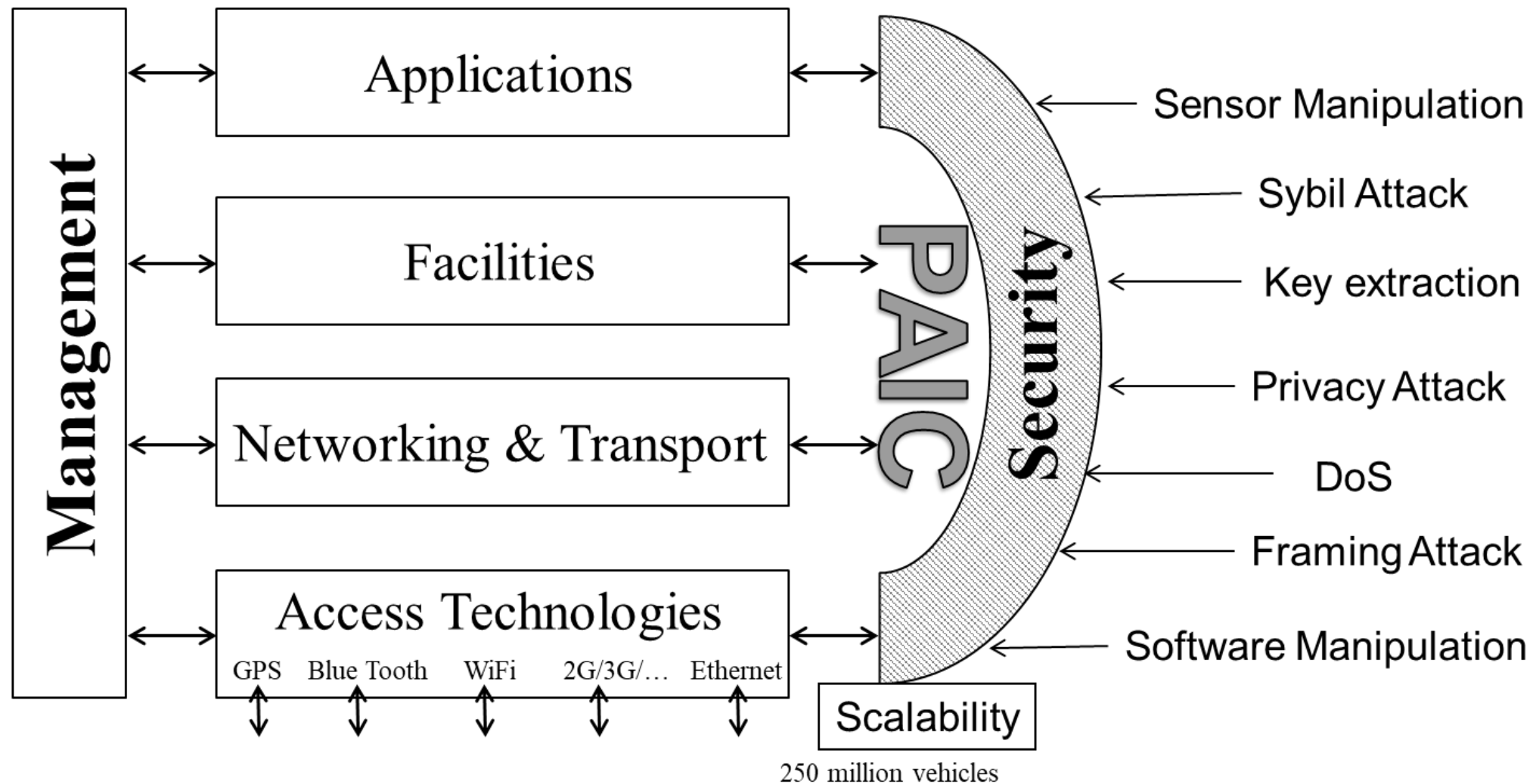




Figure 16: Draft Reference Architecture of the Car2Car Communication Consortium

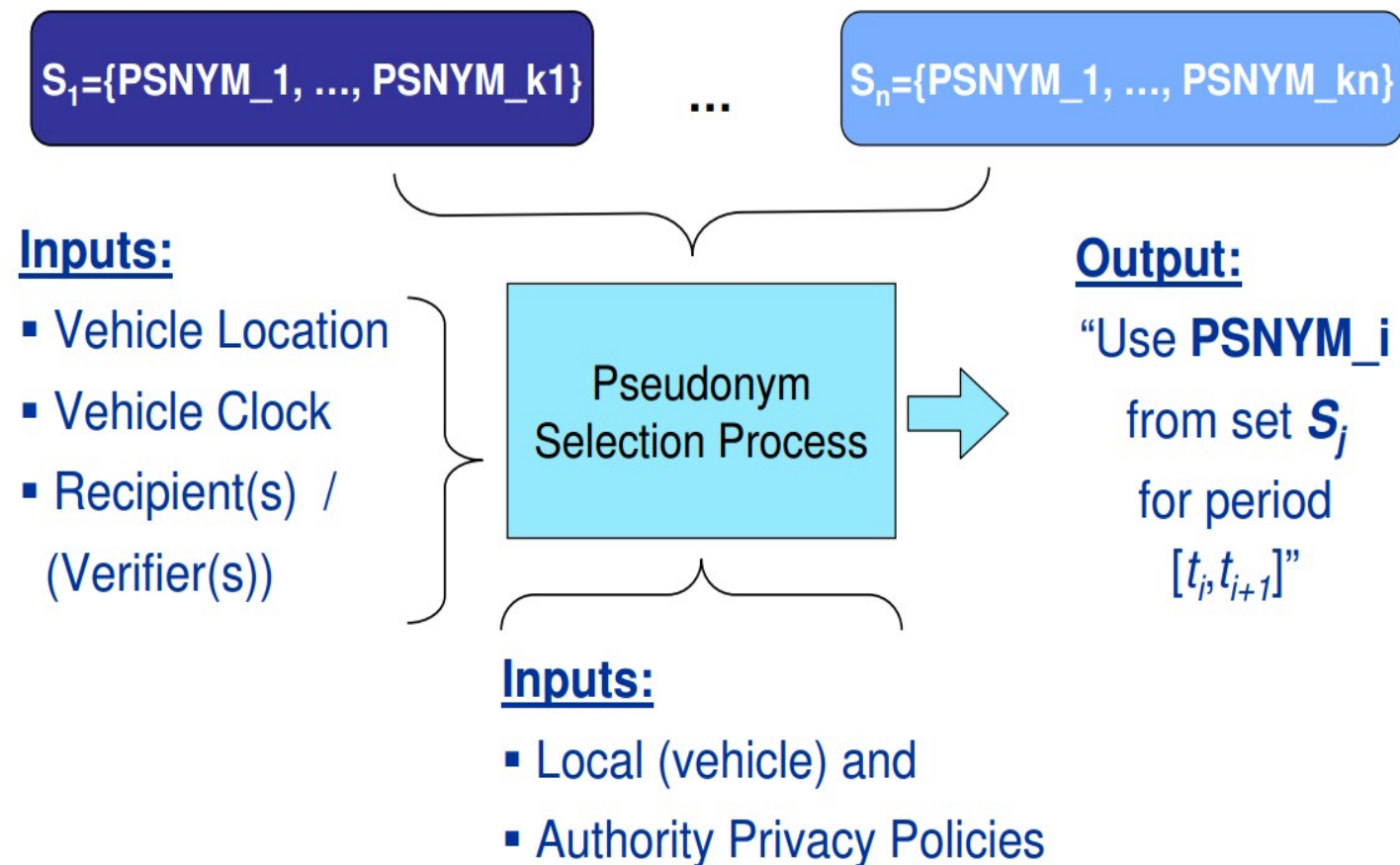


## Privacy Issues:

- Untraceability: vehicle's action should not be traced
- Unlinkability: vehicle's identity should not be identified
  - Weak Anonymity: vehicles should not be identified from the messages they send
  - Strong Anonymity: no message are linkable vehicles
- Location Privacy
  - Location of a vehicle over time should remain private

## Privacy Risks:

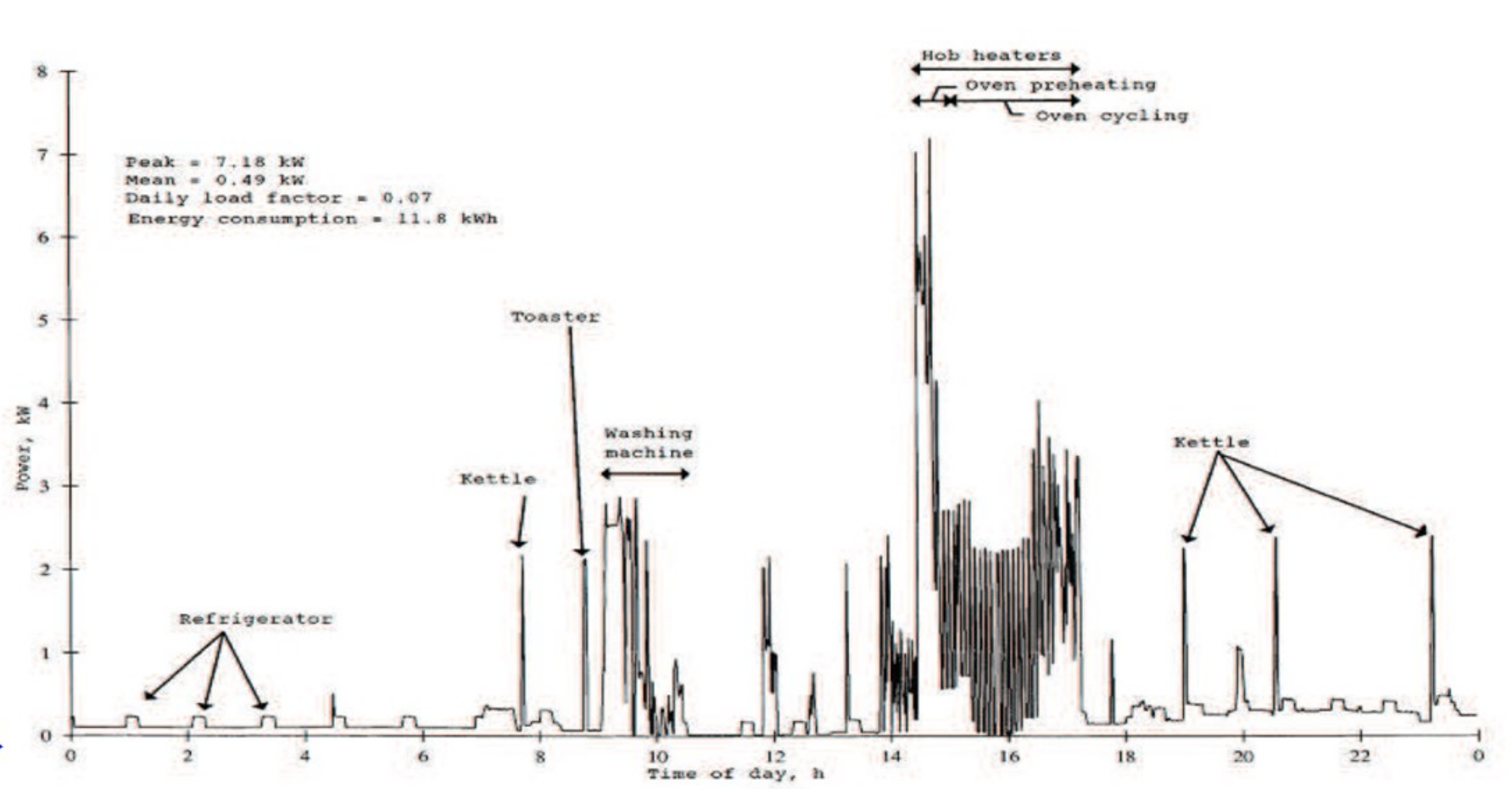
- Two types
  - Real time (where the vehicle is presently located) or
  - Historic (where the vehicle was at a certain time on a certain day).
- Locate and track specific vehicles.
  - Location  unique vehicle identifier (or series of identifiers)  an individual (a registered owner).



Not allow for message sender to be identified.

Difficult to link two or more messages to a specific node.





- Two disaggregation algorithms
- Combinatorial Optimization (CO)
  - Factorial Hidden Markov Model (FHMM)



Which  
When  
How Much

Behavioral Privacy



The passage of the EU’s GDPR ... is bringing PbD to top of mind as personal operations are adjusted to comply with new GDPR rules...In short, the GDPR has already given PbD new visibility and vigor. Positive-sum change is on its way – not just to Europe, but across the world.

---

- 1 Proactive not reactive;  
Preventative not remedial
- 2 Privacy as a default setting
- 3 Privacy embedded into design
- 4 Positive-sum, not zero-sum
- 5 End-to-end security - full data  
lifecycle protection
- 6 Visibility and transparency - keep  
it open
- 7 Respect for user privacy - keep it  
user-centric

## What it means to Nymi

**People should not have to sacrifice their privacy in order to use and benefit from technology.**

The principles of Privacy by Design provide a framework for how technology should be approached to reduce privacy risk for the end user. With these principles, we pioneered a safer way to utilize the security benefit of biometrics by minimizing the amount of personal data that is processed and retained in our solution. We also deviated from the status quo that centralizes storage of biometrics, and instead, designed a way for people to remain in possession of their data at all times.

- Privacy and security risks are best managed by proactively embedding the principles of *Privacy by Design*;
- Focus on prevention: It is much easier and far more cost-effective to build in privacy and security, up-front, rather than after-the-fact, reflecting the most ethical treatment of personal data;
- Abandon zero-sum thinking – embrace doubly-enabling systems: Privacy and Security; Privacy and Data Utility;