

# Round Table Introduction

Irma van der Ploeg

## Key Questions

# Areas of concern

- Tracking and tracing – loss of free movement and anonymity  
Ubiquitous identification : visibility anytime, any place.
- Data accumulation and retention, connecting databases, compiling extensive personal datasets, explosion of amount of data on behavior, movements, and preferences; profiles unprecedented in detail, precision, availability, etc.
- Nature of data collection – integrity of the person  
Body sensors, biometrics from a distance, covert data capture, 'networked persons'
- Changing relation to (built) environment – the quality of our 'being in the world'  
Living between smart objects, sensing homes, watching walls, communicating lampposts
- Opacity / transparency – control, consent, accountability

# Different organisation levels of technology raise different issues

- **Artefacts**

Specifications of tags, Item level tagging (life cycle, mobility, personal nature of item), types of sensors, pattern recognition algorithms

- **Configurations**

Connecting various technologies, multi modal , interoperability, and system integration, comm. Networks, remote sensing and access, database architecture, smart homes vs street surveillance.

- **Governance**

Rules & regulation, audit & accountability, ownership of data, stakeholder involvement

- **Countermeasures**

Security features, PETs , PbyD, User Centered and Value Sensitive Design, Retention vs deletion of data

## RFID pill to act as your doctor on demand at walking events

Filed in archive [Sports](#) by [gautam](#) on July 25, 2008



[Photo courtesy of iStockphoto, Image# 4707225](#)

Every year hundreds of people participate in various marathon and walking events in support of some cause but these people are not athletes but people from every walk of life and there is always a chance that they might fall ill since they are not used to such strenuous physical activity in everyday life. At times it might also turn out to be life threatening and in order to avoid such situations, Dutch researchers at Radboud University have created an **RFID pill which would keep a watch on the temperature** of participating people.

Comprising of an **RFID tag and thermometer**, the **RFID pill needs to be swallowed** before the start of any physical activity and with the aid of event processing technology it becomes easier to **monitor body temperature as a signal is send every ten seconds**. In case the temperature shoots up an onsite medical team is **alerted** which is able to offer medical assistance within no time. A pilot has already been conducted at International Four Day Marches Nijmegen and hopefully it may soon find a place in other events around the world too.

# Iris on the Move

(<http://www.sarnoff.com/products/iris-on-the-move>)



Utilizing iris recognition, Sarnoff has developed an innovative solution that **combines security, high-throughput and unprecedented ease of use**. Iris on the Move® (IOM) is the only **biometric identification** system that **performs at the speed of life**—capable of capturing an iris image at a distance while the individual is in motion.

Iris on the Move is available in three unique configurations that fit a wide range of applications.

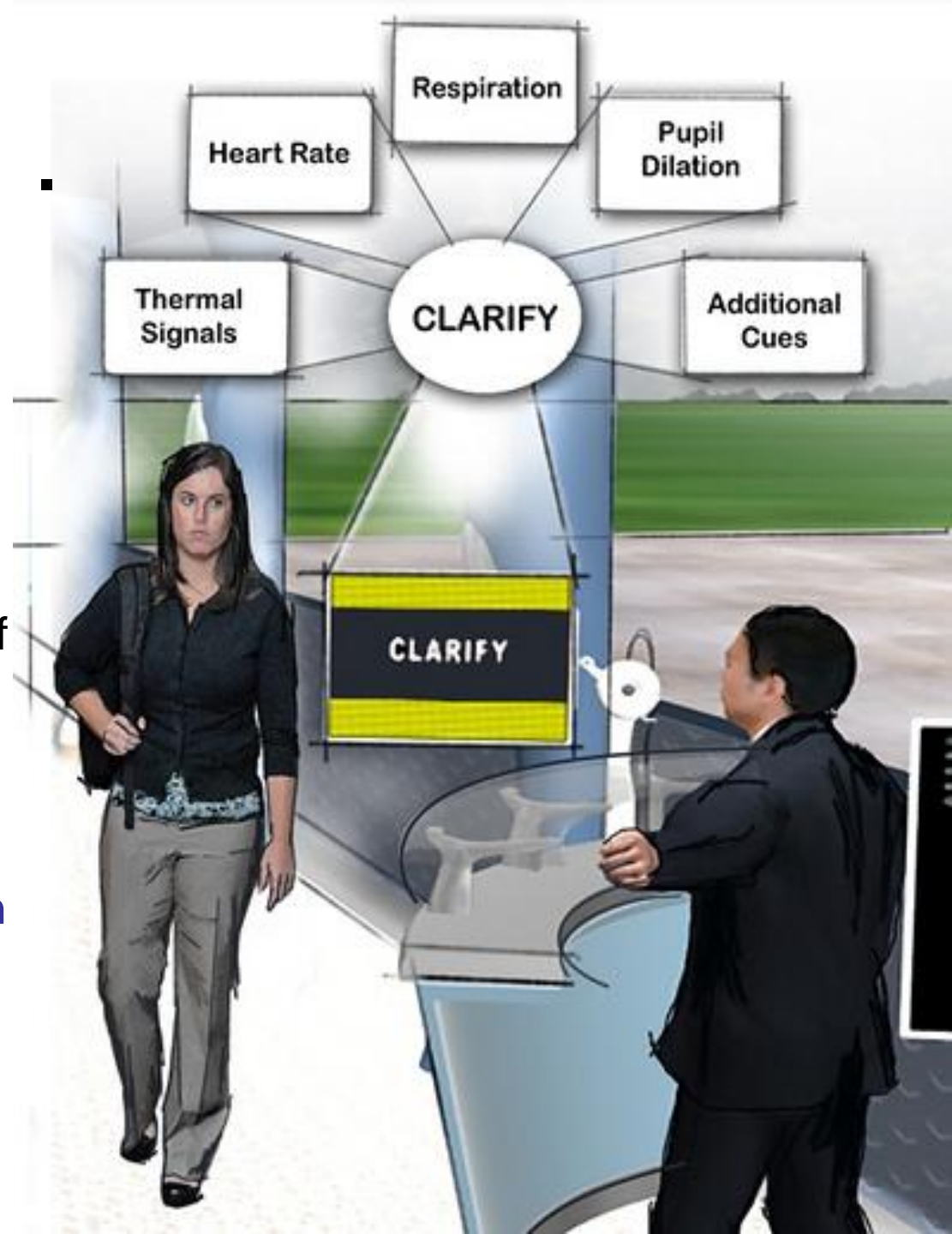
- **Portal System:** With a throughput speed of 30 people per minute, the Portal suits applications that require the processing of large numbers of people in a short amount of time

- **Drive-Through System:** Using Pan-Tilt-Zoom technology to capture iris images at varying heights, this system eliminates the need for drivers to exit their vehicles

- **Compact System:** With a miniaturized design, the system is ideal for areas where space is an issue while still maintaining the ability to capture iris images from moving subjects

## 'Hostility Detector'

**FAST** (Future Attribute Screening Technologies), a system the U.S. Department of Homeland Security (DHS) is testing that measures **facial expressions, pupil dilation, pulse/breathing rates, and skin temperature** to determine if someone has **hostile intent**.



# DHS Impression of the 'mindreader' in action.



# FAST: 'Anxiety detector' / 'terrorist spotter' / 'the new polygraph' ?



Or covert medical exam without consent?

“The DHS says that [privacy] is **not a problem, since the data is never linked to an identity** and is only used to help officers decide if a suspicious person should be interviewed.”

(Illustrating the relevance of: Article 29 Data Protection Working Party (2007), *Opinion 4/2007 on the Concept of Personal Data*, June 20, Brussels)

# Tasks ahead

## *Background doc*

- Meeting 1 :
  - Precise topic delimitation & formulation key questions

## *1st draft brief*

- Meeting 2:
  - Assessing positions and arguments concerning these issues in relevant EU docs
  - Identification of issues not (adequately) addressed

## *2nd draft brief*

- Meeting 3:
  - Developing position on these issues

## *Final draft*

# Q1

*A Is it productive to restrict our FG to the particular subset of embedded technologies/applications involving human bodily identification and monitoring?*

*And*

*B What would be the exemplary applications?*

# Q2

- A How are systems targeting the human body **different** from an ethical/social/political point of view?
- B What type of systems and applications targeting the human body gives rise to **which issues** in particular, and why?
- C What specific **new vulnerabilities** emerge with/from these systems, threatening whom in particular?
- D What kind of practices are enabled by data processing and **profiling using or producing body data** generated by Aml systems?

Possibilities here include:

- ◇ Biometric data *put on* RFID chips (e.g. e-passports) in ID-documents and cards
- ◇ Biometric identification/authentication in Aml systems
  - for public security reasons , e.g. acces control/crime control in public events; continuous authentication in securing critical infrastructures (e.g. ACTIBIO)
  - for system/network/information security reasons
  - for convenience reasons (intuitive interfaces)
- ◇ RFID chips *linked to* body data (index to retrieve medical records),  
and  
possibly *implanted in* bodies (Verichip)
- ◇ Body monitoring sensors to identify `aggression`, `hostility`
- ◇ Body monitoring sensors *combined with* RFID
  - for safety reasons in work environments (The Indian mine workers example), or home environments ('safe living' for the elderly), public sports events (marathon runners' pill)
  - for medical reasons in health care (e.g. telemonitoring)
  - for identification/authentication purposes (see above)
- ◇ Health risk profiling using RFID data

# Q3

- 3 To what extent is covert capture of personal and identifying data, or secondary use of such data, for security and crime prevention interests justifiable? Where, at what point and by whom should such judgements be made?
- 2 To what extent is covert capture of personal and identifying data in Embedded Systems and Aml required for convenience and usability reasons? Can this be a matter of detail and nuance rather than an it being an either/or issue?
- 5 Are there prevalent reasons NOT to have identification/authentication procedures disappear into invisibility?
- 4 How should issues of transparency, consent, and possibilities for democratic control be negotiated in such systems?
- 6 Are there viable technical options for reasonable balances between convenience, security and transparency?