

# Safeguards in a World of Ambient Intelligence - First Expert Workshop

Fraunhofer Institute Systems and Innovation Research, Karlsruhe

EC/JRC - Institute for Prospective Technological Studies, Seville

VTT Electronics, Oulu

Vrije Universiteit Brussel - Research group Law Science Technology & Society

Trilateral Research and Consulting, London

## Agenda

### Morning

- 09:00** Introduction (Michael Friedewald)
- 09:45** Review of Aml projects and scenarios: the analytical framework (Elena Vildjiounaite)
- 10:10** Results of the Review (Elena Vildjiounaite) – subsequent discussion
- 10:45** Coffee Break
- 11:00** Threats in future Ambient Intelligence Application: First evidence (Michael Friedewald) – subsequent discussion
- 11:30** First Results of the Legal Analysis (Wim Schreurs, Michiel Verlinden) – subsequent discussion

### Afternoon

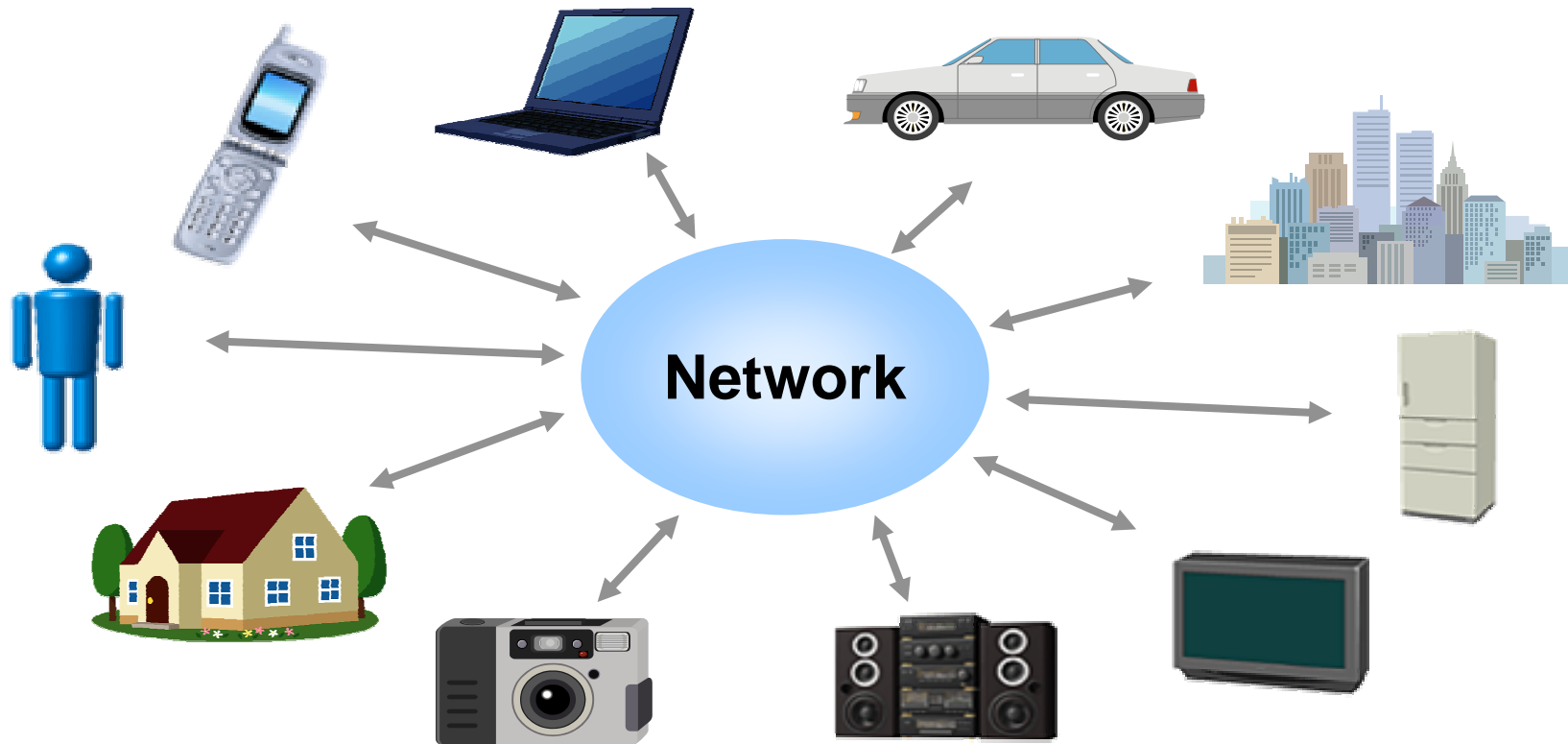
- 12:15** Lunch Break
- 13:30** Dark scenarios Part 1: Identification of major issues and drivers (post-it session) (Ioannis Maghiros, Yves Punie)
- 15:00** Coffee Break
- 11:00** Dark scenarios Part 2: Clustering and prioritisation (Ioannis Maghiros, Yves Punie)
- 16:30** Consolidation, Conclusion, Next Steps
- 17:30** End of the Workshop

# Introduction to SWAMI

## Objectives of the Workshop

Michael Friedewald

## Introduction - Future Aml Information Society

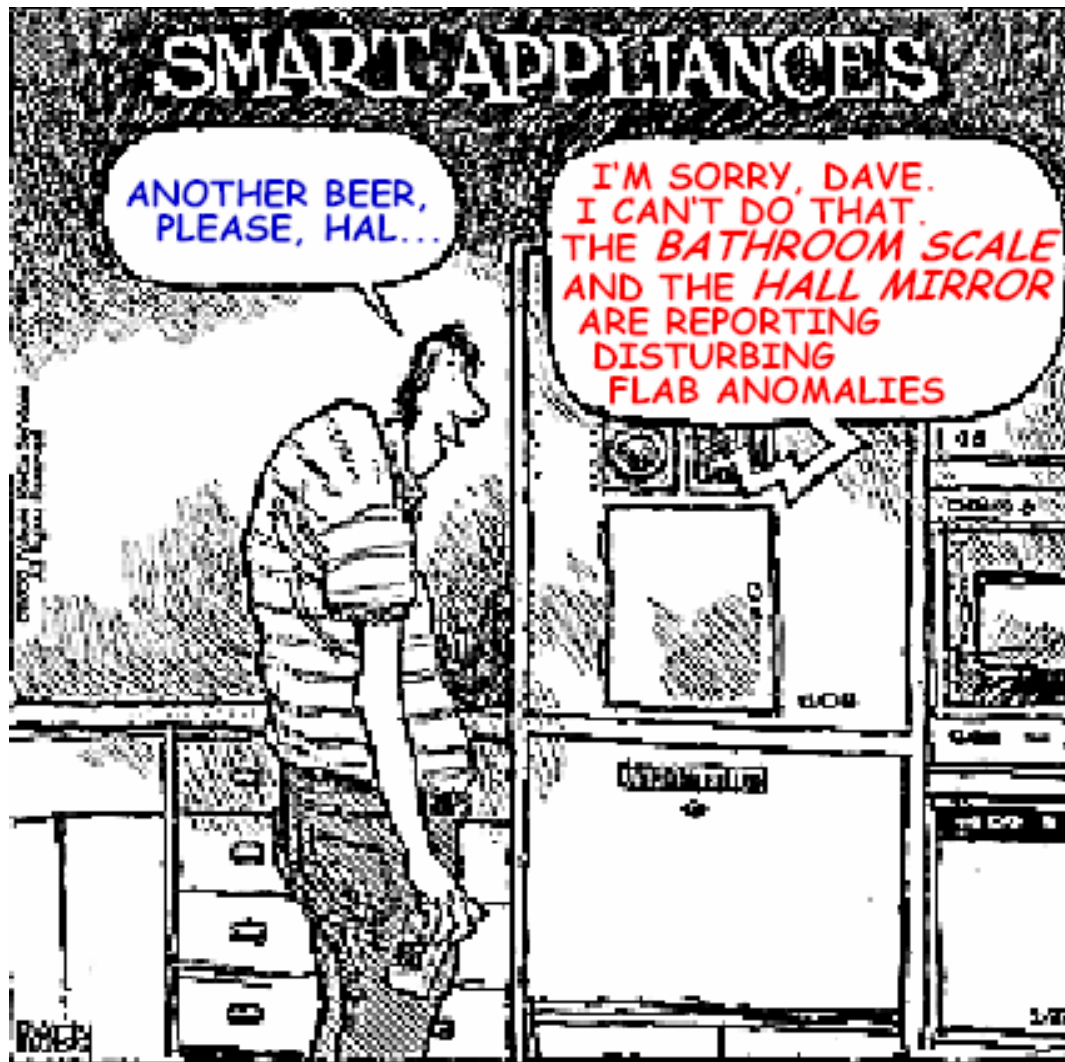


There are not only chances but also risks associated with the Aml Information Society

## **Why consider risks anyway? Why not think positively?**

### **Little emphasis on ambivalence of Ambient Intelligence**

- Scenarios depict typical successful users in a perfect world ⇔ struggle, uncertainties, irregularities, malfunctions...
- Normative claims ⇔ Real technological development
- Disappearing computing ⇔ taken for granted ness (physical versus mental)
- Invisible computing ⇔ Human-centred computing
- Blurring of the boundaries between artefact and function
- Ownership, usage, domestication
- Little consideration of power relations between actors
- Difference between intended and real use



Cartoon by  
Jeff MacNelly

## **Why consider risks anyway? Why not think positively?**

### **Little emphasis on ambivalence of Ambient Intelligence**

- Scenarios depict typical successful users in a perfect world ⇔ struggle, uncertainties, irregularities, malfunctions...
- Normative claims ⇔ Real technological development
- Disappearing computing ⇔ taken for granted ness (physical versus mental)
- Invisible computing ⇔ Human-centred computing
- Blurring of the boundaries between artefact and function
- Ownership, usage, domestication
- Little consideration of power relations between actors
- Difference between intended and real use

**Crucial: How can the privacy, identity and security of the Aml user be protected?**

## **Facets of „Privacy“**

### **Bodily Privacy**

- Protection of person's physical selves from invasion

### **Territorial Privacy**

- Setting limits in intrusion into domestic/workspace/public sphere

### **Privacy of communications**

- Security Phone Calls, Letters, E-Mails, etc.

### **Informational Privacy**

- Rules for collection and handling of personal data ➡ data protection



## Privacy Boundaries and crossing of privacy boundaries

### Natural

- Physical limitations (closed doors)

### Social

- Confidentiality of physicians, lawyers, ...

### Spatial / Temporal

- Family vs. Work, adolescence vs. midlife

### Smart Appliances

- „Spy“ in your own home

### Family Intercom

- Grandma knows you're at home
- Parents know where children are

### Consumer Profiles

- Record time and place of activity

## **The crucial questions?**

### **Collection Scale**

- To what extent is my life visible to others? Who can view my data?

### **Collection Manner**

- How obviously is data collected?

### **Collection type**

- What type of data is recorded?

### **Motivation**

- What are the driving forces?

### **Accessibility**

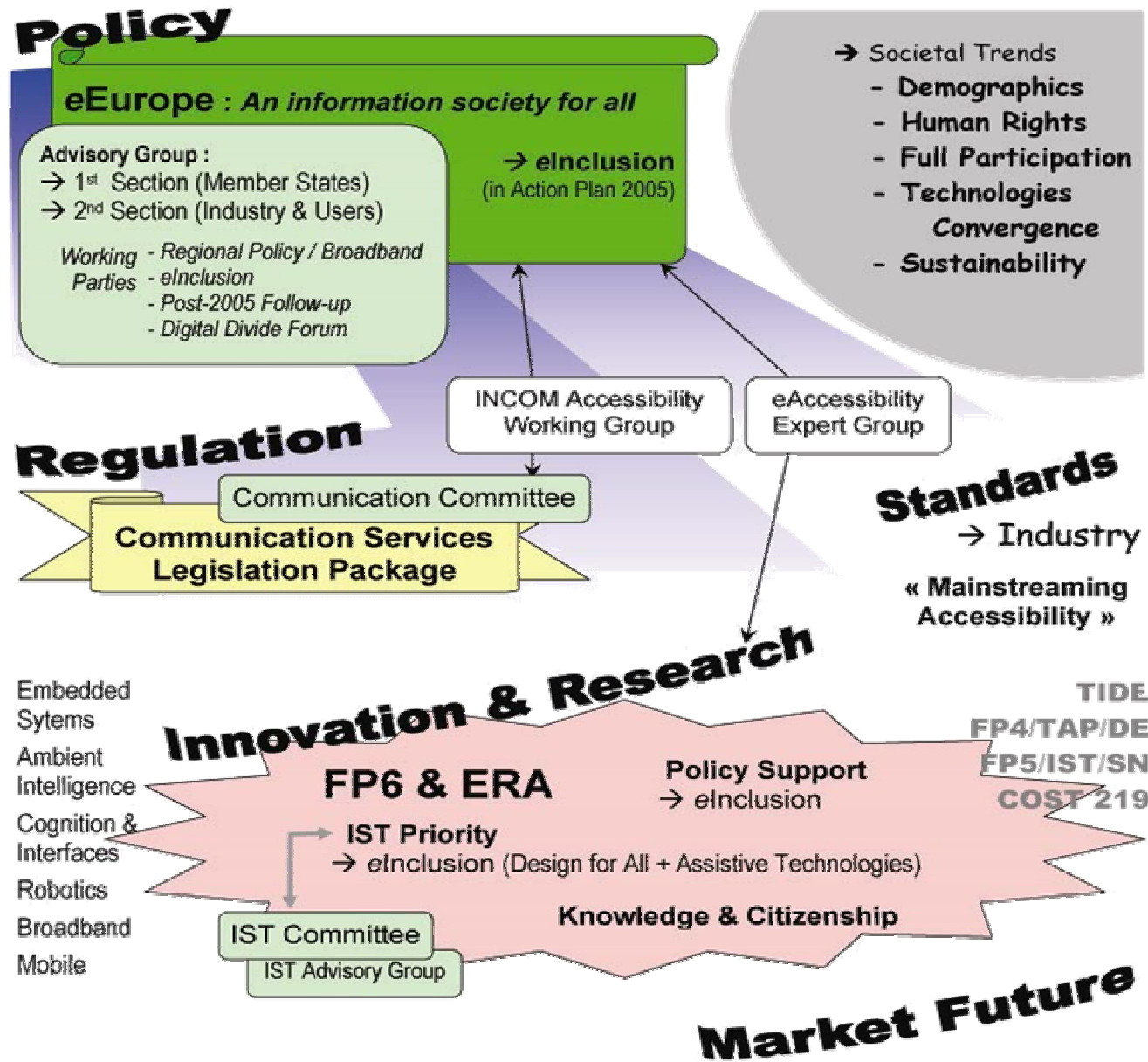
- How does one find anything in this data?

## **Privacy Excuses**

(after Langheinrich 2004)

- Optimists:** “All you need is really good firewalls.”
- Self-Regulation:** “It's maybe about letting them find their own ways of cheating, you know...”
- Not my problem:** “For my colleague it is more appropriate to think about privacy issues. It's not really the case in *my* case.”
- Gets in the way:** “Somehow privacy also destroys this, you know, sort of, like, creativity...”
- Impossible:** “I think you can't think of privacy when you are trying out... it's impossible, because if I do it, I have troubles with finding [a] Ubicomp future”
- Thus:** **Ways have to be found to build efficient, acceptable and flexible Safeguards for a World of Ambient Intelligence**  
➔ **An issue on the agenda of the European Commission**

# SWAMI Safeguards in a World of AMbient Intelligence



Source: EC, DG INFSO 2005

First SWAMI Expert Workshop, Brussels, 1 June 2005

## Goal of SWAMI

### Analysis

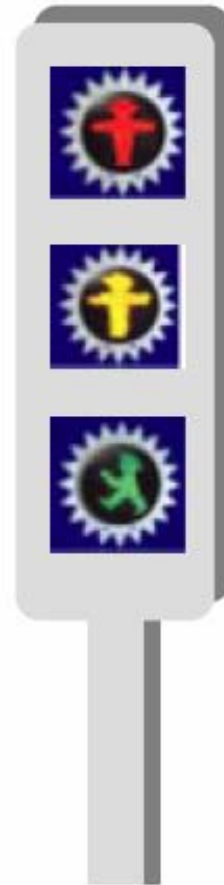
#### **Threats for the active party**

- eavesdropping of data
- unauthorised changing of data
- denial of service

#### **Threats for the passive party**

- threats to data privacy
- threats to location privacy
- ....

### Assessment



### Recommendation

- technical measures
- organisational measures
- legal measures
- research agenda
- ...

## Approach

1. To identify the social, legal, organisational and ethical implications related to *privacy, anonymity, manipulation and control, and identity*.
2. To *create and analyse “dark” scenarios* on Aml that highlight and detail the key socio-economic, legal, technological and ethical risks related to identity, privacy and security.
3. To identify *research and policy options* on how to build into Information Society services and systems the safeguards and privacy enhancing mechanisms needed to ensure user control, user acceptance and enforceability of policy in an accessible manner.



Interdisciplinary Approach

## **Step 1: State-of-the-art-overview**

- 1. Review existing literature (scenarios, foresight studies, roadmaps) and projects on relevant aspects of Ambient Intelligence - comparison of EU vs. US/Japan**
- 2. Describe prospects and benefits of Aml in important fields of applications and identify important issues re. privacy, identify, safety**
  - Home
  - Health
  - Shopping and Commerce
  - Mobility, travel, nomadic
  - Office Work
  - Learning
  - Emergency Management
- 3. Discussion and validation of results at first workshop with external experts**  
**Identification of main factors for scenarios development**  
**Rest of today**

## **Step 2: Development of “Dark Scenarios”**

### **1. Objective**

- Highlight vulnerabilities and risks of Ambient Intelligence with regard to identity, privacy, security.
- Highlight Social, economic, legal, technological and ethical implications

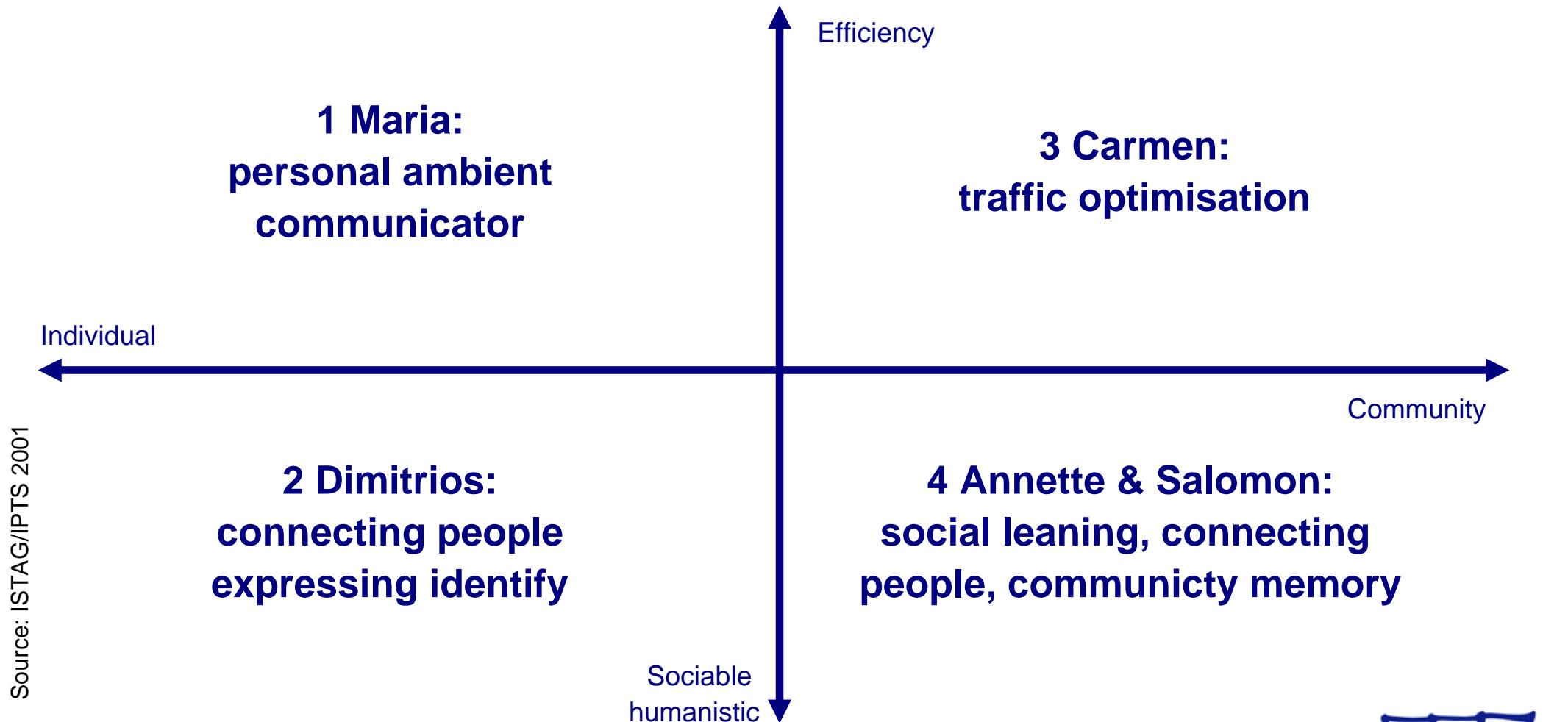
### **2. Dark scenarios = Worst case/undesirable scenarios**

- Identification of main axes for scenario in expert workshop
- Development of 4-5 contrasting scenarios with the combination of two axes
- Inclusion of cross-references to projects that are relevant to scenarios
- Identification of legal implications

### **3. Result: Characterisation of “The dark side of Ambient Intelligence”**



## Example: ISTAG Scenarios on Aml in 2010



## **Step 3: Building policy options**

### **1. Objective:**

**Formulate and consider the possibilities to overcome the problematic aspects of Ambient Intelligence**

### **2. Compare bright and dark side of Aml ➔ Detection of lacunae in existing European framework**

### **3. Considerations of the feasibility of privacy enhancing mechanisms**

### **4. Presentation and discussion of results in the second workshop with external experts and stakeholders**

**When: November 2005**

## **Success of SWAMI relies on the participation of stakeholders**

- **Policy makers**

- European Commission
- IST Advisory Group
- ESDIS (HLG on Employment and Social Dimension of the IS)

- **Technology developers**

- Aml projects on European and national level
- Agencies
- Industry

- **Civil society constituencies**

- Consumer protection
- Non Government Organisations
- Media

## Agenda

### Morning - Validation

- 09:00** Introduction (Michael Friedewald)
- 09:45** Review of Aml projects and scenarios: the analytical framework (Elena Vildjiounaite)
- 10:10** Results of the Review (Elena Vildjiounaite) – subsequent discussion
- 10:45** Coffee Break
- 11:00** Threats in future Ambient Intelligence Application: First evidence (Michael Friedewald) – subsequent discussion
- 11:30** First Results of the Legal Analysis (Wim Schreurs, Michiel Verlinden) – subsequent discussion

### Afternoon - Preparation of scenarios

- 12:15** Lunch Break
- 13:30** Dark scenarios Part 1: Identification of major issues and drivers (post-it session) (Ioannis Maghiros, Yves Punie)
- 15:00** Coffee Break
- 11:00** Dark scenarios Part 2: Clustering and prioritisation (Ioannis Maghiros, Yves Punie)
- 16:30** Consolidation, Conclusion, Next Steps
- 17:30** End of the Workshop