Minutes of the First Expert Workshop on „Safeguards in a World of AMbient Intelligence“ (SWAMI)

Fraunhofer Institute Systems and Innovation Research

Participants:

- Consortium:
  Petteri Alahuhta (VTT Electronics), Bernd Beckert (Fraunhofer ISI), Michael Friedewald (Fraunhofer ISI), Serge Gutwirth (VUB), Ioannis Maghiros (EC/JRC-IPTS), Yves Punie (EC/JRC-IPTS), Wim Schreurs (VUB), Els Soenens (VUB), Michiel Verlinden (VUB), Elena Vildjiounaite (VTT Electronics), David Wright (Trilateral)
- External Experts:
  Laurent Beslay (European Data Protection Supervisor, Brussels, BE), Ian Brown (Foundation for Information Policy Research, London, UK), Markus Hansen (Independent Data Protection Centre Schleswig-Holstein, Kiel, DE), Mario Hoffmann (Fraunhofer SIT, Darmstadt, DE), Pertti Huuskonen (Nokia Research Centre, Tampere, FI), Achilles Kameas (Research Academic Computer Technology Institute, Patras, GR), Spyros Lalis (University of Thessaly, GR), Miriam Lips (Tilburg University, NL), Irene Lopez de Vallejo (University College London, UK), Gregory Neven (KU Leuven, BE), Albrecht Schmidt (University Munich, DE), Stefaan Seys (KU Leuven, BE), Michael Vanfleteren (KU Leuven, BE)

Authors: M. Friedewald,
B. Beckert
P. Alahuhta
Y.Punie
Institution: Fraunhofer ISI
phone: +49 721 6809-146
Date: 06.06.2005

Date	Wednesday, 01 June 2005, 9:00 – 17:15
Place:	Koordinierungsstelle EG der Wissenschaftsorganisationen (KoWi), Rue du Trône 98, B-1050 Bruxelles

Agenda

09:00 – 9:50	Welcome, self presentation of participants, Introduction on SWAMI and on objectives of Workshop (Michael Friedewald)
09:50 – 10:10	Review of AmI projects and scenarios: the analytical framework (Elena Vildjiounaite)
10:10 – 10:45	Results of the Review (Elena Vildjiounaite) discussion of results
11:00 – 11:30	Threats in future Ambient Intelligence Application: First evidence (Michael Friedewald) discussion of results
11:30 – 12:15	First Results of the Legal Analysis (Wim Schreurs, Michiel Verlinden) discussion of results
13:30 – 15:00	Dark scenarios Part 1: Identification of major issues and drivers (post-it session) (Ioannis Maghiros, Yves Punie)
15:15 – 16:30	Dark scenarios Part 2: Clustering and prioritisation (Ioannis Maghiros, Yves Punie)
16:30 – 17:30	Consolidation, Conclusion, Next Steps

1. Introduction to the SWAMI-project by Michael Friedewald

Michael Friedewald, the co-ordinator of the SWAMI project welcomed the participants of the first Expert Workshop. After a self-introduction of the participants Friedewald gave an overview of the objective and the approach of the Project. The presentation can be found on the SWAMI website (swami.jrc.es).

Discussion:

- Q: Are we going to interview Hackers or hacker groups like the German CCC (“Chaos Computer Club”)?
- A: Probably not, because future scenarios and developments are considered in the project. Hackers are focussed on security gaps in current, existing systems. This is where they are experts in. Some participants of the workshop also report difficulties getting hackers to co-operate in this kind of research.

- Q: The question was raised whether or not we can use notions of privacy, identity and data protection of today and apply them to the situation in the future. It was stated that notions and assessments change over time and that our perception of privacy today might not be valid for future generations. Also, social learning was an issue. It was stated that computers would be used for other purposes than they are used today.
- A: The answer to this question is difficult, however the point has to be addressed. One way out of the dilemma is to think conceptionally and to bring together social and technological developments.

- Q: A vivid discussion developed upon reasons under which people are willing to give up privacy. Some people voluntarily give up privacy for better living conditions (housing in own homes in rural areas vs. moving into large apartment blocks without privacy the urban settlements was given as an example). However, most of the time people are economically forced to give up privacy.
- A: This aspect is covered in the project under the heading “Digital Divide”

2. Presentation of the SWAMI analytical framework and results of the review presented by Elena Vildjiounaite

Elena Vildjiounaite presented the results of the first work package of the SWAMI project. First she gave an overview of the chosen method to analyse existing scenarios, then presented the vision developed in various application contexts. The presentation can be found on the SWAMI website (swami.jrc.es).

Discussion:

- Q: How do we define what an actor is? Actor is usually a person but it could also be an intelligent software-agent, an avatar or other software agents. Just like real persons, these programs can make suggestions and make decisions in certain situations. The big question then is: Who is responsible and liable for the decisions made by those agents? Are they having rights of their own?
- A: Should be considered in further work. Perhaps “intelligent agents” should also be called as actors.

- Q: How can persons stop to be always connected, how can they opt out of an interconnected world? Will there be buttons to switch-off future devices, what does this say about the person, when he/she turns off devices?
- A: The opting-out question will be addressed in the scenarios. However, it was also mentioned that right now a generation grows up in which people don’t even know what it means to be disconnected. It can be assumed that they probably don’t ever want to be disconnected. Maybe future generations will take AmI for granted and AmI will be for them like electricity for us today. It should be avoided to interpret the future in today’s terms. As a solution it was suggested that the project focuses on “risks of a transparent society” rather than on “notions of privacy of today as opposed to tomorrow”. The relevant risks are for example: spamming by companies, surveillance by government, abuse, threats.

Further points in the discussion were:

- Should we be looking how the concept of privacy is changing?
- Privacy risks are contradictory. More and more can be done at home. There may be a new notion for privacy.
- Why are reality TV-shows so popular today? What does this say about the notion of privacy?
- We are far from an equal society in various areas of life. Housing, work, etc. How about privacy? Digital divide is evitable and reflects unequal conditions in offline-society.
- Privacy, data security only for the rich: You can “buy” privacy in the future just as other goods.

3. Threats in future Ambient Intelligence Application presented by Michael Friedewald

Michael Friedewald presented first evidence for possible threats in a world of Ambient Intelligence that were extracted from existing scenarios. They include: (1) Surveillance of users, (2) Identity theft, (3) Malicious attacks, (4) Digital Divide and (5) Spamming. These will be used as the basis for the development of more elaborated dark scenarios in the subsequent work. The presentation can be found on the SWAMI website (swami.jrc.es).

Discussion:

- Blackmailing as a new thread. “Pay me a certain amount of money or we will break one of your AmI-system”.
- How to handle threads that can also be considered customization of consumer needs like personalisation / profiling at Amazon.com
- Spamming might not be a major thread in the future. Intelligent systems have to be developed to control spamming. Also: The more you know about the person the more personalised messages you can deliver. People will learn to ignore spamming.
- One solution to tackle some threads is to have as free markets as possible where many suppliers of goods exist. If consumers do not like the product, they can buy another product – or do not buy at all. In this context, monopolies have to be avoided.

4. First Results of the Legal Analysis presented by Wim Schreurs and Michiel Verlinden

Wim Schreurs en Michiel Verlinden gave a presentation about the results of the overview of the existing legal framework relating to Ami, prepared by the VUB for the report. This overview was not limited to privacy and data protection law only. E-commerce, consumer protection, torts and liability, I.P. and I.C.T. law were shortly described. More in particular, for each law, the relevant issues and challenges for Ami were explicitly but shortly highlighted in order to start the discussion. The presentation can be found on the SWAMI website (swami.jrc.es).

Discussion

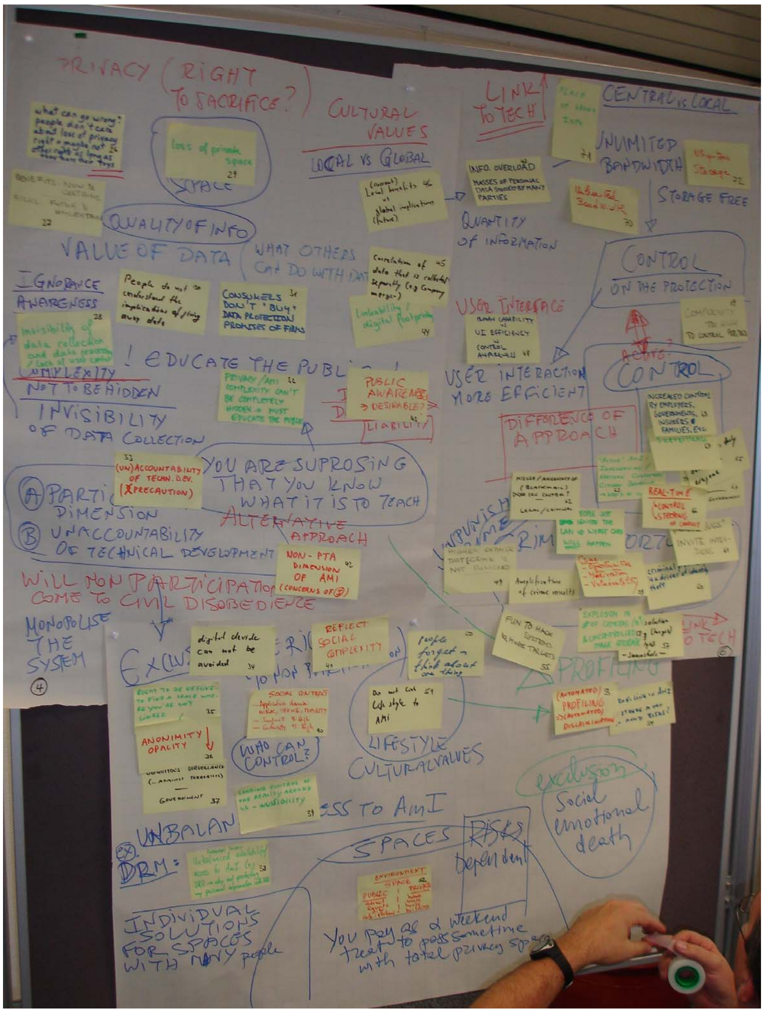
- Anonymous data can be linked to a certain person in some cases relatively easily using time-based data correlation – Data is statistically linkable.
- Using such the data is solved in data protection law. The user is liable of the use of data. Example: In US government collects data of the whole population and that data is available on the Web. Persons can be identified by using data mining technologies, even if the data was anonymised before.
- Right to be informed – is it enough to inform the visitors of a building at the front door that “we are collecting data for user experience”? What might be a specific enough purpose statement for informing the user? We collect data for future purposes?

5. Dark Scenarios sessions 1 and 2 moderated by Ioannis Maghiros and Yves Punie

The two sessions to prepare for the dark scenarios consisted of a post-it session to identify the major drivers and/or issues that need to be taken into account when developing dark scenarios and a session that focussed on the clustering and prioritisation of these drivers/issues.

Yves Punie first introduced the scenario exercise and argued that dark scenarios need to highlight risks and vulnerabilities. It is not their objective to identify "everything" that can go wrong with AmI and, as a result, to create a doom scenario, but rather to identify the most important and most probable things that can go wrong (intended and unintended), and, at a second stage, to discuss the social, legal, economic and technological implications of these things that can go wrong.

The post-it session consisted of a lively debate and many different ideas were raised.


PRIVACY (RIGHT TO SACRIFICE?)
what can go wrong? people don't care about loss of privacy right + maybe not other rights as long as they have their toys 26
loss of private space 27
SPACE
QUALITY OF INFO
VALUE OF DATA
WHAT OTHERS CAN DO WITH DATA
CULTURAL VALUES
LOCAL VS GLOBAL
(current) Local benefits vs global implications (future) 46
LINK TO TECH
INFO. OVERLOAD
MASSES OF PERSONAL DATA STORED BY MANY PARTIES
CENTRAL VS LOCAL
UNLIMITED BANDWIDTH
Unlimited Bandwidth 70
STORAGE FREE
QUANTITY OF INFORMATION
IGNORANCE
AWARENESS
People do not understand the implications of giving away data 30
CONSUMERS DON'T 'BUY' DATA PROTECTION PROMISES OF FIRMS 31
Correlation of data that is collected separately (e.g. Company merger) 45
Linkability / digital footprint 44
USER INTERFACE
HUMAN CAPABILITY
UI EFFICIENCY
CONTROL AWARENESS 48
CONTROL
ON THE PROTECTION
CONTROL
INCREASED CONTROL BY EMPLOYERS, GOVERNMENTS, INSURERS & FAMILIES, ETC.
Invisibility of data collection and data processing 28
COMPLEXITY
NOT TO BE HIDDEN
INVISIBILITY OF DATA COLLECTION
! EDUCATE THE PUBLIC !
PRIVACY/AMI COMPLEXITY CAN'T BE COMPLETELY HIDDEN → MUST EDUCATE THE PUBLIC 32
PUBLIC AWARENESS → DESIRABLE?
LIABILITY
USER INTERACTION MORE EFFICIENT
DIFFERENCE OF APPROACH
(UN)ACCOUNTABILITY OF TECHN. DEV. (PRECAUTION) 33
YOU ARE SUPPOSING THAT YOU KNOW WHAT IT IS TO TEACH
ALTERNATIVE APPROACH
A PARTICIPATION DIMENSION
B UNACCOUNTABILITY OF TECHNICAL DEVELOPMENT
NON-PTA DIMENSION OF AMI (CONCERNS OF B) 42
WILL NON PARTICIPATION COME TO CIVIL DISOBEDIENCE
MONOPOLISE THE SYSTEM
4
EXCLUSION
digital divide can not be avoided 34
REFLECT SOCIAL COMPLEXITY 41
ANONIMITY OPACITY 36
UBIQUITOUS SURVEILLANCE (… AGAINST TERRORISM) GOVERNMENT 37
SOCIAL CONTRACT
WHO CAN CONTROL?
people forget … think about one thing
Do not link Life style to AMI 51
LIFESTYLE
CULTURAL VALUES
UNBALANCED ACCESS TO AmI
EX. DRM:
SPACES
ENVIRONMENT SPACE
PUBLIC
PRIVATE
RISKS
Dependent
INDIVIDUAL SOLUTIONS FOR SPACES WITH MANY people
You pay as a weekend treat to pass sometime with total privacy space
IMPUNISM
CRIME
MISUSE / AWARENESS OF (BLACKMAIL) HOW CAN CONTROL? LEGAL / CRIMINAL
HIGHER CHANCE THAT CRIME IS NOT PUNISHED 49
Amplification of crime result
REAL-TIME CONTROL STEERING
INVITE INTRUDERS
criminal … theft
FUN TO HACK SYSTEMS & MORE TARGETS 55
EXPLOSION IN # OF CAMERAS … & UNCONTROLLED IMAGE STORAGE
PROFILING
(AUTOMATED) PROFILING => (AUTOMATED) DISCRIMINATION
… AND RISKS? 54
LINK TO TECH
6
exclusion
Social emotional death

Am I like electricity people would not want to opt out
LINK TO SOCIAL
UPGRADE SYSTEM
MORE RISK
POLLUTION WASTE
RECYCLING
INTERFACES
IMS
RELIABILITY
reliability of data
GROWING DEPENDANCE
THE WAY TECHNOLOGY WORKS
ENGINEERING SYSTEMS THAT ARE RECOVERABLE
RECOVERABILITY
REVOCATION OF KEYS
IRREVOCABILITY
Statistical post-processing of data
irreversibility of criminal acts
CRIME
WHO PAYS
COST/BENEFIT
INVISIBILITY OF MONEY
ISM/RFID
Advertisement
INVISIBLE PAYMENTS
Efficiency of business process
Monopolies become more dangerous
Cost/Benefit is security/privacy dependent on this?
Discrimination
RELATION TO CRIME OPPORTUNITY
INSURANCE IMPACT
(HEALTH monitoring)
Spreading risk will not work anymore

During coffee break, a first clustering was constructed by the IPTS team and presented at the start of the second section. The proposed clustering changed slightly.

The table below presents the result of this exercise.

Position	Top 10 Issues/Drivers	Impact average[1]	Certainty average	Impact * certainty
1	Loss of Control	4,53	4,26	19,30
2	Increased possibilities for surveillance	4,16	4,21	17,51
3	Profiling	3,79	4,42	16,75
4	Risk – Trust - Crime opportunities	3,47	4,16	14,44
5	Complexity (Value)	3,47	4,05	14,08
6	Individual transparent, power opaque	3,89	3,53	13,73
7	Dependence	3,37	3,63	12,23
8	Non-participatory (Process)	3,32	3,37	11,17
9	Exclusion	3,32	3,26	10,82
10	Costs	2,84	3,63	10,32

The drivers/issues are ranked, as the table shows. The ten clusters were ranked by the participants according to impact and certainty. Drivers or issues that are expected to have a major impact got 5 points against 1 point for little impact. Also, the degree of certainty that these drivers will have an effect was raked according to 5 (high certainty) and 1 (low certainty). The average of both is multiplied to get an assessment score that indicates the

[1] Total score divided by numbers of votes cast. They were 19 votes cast.

importance of the driver/issue, with lowest being between 1 and 5 and highest between 20 and 25. The ranking is shown in the table below. Although the method of multiplying impact and certainty averages is typically done in risk assessment to get a risk score, the table below should not be interpreted as such because the drivers/issues are not defined in terms of for example, concrete threats.

The issues that are regarded as most important both in terms of impact and certainty are: fear for loss of control; the increased possibility for surveillance offered by AmI and the observation that AmI needs to contain lots of personal info (profiling). This does not mean however, that the others are to be neglected when considering and developing the dark scenarios.