Legal Safeguards for Ambient Intelligence: Some Privacy Aspects

Paul De Hert
Serge Gutwirth
Anna Moscibroda

Vrije Universiteit Brussel

Outline

The SWAMI project
- About SWAMI
- State-of-the-art
- SWAMI 'Dark' scenarios
- Proposing safeguards

SWAMI legal aspects
Legal & regulatory safeguards
Conclusions

The SWAMI project

Safeguards in a **W**orld of **Am**bient **I**ntelligence

- Research project founded by FP6
- Multidisciplinary consortium
  - Vrije Universiteit Brussel, BE
  - ISI - Fraunhofer, DE
  - Institute for Prospective Technological Studies, JRC
  - VTT Electronics, FI
  - Trilateral Research and Consulting, UK

- Ended July 2006

The SWAMI project

Objective

To identify and analyse social, economic, legal, technological, and ethical issues related to identity, privacy and security in the context of Ambient Intelligence (AmI), and reflect on safeguards for Information Society by creating and analysing four 'dark' scenarios

---

The SWAMI project

Steps

- Reviewing existing scenarios on AmI
- Developing 'dark' scenarios
- Analysing scenarios and identifying risks and vulnerabilities
- Proposing safeguards

The SWAMI project

Reviewing existing scenarios on AmI

- Finalised January 2006
- Conclusion: Most AmI scenarios are too 'sunny', not representative of 'real' world conflicts
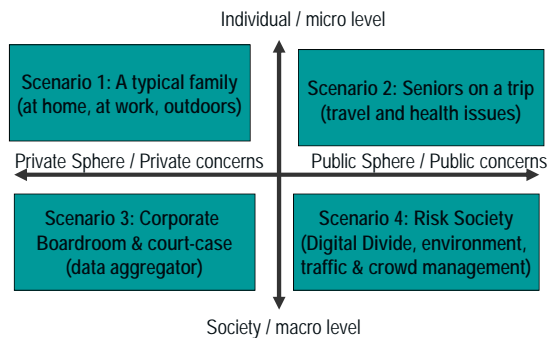
1

The SWAMI project

Developing 'dark' scenarios

- Adverse but realistic situations highlighting key socio-economic, legal, technological and ethical risks of AmI
- Finalised January 2006

SWAMI 'dark' scenarios

Individual / micro level

Scenario 1: A typical family (at home, at work, outdoors)	Scenario 2: Seniors on a trip (travel and health issues)

Private Sphere / Private concerns — **Public Sphere / Public concerns**

Scenario 3: Corporate Boardroom & court-case (data aggregator)	Scenario 4: Risk Society (Digital Divide, environment, traffic & crowd management)

Society / macro level

SWAMI 'dark' scenarios

Analysing scenarios

- Conclusion: AmI endangers privacy
  - ➢ Increased surveillance, e.g. via implants and sensors, make it impossible to hide our doings, or even feelings
  - ➢ Increased connectivity and data exchange facilitate extensive profiling
  - ➢ Borders between various spaces, social roles and spheres of live blur
  - ➢ 'expectation of being monitored' especially within the public spaces (work)

The SWAMI project

Proposing safeguards

- technological
- socio-economic
- legal & regulatory

- for EU
- for MS
- for industry
- for academia
- for civil society organisations
- for individuals

[SWAMI Deliverable D3, *Threats, Vulnerabilities and Safeguards in Ambient Intelligence*, July 2006]

Outline

The SWAMI project
SWAMI legal aspects
- State-of-the-art
- Legal analysis of the scenarios
- Developing safeguards

Legal & regulatory safeguards
Conclusions

SWAMI legal aspects

Steps

- A state-of-the-art of existing legal framework for AmI
- Legal analysis of the SWAMI 'dark' scenarios
- Developing legal and regulatory safeguards

SWAMI legal aspects

A state-of-the-art

- Description of the European legislation relating to Ami- broad subject matter covered:
  - ➢ Privacy and Data Protection
  - ➢ Intellectual Property Rights
  - ➢ E-commerce and Consumer Protection
  - ➢ Torts and Liability
  - ➢ I.C.T. Law
  - ➢ Criminal Law
  - ➢ Antidiscrimination law
  - ➢ Jurisdiction and Applicable Law

SWAMI legal aspects

Legal analysis of 'dark' scenarios

- Highlighting situations in the scenario that raise legal questions
- Indication and assessment of existing legal rules on EU level
- Results: Identification of existing lacunae

SWAMI legal aspects

Developing safeguards

- Aim: to identify the research and policy options built into the Information Society Services, the safeguards addressing key risks and vulnerabilities

---

Outline

The SWAMI project

SWAMI legal aspects

Legal & regulatory safeguards
- Legal and regulatory safeguards for privacy
- Digital Territories
- RFID

Conclusions

Legal & regulatory safeguards

Based on results of legal analysis of scenarios

- There is legal framework for privacy
- But AmI challenges this framework
- Data Protection principles difficult to reconcile with the AmI requirements (e.g. proportionality principle v. need of extensive profiling)

Legal & regulatory safeguards

Safeguards for privacy

- Need for AmI specific safeguards
- Addressing particular technologies
- Building upon existing framework
  - ➢ **OPACITY** (Saying under no circumstances)
  - ➢ **TRANSPARENCY** (saying yes but)
- Most challenges should be addressed by transparency tools
- Privacy by design

Legal & regulatory safeguards

AmI specific privacy safeguards- examples:

- Digital territories
- Legal safeguards for RFID

Legal & regulatory safeguards

Digital Territories (DT)- concept:

- Digital space which can be accessed anytime/anywhere
- A 'bubble', a private digital space of individual
- Borders and transparency of a 'bubble' are controlled by individual himself
- Aims to empower individual with control over his private sphere and dissemination of his personal data

[IPTS Report, *D1gital Terrot0iries: Towards the protection of public and private space in a digital and Ambient Intelligence environment*, 2007]

Legal & regulatory safeguards

Digital Territories-Lacuane in legal framework

- Data Protection (DP) law does not distinguish between different categories of personal information (except sensitive data), or different contexts of data collection
- How to protect the private sphere in public spaces: Reasonable expectation of privacy v. expectation of being monitored
- Hard formal requirements of DP law (consent, information requirements)
- Data retention obligation could apply to some interaction made via DT
- But no procedural guarantees when the private digital territory is accessed – a bubble is not a home in the legal sense

Legal & regulatory safeguards

Digital Territories- what we propose:

- As the DT is a useful concept for the privacy protection in borderless AmI, adequate legal framework is needed
- e.g. procedural safeguards in case the information in the 'bubble' are being accessed (search warrant)
- Technical security measures protecting the bubble required/enforced by law, PETs, IMS, …
- It is a new concept- further research into technical and legal issues is needed

Legal & regulatory safeguards

RFID – description:

- RFID system is a tag with corresponding reader, computing device and software, reference database, external interfaces, …
- Enables M2M communication
- Enables real-time monitoring and real-time automated decision making

Legal & regulatory safeguards

RFID- lacuane in legal framework

- No law addressing specifically the RFID -General privacy law apply. But which law? (e.g. traffic data)
- What is a personal data within the RFID context?
- Profiling based on non-personal data still affects individuals- no framework for such profiling activities
- Hard formal requirements of DP law (expressing consent, information requirements)

Legal & regulatory safeguards

RFID - what we propose:

- DP guarantees should be respected if personal data are processed by RFID
- In any case, the individuals should be informed about presence of tags and readers
- Simplify notices and pictograms
- Possibility to remove/ deactivate tag
- PETs, TETs and privacy technology assessment- a legal obligation
- RFID specifications, privacy standards, code of conducts and guidelines recommended
- Further research into technology and safeguards needed

Conclusions

- To take full advantage of AmI we need to consider its 'dark' side
- Analysis of adverse scenarios discloses lacuane in regulatory framework
- Transparency as default position
- DT and measure for RFID systems are examples of Ami specific privacy safeguards
- But there is no closed list of solutions/safeguards
- Privacy by design

Thank you !
Questions ?

http://swami.jrc.es/pages/index.htm

EXTRA SLIDES

SWAMI 'dark' scenarios

Threats and Vulnerabilities to Privacy

Threats
- Cracking
- Surveillance
- Function creep
- Profiling
- Possible erosion of rights and values

Vulnerabilities
- Lack of adequate security measures
- Lack of enforcement
- Lack of public awareness

EU Framework on Privacy

- **Art. 8 ECHR**
- **Art. 7 CFR EU**
- **Data Protection Directive 95/46**
- **Privacy & Electronic Communication Directive 2002/58**