International Telecommunication Union

TOMORROW’S NETWORK TODAYS WORKSHOP

UBIQUITOUS
NETWORK SOCIETY AND PRIVACY

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Cosimo Comella
Italian Data Protection Authority
www.garanteprivacy.it

Ubiquitous computing in a privacy perspective: opportunity and concerns

- Accomplish an increasing number of personal transactions using portable devices
- Anywhere: every physical object infused with computational and communication capabilities
- Transparency: technology is (almost) invisible to the human user

Privacy sensitive ubiquitous applications

- Micropayments
- Domotica systems
- Tracking of mobile assets and goods
- Children monitoring

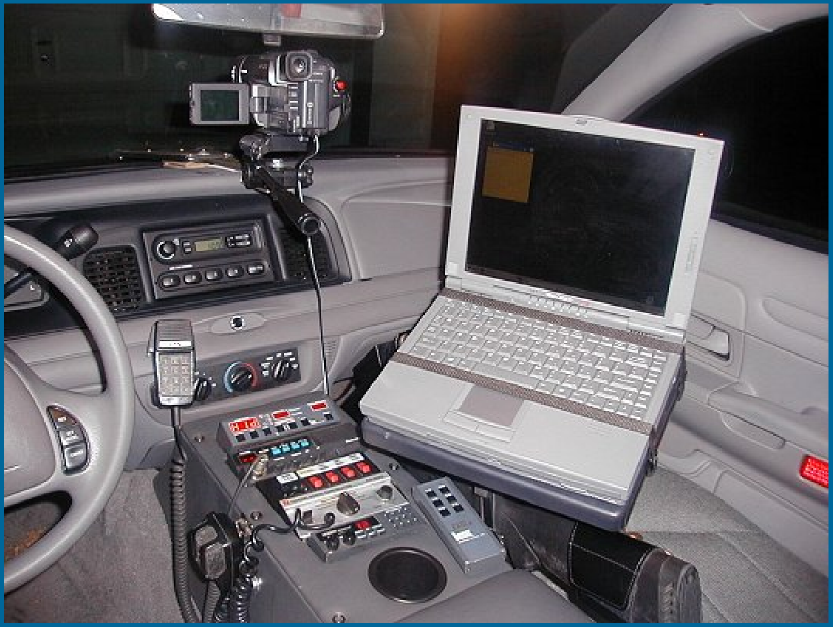
…Privacy sensitive ubiquitous applications

Healthcare and medical applications

- Monitoring micro-dose drug release
- Tracking blood for transfusions
- Clinical informations on personal transponder

…Privacy sensitive ubiquitous applications

- Research for Secure Europe: 1 billion euro per year
- Protecting against terrorism
- Tracking the movement of threatening substances and persons
- Safe driving

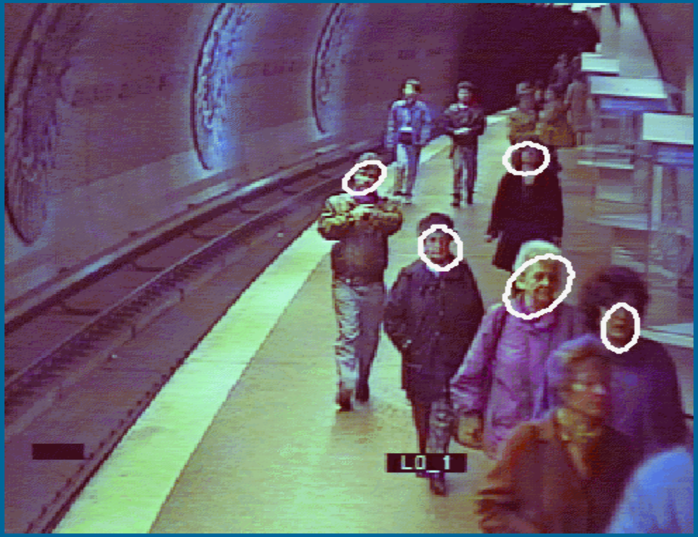


Privacy Issues

- Invisible and ubiquitous design
- Automatic user recognition and tracking
- Peer-to-peer paradigm
- Data-mining

Automatic user recognition and tracking

- Digital video surveillance



Peer-to-peer paradigm

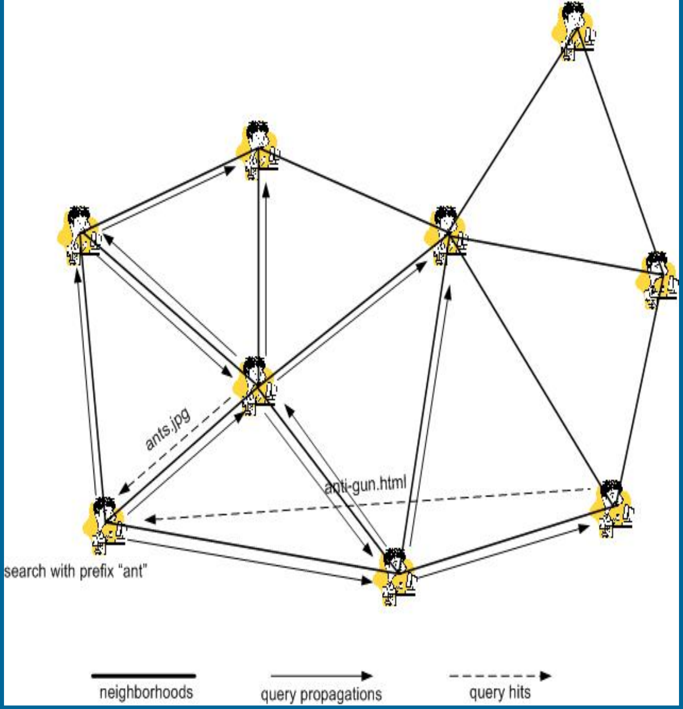
- Personal resources sharing
  without any content control
  to access services
- Example:
  traffic congestion signalling
  to a broadcasting station

Data mining and datawarehousing

- Can enhance the control capabilities
- Speed up data analysis and inferential processing

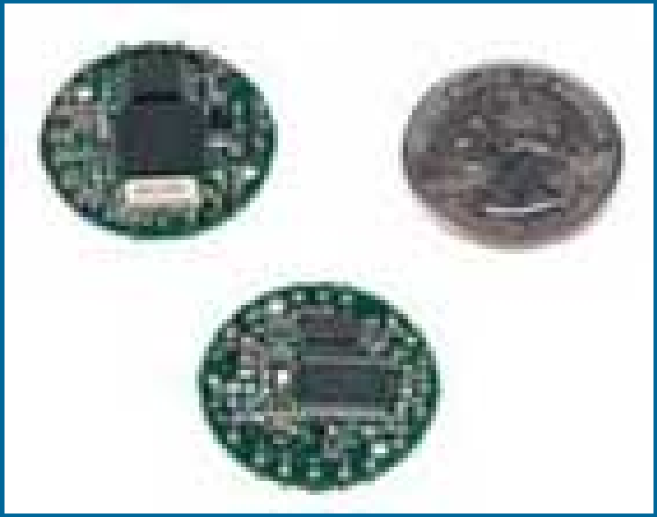
Another Scenario: Wireless Sensor Networks (WSN)

- Collection of sensors not relying on a fixed infrastructure to keep the network connected
- Sensors can be Mobile
- A WSN can be formed, merged or partitioned on the fly
- Every node can act as router
- Every node can process personal data



Ubiquitous Computing: Privacy Challenges

- Ubiquitous computing raises challenges to privacy and security
- Normally undetectable activities could be analyzed and linked with new technologies
- Example: micropayments



Ubiquitous computing and RFID

- Radio Frequency Identification
- Tags can be read without owners’ knowledge
- Tags and readers can be covertly embedded in the environment

…Ubiquitous Computing and RFID

- Security and Privacy problems
  - Inside the supply chain
  - Transition zone (where tagged items change hands from vendors to consumers)
  - Outside the supply chain

RFID Standards and Interoperability

- Universal Product Code bar codes
- Electronic Product Code (Auto-ID Center, MIT, EPCglobal)
- Universally accesible Object Name Service (ONS) database
- EPC promoted as a single open worldwide RFID standard

Resource for privacy inside RFID technology

- Several thousand transistors inside a tag
- Between 250 and 1,000 gates only available for security features
- Difficult to implement encryption algorithms

Solutions to Privacy Challenges

- Technical solutions
  - Killing or removing tags
  - The encryption option
  - Passwords and Pseudonyms
  - Blocker tags
- Policy solutions

European Privacy Legal Framework (related to Ubiquitous Computing and RFID)

- Directive EC/46/1995
  Directive on the protection of individuals regarding personal data processing and movement
- Directive EC/58/2002
  Directive regarding privacy and electronic communication
- Article 29 Data Protection Working Party
  - Working document on data protection issues related to RFID technology
  - January 19, 2005 (WP 105, 10107/05/EN)

International positions on RFID Technology

- 2003 International Conference of Data Protection & Privacy Commissioners
  - Resolution on Radio-Frequency Identification
  - Sydney, November 20, 2003

Ubiquitous Computing and RFID: An Example of Regulation

- Italian DPA General Provision on RFID
- To implement EU principles, in particular developed by art. 29 WP, at national level
- To adapt the general rules concerning data protection to the specificities of RFID
- To give guidelines to practitioners and producers, in the light of the increasing investments in this sector
- It regards RFID implementation involving the processing of personal data relating to *identified or identifiable* third parties (not f.i. corporate distribution chain)

General Principles of EU Data Protection

- **Data Minimisation Principle**: avoiding the use of personal data if this is not absolutely necessary in connection with the purposes to be achieved
- **Lawfulness**: legal grounds → for public bodies: discharge of public tasks; for private entities: compliance with legal obligations, or freely given, explicit consent by the data subject
- **Purposes and Data Quality**: data controllers may only process personal data for specific, explicit and lawful purposes; data must be relevant, not excessive, accurate and updated; erased or anonymised after having achieved the purpose

General Principles of EU Data Protection

- **Proportionality:** data controller must verify that processing mechanisms are not disproportionate compared to the purposes to be achieved (f.i. no functioning of tags outside the shop unless this is necessary to deliver a service specifically and freely requested by data subject)
- **Information Notice:** data controller must refer to the presence of RFID tags and specify that personal data may be collected without data subjects' intervention; how to remove/deactivate tags should also be highlighted; appropriate information notice placed on objects and/or tags if tags remain active once outside the premises where RFID technologies are implemented

General Principles of EU Data Protection

- **Consent:** should be specific and explicit (data subject’s conclusive conduct is irrelevant in this respect; for sensitive data it must be given in writing and the processing may only be carried out upon the Garante’s prior authorisation)
- **Exercise of Rights:** manufacturers of RFID systems should lay down suitable mechanisms for ensuring that data subjects can easily exercise their rights (right of access, erasure, rectification etc.)
- **Tag Deactivation/Removal:** data subject must be afforded the possibility to have the RFID tags removed and/or deactivated, free of charge and in an easy manner once use is over

The Especially Sensitive Issues in This Sector

- We are dealing with personal dignity and integrity
- RFID may impact on freedom of movement
- Processing of personal data may be carried out without data subject’s knowledge
- Increased risks if RFID devices are integrated within network infrastructures
- Enhanced safeguards for employment context and underskin implants

Employment Context

- When RFID is used to check access to workplaces, it should be considered that specific legislation in Italy prohibits implementation of devices and equipment for the distance monitoring of employees’ activity
- If such devices are necessary for other purposes, (f.i. controlling access to certain areas), the safeguards set out in relevant labour laws and in the DP laws must be complied with (data minimisation, purpose specification and proportionality principles)

Underskin Implants

- In principle subcutaneous microchip implants must be ruled out, because in conflict with personal dignity and bodily integrity
- Allowed only in exceptional cases further to documented, justified requirements concerning protection of individuals' health
- Data subject should be in a position to have the microchips removed at any time and free of charge, and the presence of the tag in his/her body should not be revealed
- This kind of processing requires the Garante's prior checking

Additional Requirements (Imposed on Data Controllers by the DP Code)

- Notification of the processing to the Garante:
  - concerning data on the geographic location of individuals and/or objects by means of electronic communication networks
  - carried out with the help of electronic means in order to define a data subject’s profile or personality, or else analyse his/her habits and choices as regards purchased products
- Obligations related to security measures
- Specifying the entities that are authorised to process data in their capacity as either data processors or persons in charge of the processing

For a Responsible Development of Ubiquitous Computing

- The role of IT researchers and technologists
- Privacy principles embedded in the applications
- Security and privacy ensured "by design"
- Relationship with public institutions, lawmakers, political bodies
- The role of international organizations: OECD, Council of Europe, UE WP Art. 29

Examples of IT Industrial Acceptance of EU Privacy Principles

- The Microsoft Passport case

  The software giant agreed with UE a 18-month roadmap to reach full compliance with EU data protection directive (EC/46/1995) of its SSO system
- The Google Gmail case

  Email profiling for individual ads generation
- Privacy options now available to web users in all major web browsers

  Cookies, popup, active content management

Final Remarks

Asleep or awake, working or eating, indoors or out of doors, in the bath or in bed -- no escape. Nothing was your own except the few cubic centimetres inside your skull.

George Orwell, 1984 (1949)

References

- Italian DPA (Garante per la protezione dei dati personali) http://www.garanteprivacy.it/
- English version of the RFID general provision:

  http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107