Visions for Ubiquitous Spatial Computing

A Privacy Protection Perspective

Professor Harlan J. Onsrud
Department of Spatial Information Science and Engineering
and
National Center for Geographic Information & Analysis
University of Maine
7 June 2007 Halifax Nova Scotia

How can privacy be protected in ubiquitous spatial computing environments?

- Confidentiality

  - allow human identity linking to objects and services but a legal obligation imposed to protect
    - sensor use in medicine and science
    - sensor use internal to businesses
- Anonymity

  - deliver object or provide service by never linking to human identity (not typically imposed by law)
    - anonymity possible in providing many consumer goods and services

2

Practical Example in Protecting Personal Information Privacy

- **Example:** Use of passive radio frequency identification tags in the tracking of consumer goods
  - passive RFID deployments illustrate one embodiment or microcosm of ubiquitous spatial computing
    - Low Frequency - 30 cm away
    - High Frequency - 1 meter away
    - Ultra High Frequency - 7 meters away
- **Challenge:** Design pervasive observation environments allowing protection of privacy without lessening beneficial uses

3

Use of Passive RFID Tags on Consumer Goods

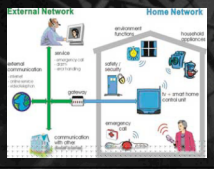



4

Use of Passive RFID Tags on Consumer Goods



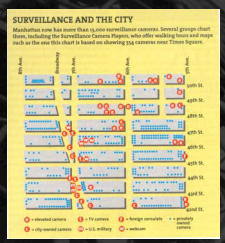


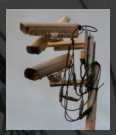



5

Inside & Outside

Every surveillance camera will now come standard with an RFID reader



15,000 cameras in Manhattan

… providing myriad benefits.

6

Threats

Unprecedented opportunities for clandestine:

snooping
stalking
manipulation
harassment
tracking
theft
profiling

Who should protect against unwanted intrusions in ubiquitous spatial computing environments?

7

Competing Privacy Protection Visions

Big Brother
Government Surveillance

Surveillance by
Corporate Elite

Pervasive Mutual
Surveillance

... "answer me one question. Are these the shadows of the things that Will be, or are they shadows of things that May be, only?"

A Christmas Carol, Charles Dickens

8

Can we construct a better privacy protection vision for our pervasive information society?

- Vision based on **legal** or **moral** standard for privacy protection?

- I prefer the moral

legal - majority rules, law varies

moral - universality of principles

9

Morally Defensible Standards

There exists a set of ***prima facie duties*** always in effect:

- **autonomy** - duty to support *self determination* in defining, planning and pursuing a good life in self and others
- **nonmaleficence** - duty to avoid unnecessary harm to others
- **beneficence** - duty to advance welfare of others when able to do so
- **justice** - duty to treat all fairly and impartially

10

How would we design distributed computing sensor environments that are morally defensible?

Greatest challenge: **support of autonomy of the individual** in our ubiquitous systems

- rejection of "one-size-fits-all" privacy protection
- support freedom to choose your individual privacy comfort level
- support freedom to change your mind at any time and location

Our problem as researchers to solve? **Who better?**

11

Individual Autonomy: Control over the sensors we wear, carry, or own

I. Protecting through Reliance on Technology

- Scenario: Unauthorized person scans the sensors on your body or in your home

12

(1) Make scan ineffective through deactivated tags

- Permanently: frying, clipping, killing
- Temporarily: Faraday cages, sleep/wake modes

Problems:

- Lose all or some benefits
- May effect tags of others

13

(2) Make scan ineffective through encryption and/or access control

- Low power encryption algorithms: stream ciphers, block ciphers, public key primitives, lightweight authentication
- Access control on or off the tags: hash locks, blocker tags, enhancer proxy

14

Example:

- Medicine, Human Subjects Research & Corporate Applications
  - encryption likely to be used where legal obligation for confidentiality exists

Problem:

- Encryption for a class of interoperable sensors is likely breakable
- Thus, need extra legal protection … cracking and distribution likely to be made illegal.

15

Example:

- Consumer Products
  - Encryption unlikely to be used on tags on most goods in the long run - interoperability a problem & more expensive

Problems:

- Encryption and access controls will lose in the marketplace
- Openness and interoperability win in the ubiquitous services marketplace (history of credit cards, GPS, web, etc.)
- Thus, encryption controls unlikely provided in this context.

16

(3) Make scan ineffective through mediator security device

(Rieback, et.al.)

- install guardian in your cell phone and in every room reader
- detects reader, if reader is not approved, jams time slot responses from all your tags (***selective jamming***) and provides ***tag spoofing***
- ***Benefit:*** Effects only tags being protected.

17

Problems:

- carry guardian with you or obtain no protection
- need automated or user friendly process for identifying which tags to protect
- spy versus spy problem - ***jamming the jammer*** makes all tags accessible

18

Individual Autonomy:
Control over the sensors we wear, carry, or own

II. Protection through Reliance on the Marketplace

- Theory: If privacy is valued by consumers, ubiquitous architectures that protect privacy will prevail

19

Problems:

- Those companies that voluntarily protect information privacy beyond the legal minimum typically lose in the marketplace
- Examples:
  - grocery discount cards prevail over privacy
  - credit cards that protect privacy have failed
  - privacy protection enablement on web has largely failed (Platform for Privacy Preferences (P3P))

20

Immediate cash or benefit

versus

complex, nebulous future non-tangible right

"Informed consent" is highly questionable

Morally defensible privacy protection has failed to result from dependence on market alone.

21

Individual Autonomy: Control over the sensors we wear, carry, or own

III. Protection through Reliance on the Law

- Goal: Pass one or more laws that would drive technological developments and the market towards morally defensible ubiquitous computing

22

Example 1:

- Pass a law:

  You may not link people's identity to RFID tags without first obtaining their explicit permission.

  90% of population supports, Congress passes

Problem:

- *corporate freedom of speech* trumps *individual freedom from trespass* or *individual privacy*
- unconstitutional

23

Example 2: What has worked?

- Pass a law which establishes a centralized legally enforceable do not link registry (with automated checking at the time of purchase of goods, face recognition match, etc.)

  If registered, you may not link people's identity to RFID tags without first obtaining their explicit permission.

Has potential:

- most benefits of sensors retained, abuses constrained
- drives technology towards anonymity rather than confidentiality
- not unconstitutional, morally defensible
- practical: "do not call list" changed practices overnight

24

Which research questions should we address?

An infinite number … address those with greatest chance of making a difference.

Greatest gains … technological advancements accommodating and embedded within economic, legal, & societal realities

25

Credits:

Several images in this material were acquired through an advanced Google search of images contained on Creative Commons licensed web sites.

26

Other images are covered by **Fair Use** under Copyright Law

Recommended Reading:

http://www.law.duke.edu/cspd/comics

However, if you see an image in this presentation in which you are claiming ownership and would prefer not having included, let me know and I will gladly replace it with another.

27