Identifying, Tracking and Tracing:
From Geographic Space to Cyberspace and Back

Lorenz M. Hilty
Informatics and Sustainability Research (ISR) Group
Empa Materials Science and Technology and University of Zurich, Switzerland

Based on the TA-SWISS study: Localized and Identified – How Localization Technologies Are Changing Our Lives (in German):

Lorenz M. Hilty
Britta Oertel
Michaela Wölk
Kurt Pärli

Lokalisiert und identifiziert – Wie Ortungstechnologien unser Leben verändern
vdf Hochschulverlag AG
TA-SWISS, Schweizerisches Zentrum für Technologiefolgenabschätzung
2012
ISBN: 978-3-7281-3460-8

http://e-collection.library.ethz.ch/view/eth:5555

Technology Assessment for
technologies determining the locations of objects or people in geographic space

1. Which technologies are/will be in use 2010-2020?

2. Which application domains are emerging?

3. What are the main opportunities and risks for society?

4. Is there any need for action?
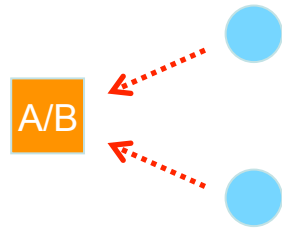
5. Recommendations

1. Technologies

- Satellite-based systems (e.g., GPS)

- Mobile phone networks (e.g., GSM)

- Wireless LAN

- Bluetooth-based networks (piconets)

- Active RFID

- Passive RFID (in structured environments)

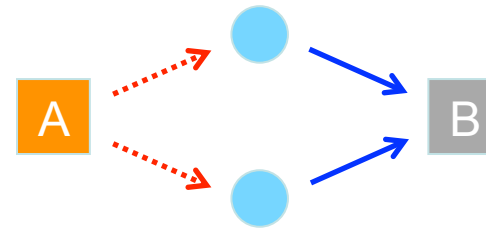- Foto/video cameras plus face recognition

- IP address location

etc.
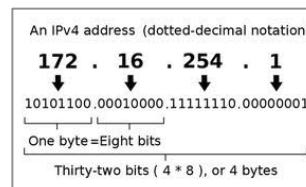
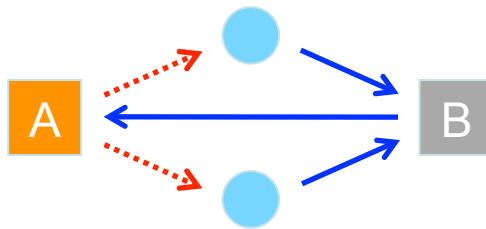Source: Hilty, Oertel, Wölk, Pärli (2012)

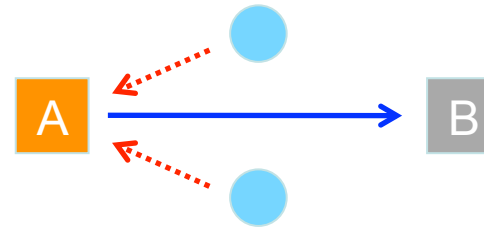# 1.1 Basic patterns of locating objects or persons

direct self-locating

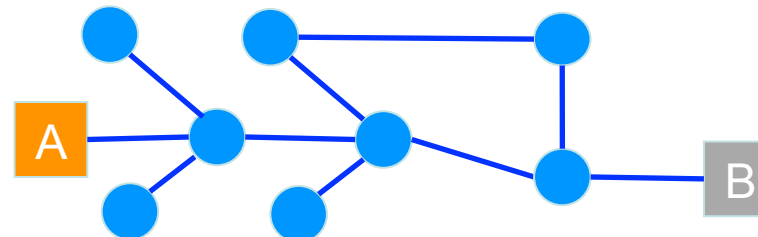direct locating of others (B locates A)

indirect self-locating

indirect locating of others

A: object or person being located
B: object or person locating
┄┄┄> signal used for locating
───> data transfer

Source: Hilty, Oertel, Wölk, Pärli (2012)

locating a node in a network
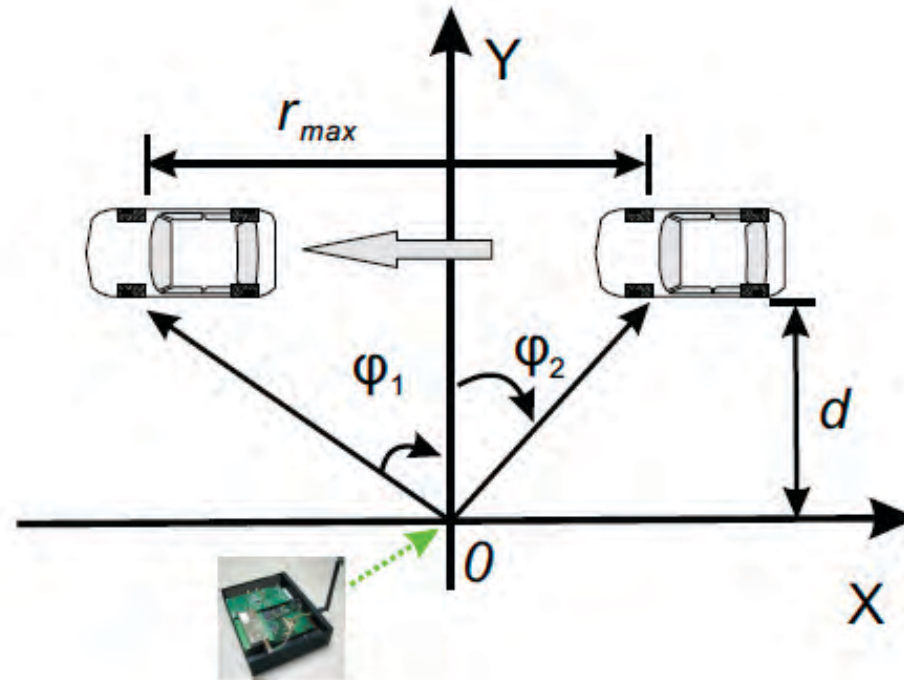
1.2 Identification of located objects

Is there a chance to defend location privacy in a connected world?

Source: Bereseford, Stajano (2003)

1.3 Locatability as a side-effect of (machine-to-machine) communication

Example: Wireless tire pressure sensors in cars

Source: Rouf et al. (2010)

2. Main application domains

Navigation

Emergency response

Toll and fare collection, insurance rate calculation

Location based services and micromarketing

Surveillance of individuals and precious goods ("geofence")
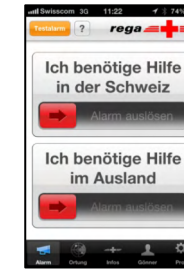
Surveillance of crowds (e.g., for traffic control)

Documentation, preservation of evidence

Source: Hilty, Oertel, Wölk, Pärli (2012)

Source: appgefahren.de, 2012
Source: netzwelt.de, 2012
Source: ADAC, 2012
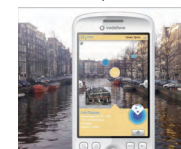Source: Rotes Kreuz SH, 2012
Source: Rega, 2011
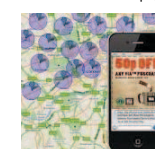Source: abudapest..om, 2012
Source: Augsburger Allgemeine, 2012
Source: Broadpit, 2010
Source: Ray Wang, 2011
Source: M3 Systems, 2007
Source: Trickr.de, 2011
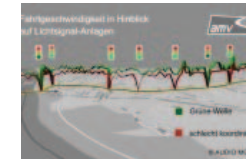Source: Safety Basement, 2012
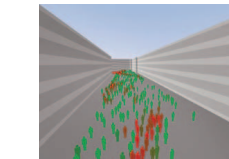Source: Sbhusansharma, 2008
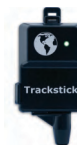Source: Keruve, 2011
Source: Automotivsstreetstyle, 2010
Source: AMV networks, 2010
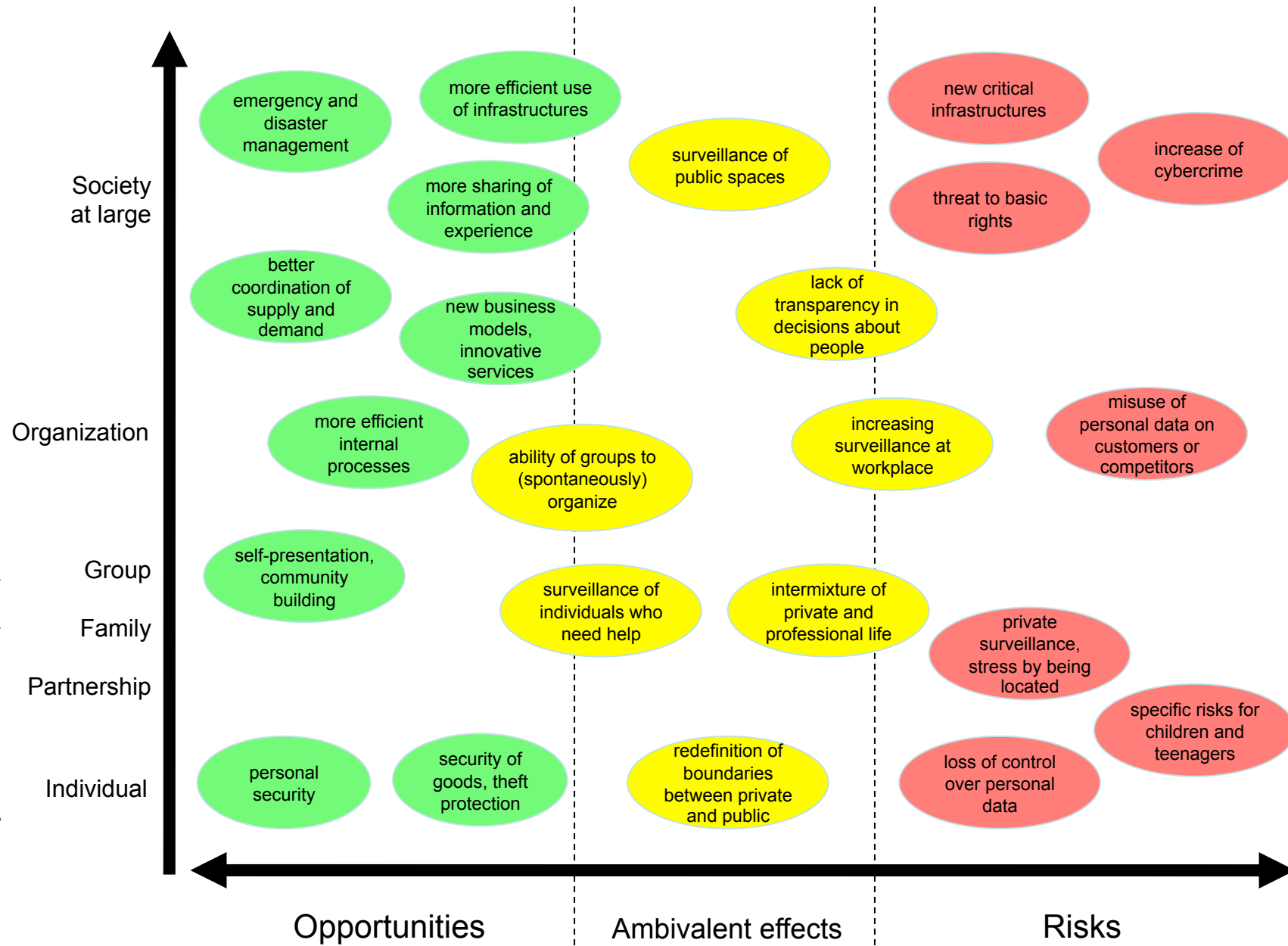Source: Siemens, 2009
Source: Trackstick.com, 2012
Source: ArtikelMagazin, 2010

3. Opportunities and risks (focus on mobility and social networks)

Source: Hilty, Oertel, Wölk, Pärli (2012)

Society at large

- emergency and disaster management (green)
- more efficient use of infrastructures (green)
- more sharing of information and experience (green)
- surveillance of public spaces (yellow)
- new critical infrastructures (red)
- increase of cybercrime (red)
- threat to basic rights (red)
- better coordination of supply and demand (green)
- new business models, innovative services (green)
- lack of transparency in decisions about people (yellow)

Organization

- more efficient internal processes (green)
- ability of groups to (spontaneously) organize (yellow)
- increasing surveillance at workplace (yellow)
- misuse of personal data on customers or competitors (red)

Group

- self-presentation, community building (green)
- surveillance of individuals who need help (yellow)
- intermixture of private and professional life (yellow)

Family

Partnership

- private surveillance, stress by being located (red)
- specific risks for children and teenagers (red)

Individual

- personal security (green)
- security of goods, theft protection (green)
- redefinition of boundaries between private and public (yellow)
- loss of control over personal data (red)

Opportunities **Ambivalent effects** **Risks**

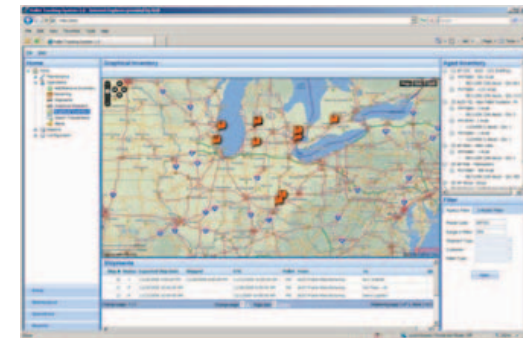## 3.1 Main areas of opportunity

Security of persons and material goods
- Emergency response
- Child safety and security
- Theft protection for cars, luggage, electronic devices, etc.

Efficiency in traffic and logistics
- Finding your destination faster
- Intelligent traffic management
- Freight tracking and tracing

Transaction cost reduction
- Automatic mobility pricing
- Fee collection for infrastructure use
- Admission charging for events etc.

Synergies between the virtual and the physical world
- Presence in social networks can be linked to real presence, contacting people is easier
- Location-based services and augmented reality (e.g. in tourism)
- Location-based crowdsourcing (e.g. monitoring infrastructures, environmental monitoring)
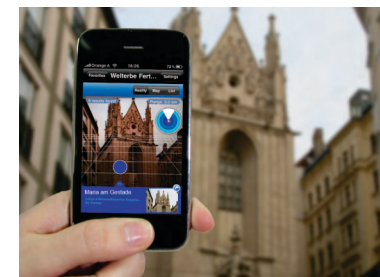
Source: Hilty, Oertel, Wölk, Pärli (2012)

3.2 Main areas of risk

**Increasing dependency on a new critical infrastructure**

- Positioning systems become a critical infrastructure.
- Availability is never 100%
- Signals can be faked (e.g. GPS signals)
- Systems can be attacked by malware

enlarged ranges

p (true location)

p' (spoofed location)
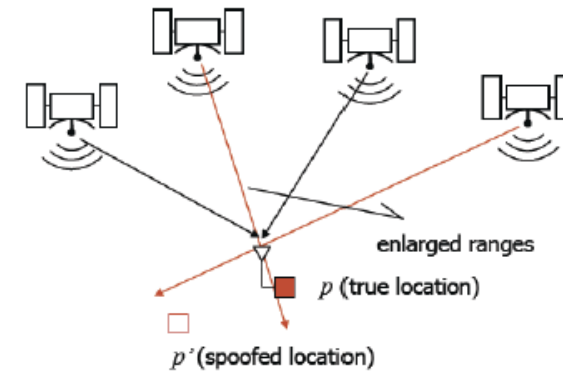
Source: S. Capkun, ETH, 2011

Loss of control over personal data

- Who is processing my movement and contact profile for what purpose?
- What decisions are based on my location data?
- Data is processed in countries with a legislation different from ours.
- New types of cybercrime (housebreaking, stalking, etc. based on location data)

LITTLE SISTER IS WATCHING YOU.
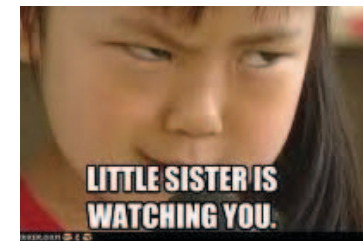
Ethical dilemma between security and individual freedom

- Complete control over children, patients, demented people?
- Surveillance of public space vs. basic democratic rights
- Private surveillance of partners, etc.

Source: Hilty, Oertel, Wölk, Pärli (2012)

4. Need for action

Need for action has been identified in the following fields:

- surveillance of people in **dependency relationships**;

- **child protection** measures pertaining social networks with localization functions;

- informational self-determination of the individual vis-à-vis the state and private-sector enterprises: **maintaining control** over one's own data;

- setting **limits to the retention of localization data**, because in many cases it can be associated with persons after the fact, possibly jeopardizing their rights to privacy ("right to be forgotten");

- permissibility of the **Terms of Service (ToS)** used by the providers of software packages and services with localization functions;

- security of positioning systems as a new **critical infrastructure**.

Source: Hilty, Oertel, Wölk, Pärli (2012)

5. Recommendations

Extract from the study's recommendations:

- Include positioning technologies in the **media education** at public schools.

- Include positioning systems in the **program for critical infrastructures** of the public authorities.

- Clarify the regulatory frameworks of **surveillance at the workplace** and of public video surveillance.

- Introduce more efficient ways to **sanction violations of the data protection rules** by public or private bodies.

- Introduce **certification schemes for location-based software products** providing a sufficient level of reliability and transparency.

Source: Hilty, Oertel, Wölk, Pärli (2012)

Contributors

References

Beresford, A. R.; Stajano, F. (2003): Location Privacy in Pervasive Computing. Pervasive Computing, IEEE, Volume: 2 Issue:1, pp. 46-55

Capkun, S. (2011): Selected Security Issues in Mobile Computing. 16th Symposium on Privacy and Security, ETH Zürich.

Hilty, L. M.; Oertel, B.; Wölk, M.; Pärli, K.: Lokalisiert und Identifiziert. Wie Ortungstechnologien unser Leben verändern. vdf Verlag, ETH Zürich 2012

Oertel, B.; Wölk, M.; Hilty, L. M.; Köhler, A.: Security Aspects and Prospective Applications of RFID systems. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2005

Rouf, I.; Miller, R.; Mustafa, H.; Taylor, T.; Oh, S.; Xu, W.; Gruteser, M.; Trappe, W.; Seskar, I. (2010): Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In Proceedings of USENIX Security Symposium'2010. pp. 323-338