



Who? Where? What?

The Challenge of Pervasive Micro-Blogging

Marc Langheinrich

University of Lugano (USI), Switzerland

Always On, Always Connected

- From Web Pages to Blogs to Twitter-**Feeds**
 - From „My CV“ to „What am I doing **right now**?“
 - People **love** staying in touch (with friends & strangers)
- Socializing Means **Sharing**
 - Ideas, experiences, feelings
- New Generation of Smartphones
 - **Simplify** pushing out updates (Twitter widgets)
 - **Automate** sharing of experiences (where, what)

Privacy?

- Maybe People **Don't Care?**
 - “By 2010,... privacy will become **a meaningless concept** in Western societies (60% probability).”

Gartner Research, 2000

- Maybe People Care, But **Not Enough**
 - „As younger people reveal their private lives on the Internet, the older generation looks on with alarm and misapprehension not seen since the early days of rock and roll. **The future belongs to the uninhibited.**”

Emily Nussbaum: “Say Everything.” New York Magazine, 2007

Privacy, Anonymity, and Secrecy

- Technologist Often Like Things **Binary** (On vs Off)
 - Privacy == Secrecy
 - Privacy == Anonymity
- People Don't Want to **Manage Their Privacy**
 - They're already busy enough managing their lives!
- People **Want to Share** Their Lives With Others
 - Any privacy overhead gets in their way
 - Some of it might even inconvenience their friends

Research Goal: Privacy for **Sharing**

1. Develop Algorithms and Systems That...

- allow people to **share data among each other**, without the need for third party data disclosure
- allow people to **publish their data** in order to find new friends, new places, without the need for third party data disclosure
- allow **third parties to aggregate** anonymous user data in order to provide novel services

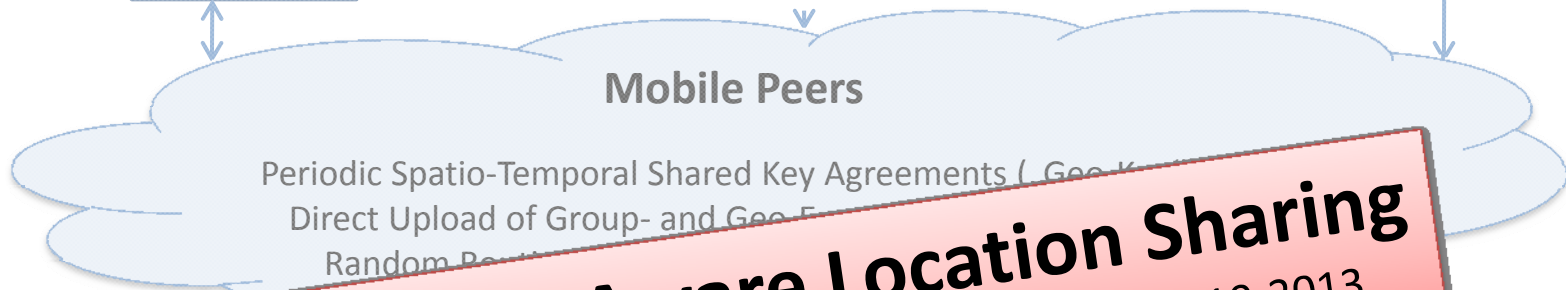
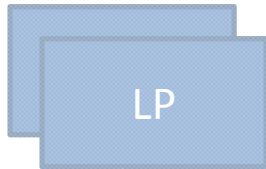
2. Develop „**Personal Information Literacy**“ Program

- Educate users to „**manage**“ their privacy just as they manage, say, their health or stock portfolio
- Develop the tools needed to do so

Location Provider
(e.g., Mobile Operator)

Prototype Alternative to P2P Geo-Key
(facilitates experimental setup w/ few users)

Self-Positioning



Anonymous use

Privacy-Aware Location Sharing

Swiss National Science Foundation, April 2010-2013

Group-based matching and disclosure (in eSpace)

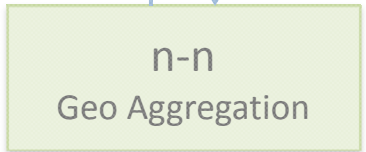
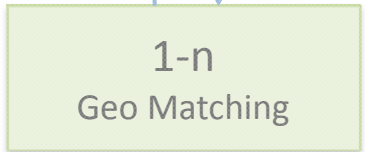
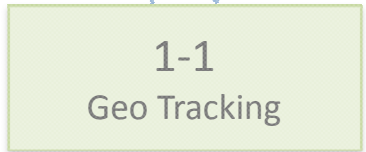
location traces (based on shared-key)

Account-based matching (in eSpace)

Account-based uploads of encrypted location traces (based on geo-key)

Anonymous aggregated city activity (network anonymity)

Anonymous geo-activity upload (time-delayed P2P routing, snippets)



Identified Access

Identified Access

Anonymous Access

Group-Encrypted Location (Location)

Also: ENISA Expert-Workshop „Emerging and Future Risk in ICT“ on Pervasive Micro Blogging (forthcoming)

Anon.Proxy, or Mix Encrypted Location (Snippets)

Service knows users, but not their geo-activity. Other users only know my traces if authorized (shared key)

Service knows users, but not their geo-activity. Other users only know my traces if overlap (i.e., same Geo-keys)

Service only knows anonymous geo-activity. Snippets do not allow RSI attacks by aggregator.