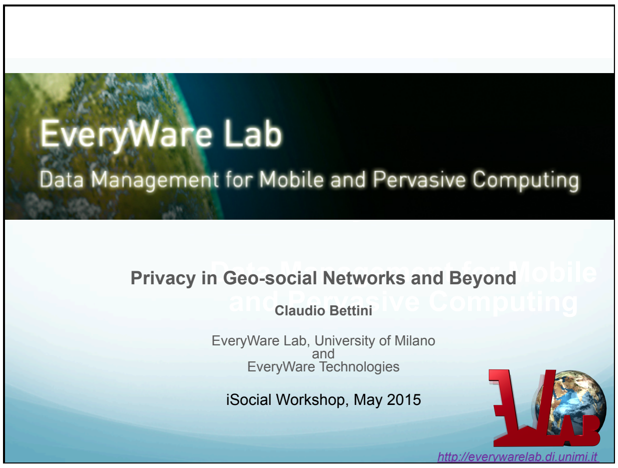


EveryWare Lab

Data Management for Mobile and Pervasive Computing

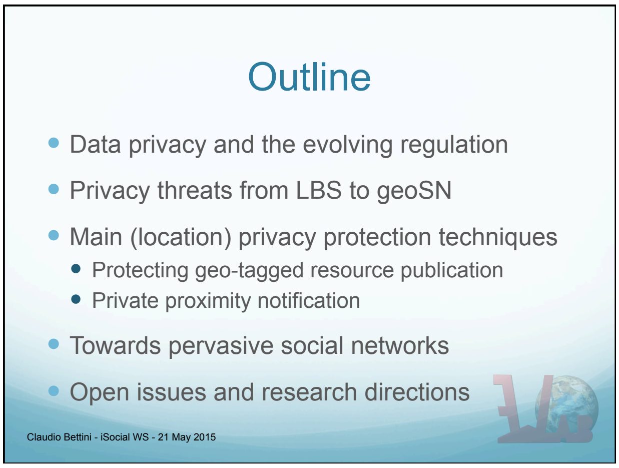
Privacy in Geo-social Networks and Beyond

Claudio Bettini

EveryWare Lab, University of Milano
and
EveryWare Technologies

iSocial Workshop, May 2015

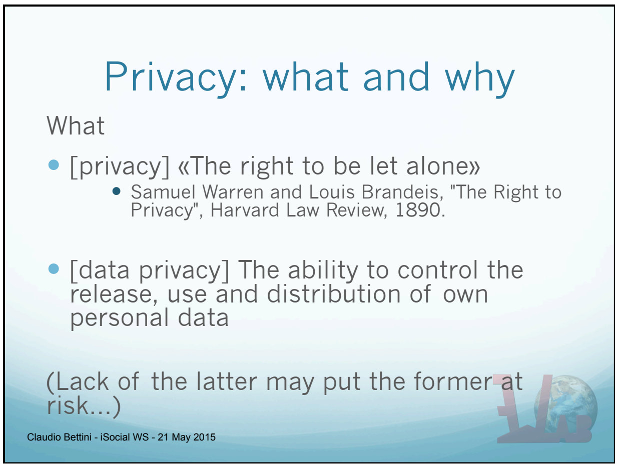
http://everywarelab.di.unimi.it



Outline

- Data privacy and the evolving regulation
- Privacy threats from LBS to geoSN
- Main (location) privacy protection techniques
  - Protecting geo-tagged resource publication
  - Private proximity notification
- Towards pervasive social networks
- Open issues and research directions

Claudio Bettini - iSocial WS - 21 May 2015



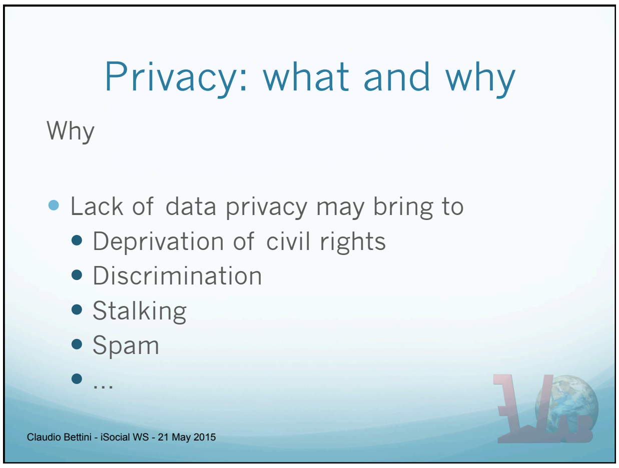
Privacy: what and why

What

- [privacy] «The right to be let alone»
  - Samuel Warren and Louis Brandeis, "The Right to Privacy", Harvard Law Review, 1890.
- [data privacy] The ability to control the release, use and distribution of own personal data

(Lack of the latter may put the former at risk…)

Claudio Bettini - iSocial WS - 21 May 2015

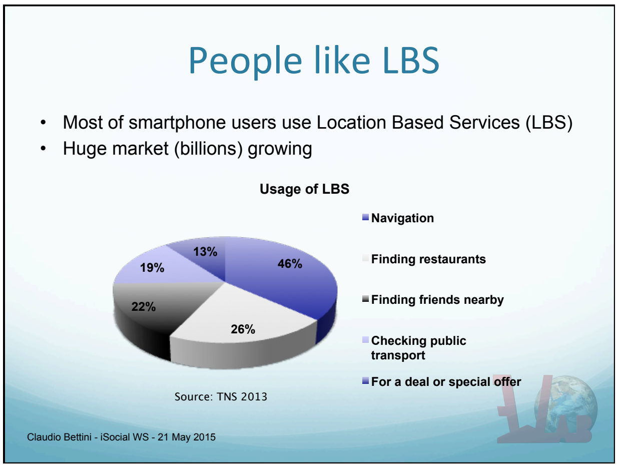


Privacy: what and why

Why

- Lack of data privacy may bring to
  - Deprivation of civil rights
  - Discrimination
  - Stalking
  - Spam
  - …

Claudio Bettini - iSocial WS - 21 May 2015

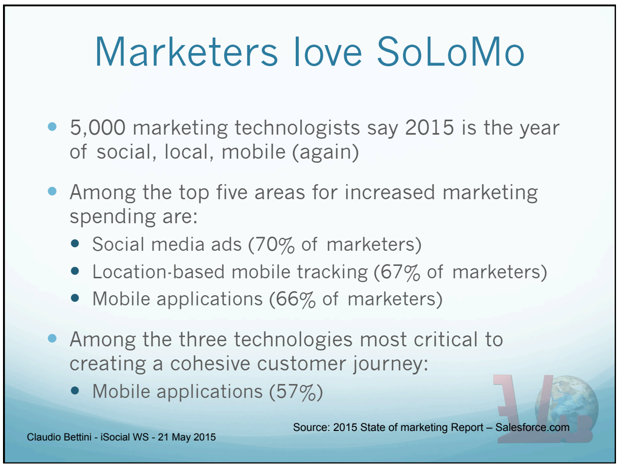


People like LBS

- Most of smartphone users use Location Based Services (LBS)
- Huge market (billions) growing

Source: TNS 2013

Claudio Bettini - iSocial WS - 21 May 2015



Marketers love SoLoMo

- 5,000 marketing technologists say 2015 is the year of social, local, mobile (again)
- Among the top five areas for increased marketing spending are:
  - Social media ads (70% of marketers)
  - Location-based mobile tracking (67% of marketers)
  - Mobile applications (66% of marketers)
- Among the three technologies most critical to creating a cohesive customer journey:
  - Mobile applications (57%)

Source: 2015 State of marketing Report – Salesforce.com

Claudio Bettini - iSocial WS - 21 May 2015

Users care about privacy

From: Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union, June 2011

- 92% of Europeans say they are concerned about mobile apps collecting their data without their consent.
- 70% users said they were concerned about how companies use their data and they think that they have only partial, if any, control of their own data.
- 74% want to give their specific consent before their data is collected and processed on the Internet.

EU Art.29 Data Protection Working Party

- A group of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission.
- Example of results:
  - Opinion 5/2009 on online social networking (SN)
  - Opinion 13/2011 on Geolocation services on smart mobile devices (adopted 16/5/2011)
  - Proposal for new data protection regulations

The data protection reform in EU

- Unique authority: a single set of rules applicable across the EU
- Privacy by default and by design
- Right to be forgotten
- Right to data portability, i.e. the right to obtain a copy of their data from one Internet company and to transmit it to another one without hindrance from the first company

See http://ec.europa.eu/justice/data-protection

On March 12, 2014 the EU Parliament voted in favor of the regulation. It is expected to be in place by end of 2015.

Privacy in the real world

Excerpt from May 2014 'Moves' app privacy policy

- If we sell all or part of our business, make a sale or transfer of assets, are otherwise involved in a merger or business transfer, or in the event of bankruptcy, we may disclose and transfer your personally identifying information to one or more third parties as part of that transaction.
- We may also generally disclose aggregate or anonymous information where reasonable steps have been taken to ensure the data does not contain your personally identifying information.

Privacy in the real world
The case of a Mobile Dating Service

[redacted]

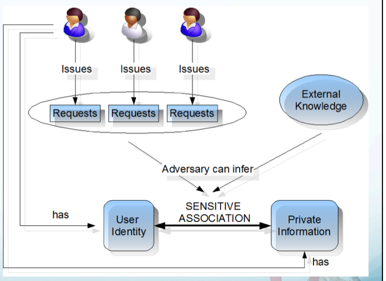
[Fattori et al, IEEE MDM 2013]

Measures in favor of privacy

- Awareness
- Transparency
- Control
- Regulation (Law enforcement)
- Protection
  - is it possible? To what extent?

Privacy threat in online services

- Adversary should not discover "**Sensitive Associations**"
- Location/context info can be used to:
  - Reveal Private Info
  - Reveal identity

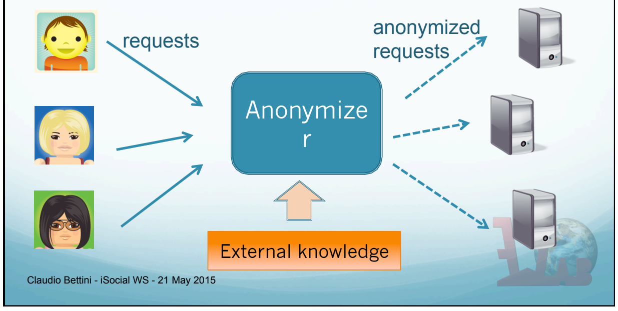


Main protection approaches

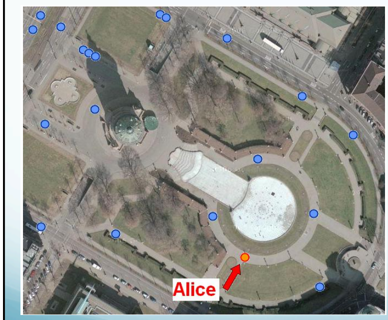
- Anonymity-based solutions protect identity
  - mostly based on pseudoids and spatio-temp. cloaking through trusted server
- Obfuscation-based solutions protect private information
  - based on cloaking, fake locations, multi-step queries, ...
- Crypto- and PIR-based solutions
  - protect the channel AND the query
- Privacy-preserving data analysis
  - ensuring that no individual's data is released or reconstructed

Anonymity architecture

- Centralized trusted server for identity privacy

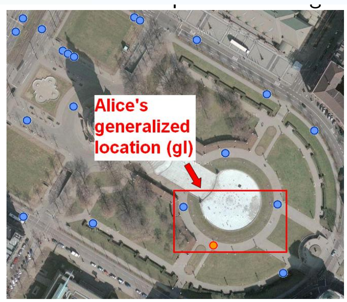


Anonymity enforcement



- Alice issues an LBS request for a veg restaurant
- Private data: she is vegetarian
- Her exact location may reveal her identity

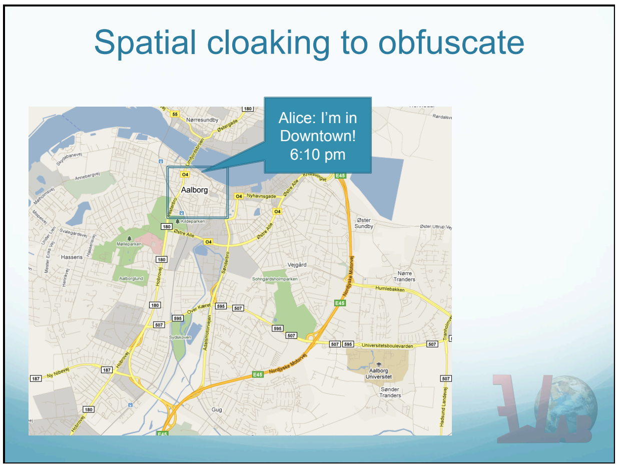
Spatial cloaking for anonymization



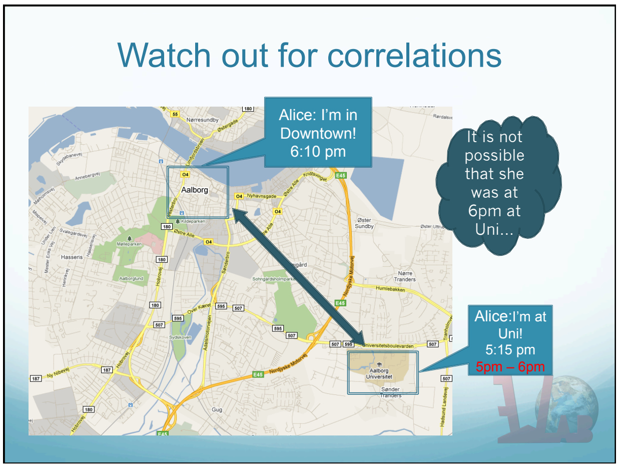
- Alice's request origin is generalized to a region with *k* candidate issuers

Main protection approaches

- Anonymity-based solutions protect identity
  - mostly based on pseudoids and spatio-temp. cloaking through trusted server
- Obfuscation-based solutions protect private information
  - based on cloaking, fake locations, multi-step queries, ...
- Crypto- and PIR-based solutions
  - protect the channel AND the query
- Privacy-preserving data analysis
  - ensuring that no individual's data is released or reconstructed

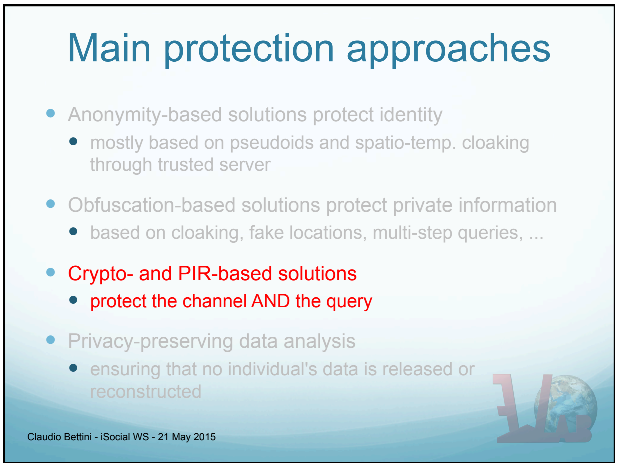


Spatial cloaking to obfuscate



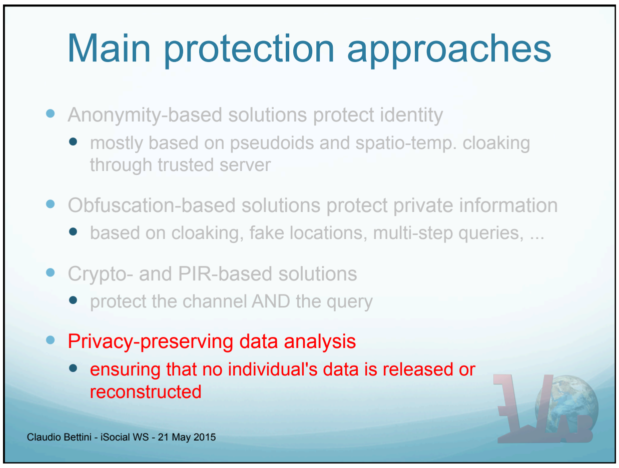
Watch out for correlations

Alice: I'm in Downtown! 6:10 pm
It is not possible that she was at 6pm at Uni…
Alice:I'm at Uni! 5:15 pm 5pm – 6pm
Aalborg



Main protection approaches

- Anonymity-based solutions protect identity
  - mostly based on pseudoids and spatio-temp. cloaking through trusted server
- Obfuscation-based solutions protect private information
  - based on cloaking, fake locations, multi-step queries, …
- Crypto- and PIR-based solutions
  - protect the channel AND the query
- Privacy-preserving data analysis
  - ensuring that no individual's data is released or reconstructed

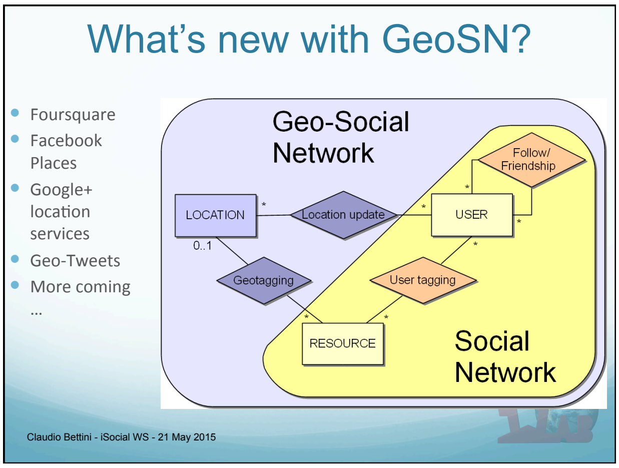


Main protection approaches

- Anonymity-based solutions protect identity
  - mostly based on pseudoids and spatio-temp. cloaking through trusted server
- Obfuscation-based solutions protect private information
  - based on cloaking, fake locations, multi-step queries, …
- Crypto- and PIR-based solutions
  - protect the channel AND the query
- Privacy-preserving data analysis
  - ensuring that no individual's data is released or reconstructed

Wernke et al., A classification of location privacy attacks and approaches. Personal and Ubiquitous Computing 18(1): 163-175 (2014)

… and hundreds of technical papers



What's new with GeoSN?

- Foursquare
- Facebook Places
- Google+ location services
- Geo-Tweets
- More coming

…

Why more difficult in GeoSN?

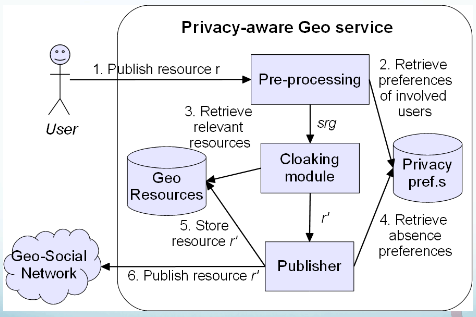
- Users share theirs as well as others' location to multiple users
- so many re-identifying shared data
- In a social context *co-location* may become private information
- Protection of *location* and *absence privacy* becomes trickier

First attempts: WYSE (**W**atch **Y**our **S**ocial st**E**p)

[Freni et al.: Preserving Location and Absence Privacy in Geo-Social Networks, CIKM 2010]

- **Location privacy through obfuscation:**
  1. Start with a spatio-temporal region wide enough to *protect* all tagged users
  2. Consider previously published resources and apply temporal or spatial generalization as needed
- **Absence privacy:**
  1. Delay the publication so that the area of interest cannot be excluded as the current location

WYSE Architecture



One size does not fit all

	Multiple user tagging/check-in	Exact location required	Real-time publication	User identity*
Facebook Places	✓	✓		R
Foursquare		✓		P
Twitter			✓	P
Google Latitude			✓	R
Gowalla		✓		P
MyTown		✓		P
SCVNGR	✓	✓		P
Whrrl		✓	✓	P
MeetMoi		✓	✓	P
Flickr	✓			P
Picasa	✓			P
Brightkite				P

[Ruiz Vicente et al, IEEE Internet Computing, 2011]

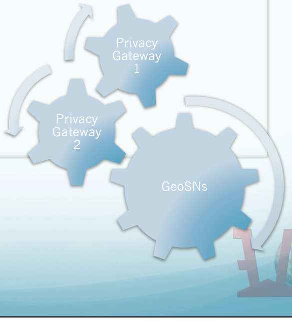
A possible architecture for Multi-GeoSN protection

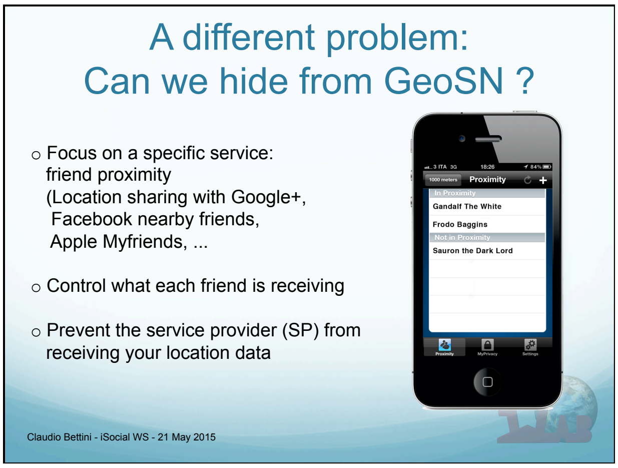
- Postings mediated by Privacy Gateways (PG)
- PG offers transparency by providing to users a view of their released data
- PG alerts for privacy violations and possibly protects

Privacy Gateway
GeoSNs

A possible architecture for Multi-GeoSN protection

- Posts by user A tagging user B forced to verify B prefs through his PG
- A's PG needs to get all location data related to A
- Inferences should be dealt with

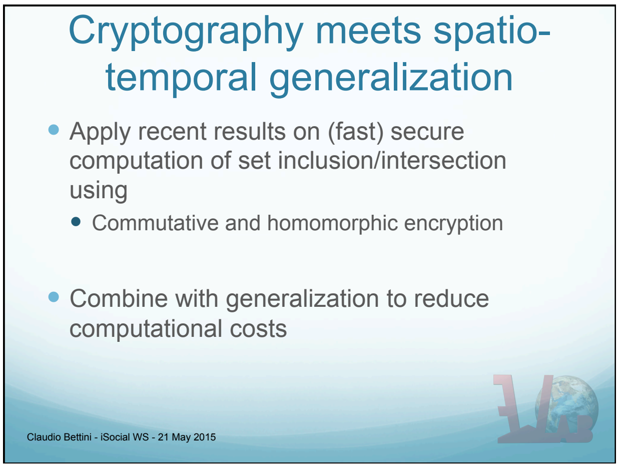




A different problem: Can we hide from GeoSN ?

- Focus on a specific service: friend proximity (Location sharing with Google+, Facebook nearby friends, Apple Myfriends, ...
- Control what each friend is receiving
- Prevent the service provider (SP) from receiving your location data

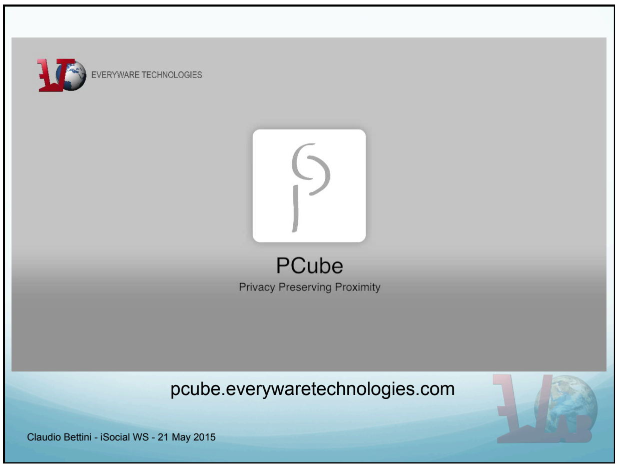
Claudio Bettini - iSocial WS - 21 May 2015



Cryptography meets spatio-temporal generalization

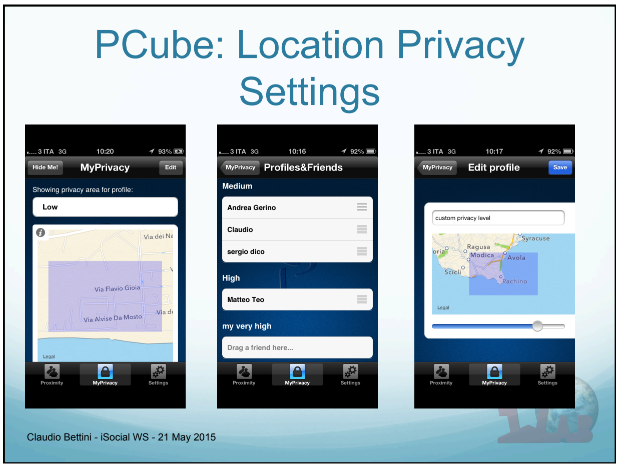
- Apply recent results on (fast) secure computation of set inclusion/intersection using
  - Commutative and homomorphic encryption
- Combine with generalization to reduce computational costs

Claudio Bettini - iSocial WS - 21 May 2015



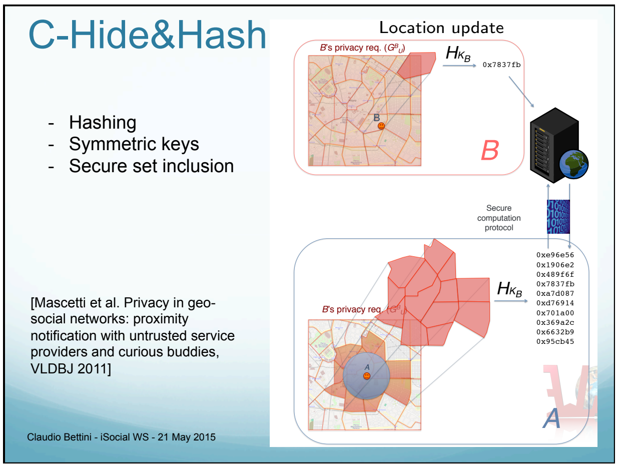
pcube.everywaretechnologies.com

Claudio Bettini - iSocial WS - 21 May 2015



PCube: Location Privacy Settings

Claudio Bettini - iSocial WS - 21 May 2015

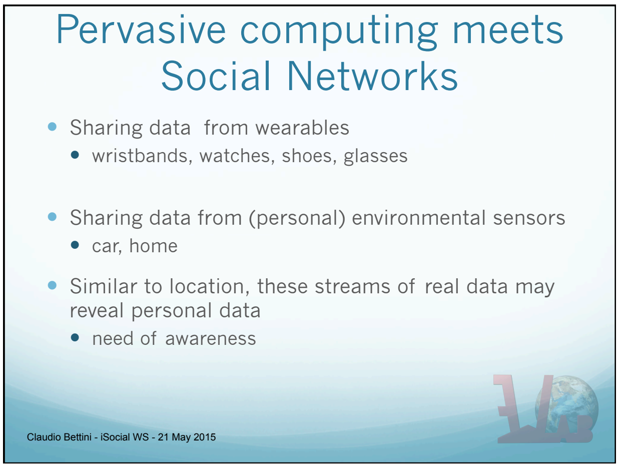


C-Hide&Hash

- Hashing
- Symmetric keys
- Secure set inclusion

[Mascetti et al. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies, VLDBJ 2011]

Claudio Bettini - iSocial WS - 21 May 2015



Pervasive computing meets Social Networks

- Sharing data from wearables
  - wristbands, watches, shoes, glasses
- Sharing data from (personal) environmental sensors
  - car, home
- Similar to location, these streams of real data may reveal personal data
  - need of awareness

Claudio Bettini - iSocial WS - 21 May 2015

Privacy in mobile and pervasive systems

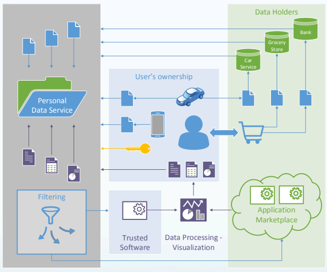
Category name	Adversaries	Sensitive data
Location Based Services	Service provider	Location, absence, co-location
Mobile Advertisement	Service provider, merchant	
Geo-Social Network applications	Service provider, other users	
Participatory sensing	Data collector, service users	Location, sensed data
Health-Care		Location, body-worn sensor data, activity
Well-Being	Service provider	
Vehicular Applications and Smart City services	Other drivers, city and road authorities	Movement traces, driving behavior, user habits
Smart Home and Smart Grid applications	Power companies, home automation service providers	Occupancy, habits and activities

[Bettini-Riboni, Privacy Protection in Pervasive Systems: State of the Art and Technical Challenges PMC Journal, 17(B), 2015]

Overall challenges

- Increase user awareness
  - Tools to monitor global personal data
  - Usable privacy preferences (learning, trust, reputation)
- Regulations to give data back to the user through API
- Support for obfuscation by SN
- Effective crypto and hybrid solutions
- Economically sustainable solutions

An emerging paradigm: PDS



[A. Acquisti et al.: Personal Data Service: Accessing and Aggregating Personal Data, Dagsthul report, 3(7):74-107, 2013]
[openPDS: Protecting the Privacy of Metadata through SafeAnswers, Yves-Alexandre de Montjoye et al., PLOS one, 2014]
[Anciaux et al: Trusted Cells: A Sea Change for Personal Data Services. CIDR 2013]

Thanks for attending this talk

http://everywarelab.di.unimi.it