Universität Karlsruhe (TH)
Forschungsuniversität • gegründet 1825

Karlsruhe Institute of Technology

Talk at Entropia/CCC Karlsruhe, 01. Mar. 2009

Thoughts and Experiments about **Privacy 2.0: Towards Collaborative Data-Privacy Protection**

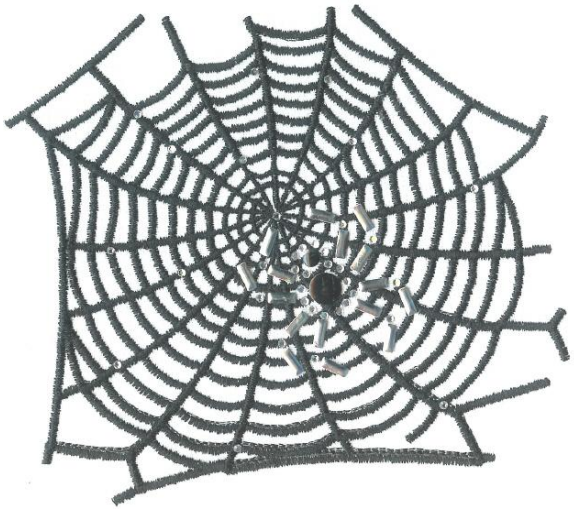
***Erik Buchmann**, Klemens Böhm, Oliver Raabe*
Universität Karlsruhe (TH), Germany

Outline

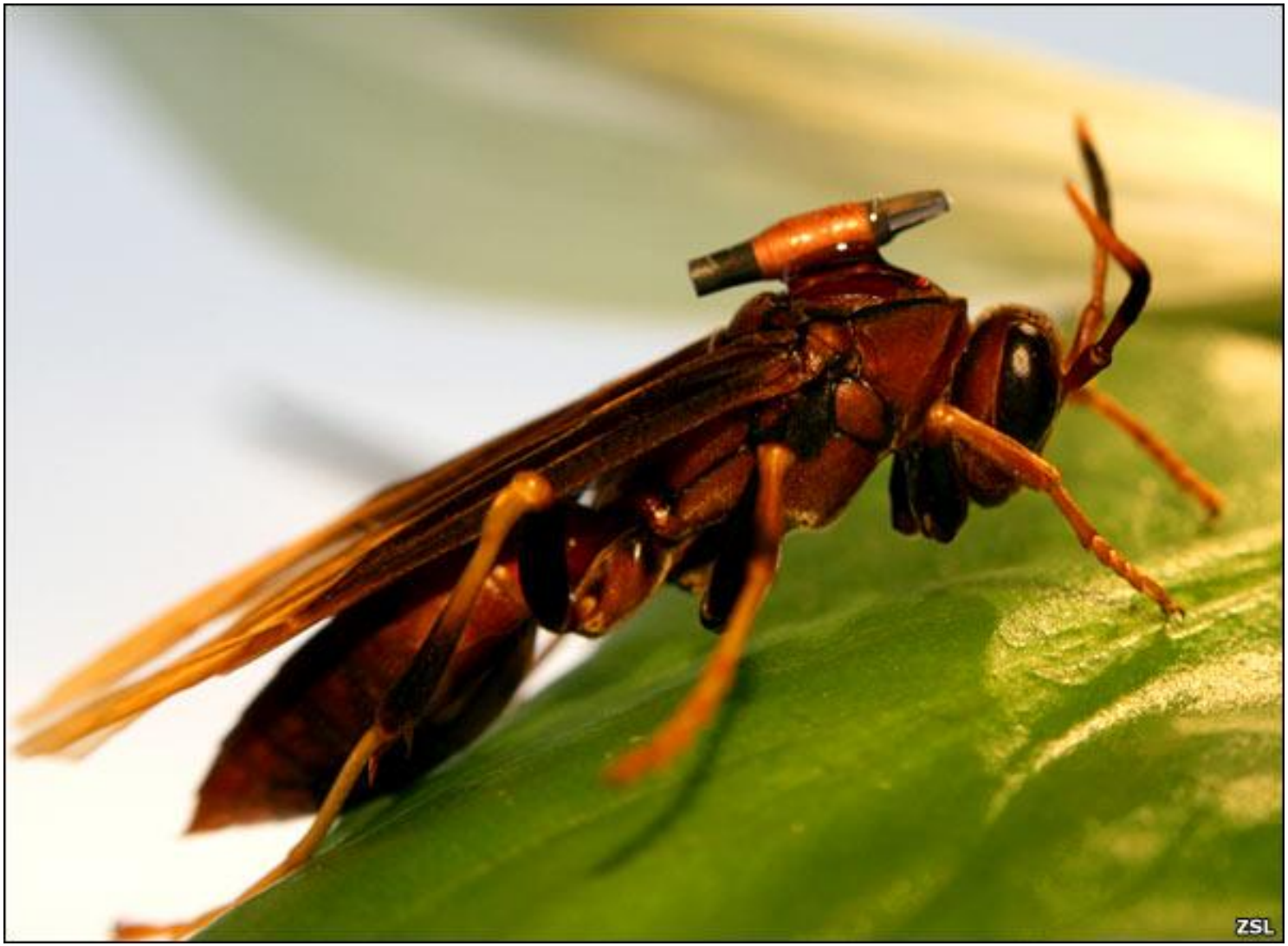
- Motivation
- Our vision: Web2.0 for privacy protection
- Realization issues
- Call for Study Volunteers

Classical Data-Privacy Protection

- Two historical building blocks:
  - protect the citicen from the gouvernment
    - right of free speech is meaningless if gouvernment can trace (and punish) the speaker
      → *privacy protection is important for democracy*
  - protect the customer from private enterprises
    - problem: customer can be remotely controlled if his deepest wishes, intentions and needs are known
      → *privacy protection is consumer protection*



Today: New Challenges



Wasp with RFID-Tag, Picture*: Zoological Society of London*

What has Changed?

- Omnipresent, personalized IT devices and applications penetrate our daily lives
  - Sensor Networks
  - Ubiquitous Computing
  - Location-based Services
  - RFID
  - ...

- Increasing complexity of IT infrastructure
- Loss of privacy as unavoidable secondary effect
- People disclose data voluntarily/unintentionally
- Personal information with an amazing level of detail

Existing Approaches for Privacy Protection

- Laws and regulations
  EU directives (95/46/EC et al.), national laws
  - e.g., german law has ~1,500 regulations, vague terms
    → **execution is challenging**

- Self-regulation
  Safe Harbor, Privacy Code of Conduct, Trust-Seals
  - many intransparent approaches
    → **too nebulous for many users**

- Privacy enhancement technologies
  P3P, Spatio-temporal Cloaking, TOR-Networks
  - complex, isolated technologies for different protocols
    → **impossible to realize consistent privacy goals**

Internet Options

General | Security | Privacy | Content | Connections | Programs | Adva

Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiabl information without implicit consent

Sites... | Import... | Advanced... | Default

Pop-up Blocker

Prevent most

Block pop

Allowed sites:

support.euro.dell.com
www1.euro.dell.com

Remove All

Specifies that you do not want Internet Explorer to use a Web site's P3P privacy policy to determine whether or not to allow the Web site to save a cookie on your computer. If you select this check box, you must specify below how you want Internet Explorer to handle first-party and third-party cookies.

A cookie is a file created by a Web site that stores information on your computer, such as your preferences when visiting that site. A first-party cookie is one that either originates on or is sent to the Web site you are currently viewing. A third-party cookie is one that either originates on or is sent to a different Web site than the one you are currently viewing.

For more information about cookies, see Internet Explorer Help.

Per Site Privacy Actions

Manage Sites

You can specify which Web sites are always or never allowed to use cookies, regardless of their privacy policy.

Type the exact address of the Web site you want to manage, and then click Allow or Block.

To remove a site from the list of managed sites, select the name of the Web site and click the Remove button.

Address of Web site:

Block

Allow

Managed Web sites:

Domain	Setting
.advertising.com	Always Block
.atdmt.com	Always Block
engage.com	Always Block
	Always Block

Remove

Remove All

ced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

kies

Override automatic cookie handling

First-party Cookies	Third-party Cookies
Accept	Accept
Block	Block
Prompt	Prompt

Always allow session cookies

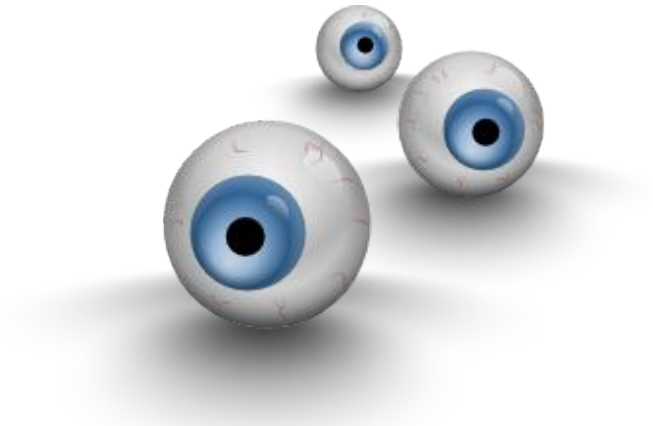
What is Needed Tomorrow?

- Holistic Approaches
  - it must be possible to realize privacy goals across the borders of technologies and protocols
- Social Standards
  - ethics about handling private data disclosed voluntarily
- Compatibility with Ubiquitous Computing
  - approaches must not consume much user attention
- Transparency
  - any flows of personal data must be traceable
- Simple use
  - users don't want to bother technological details

Our Vision: Web2.0 Technology for Privacy

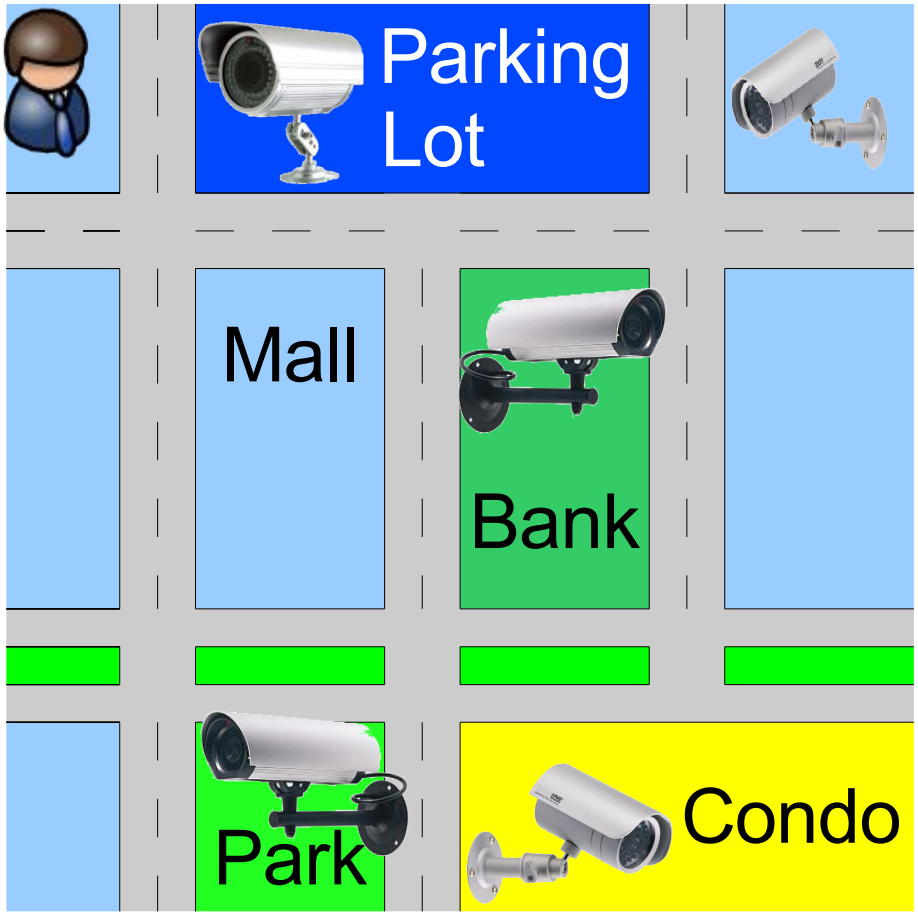
- Users provide **tags** for potential privacy threats in a **folksonomy**
  - many people observe the data collectors
  - simple use
  - best-effort-approach
- "**Proximity Alarm**" when privacy is in danger
  - "collective intelligence" evaluates privacy threats
  - user receives a warning when his awareness is required

What can we Tag?

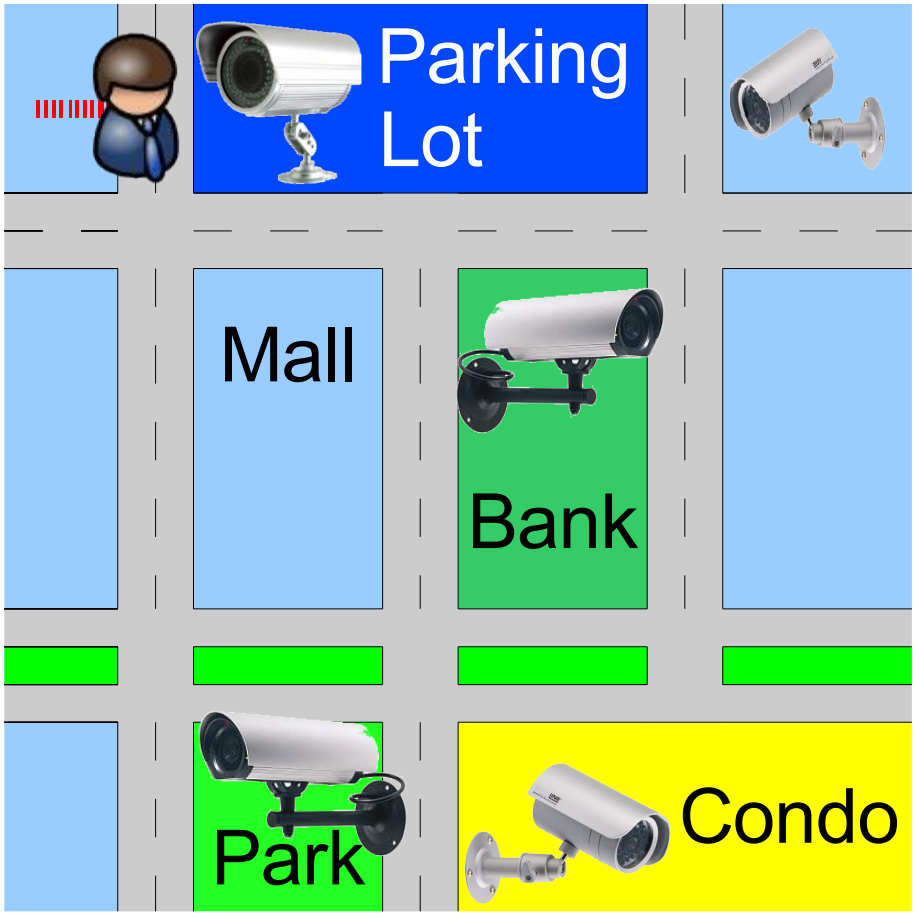


- **Locations**
  - malls using RFID technology but don't kill the tags
  - hidden surveillance cameras
  - road toll stations where license plates are scanned
- **URLs in the Internet**
  - search engines with improper data handling practices
  - social sites where personal information are displayed
- **Physical items equipped with RFID labels**
  - networked Ubicomp devices that monitor the user without his explicit consent
  - personalized identification cards with RFID tags inside

Tagging Privacy-relevant Objects

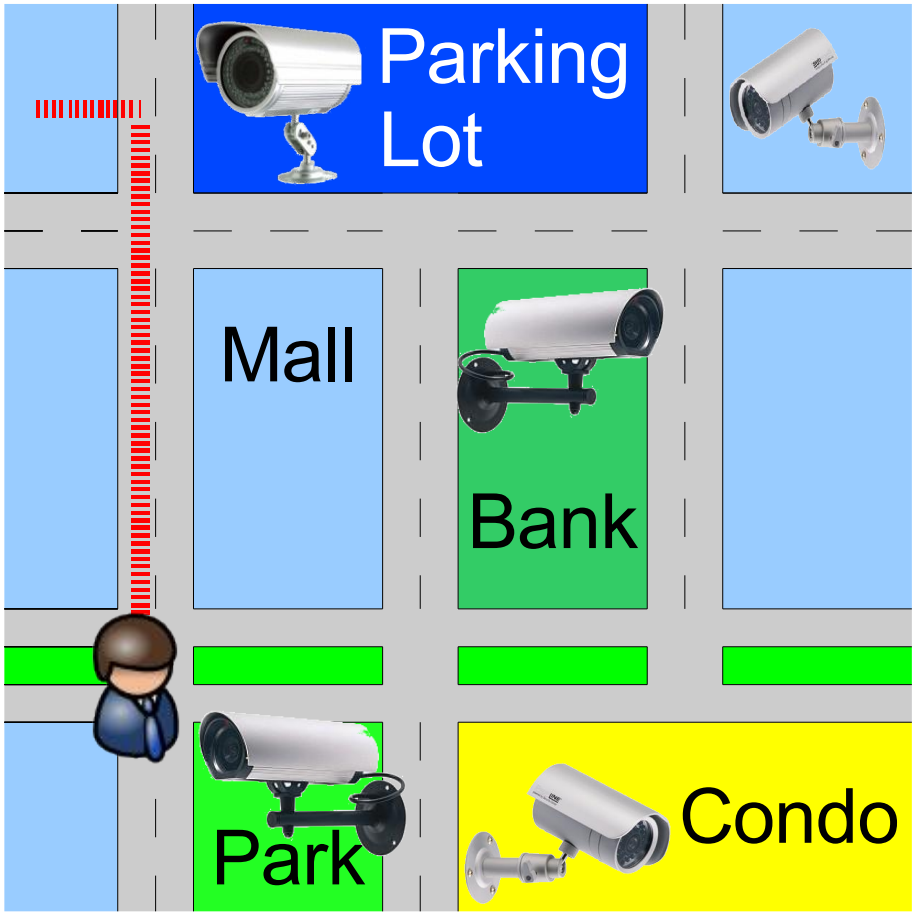


Tagging Privacy-relevant Objects



{  , garage, {safe, great!}}

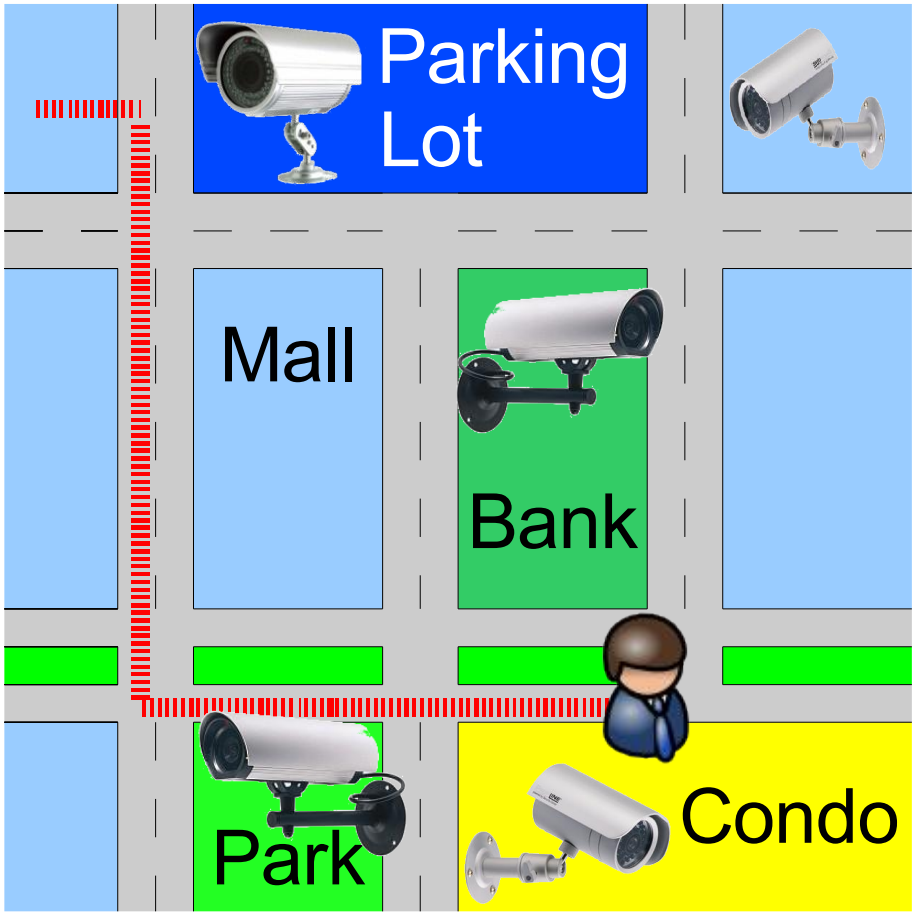
Tagging Privacy-relevant Objects



{ , garage, {safe, great!}}

{ , park, {sneaky, cam}}

Tagging Privacy-relevant Objects



{ , garage, {safe, great!}}

{ , park, {sneaky, cam}}

{ , house, {webcam, evil}}

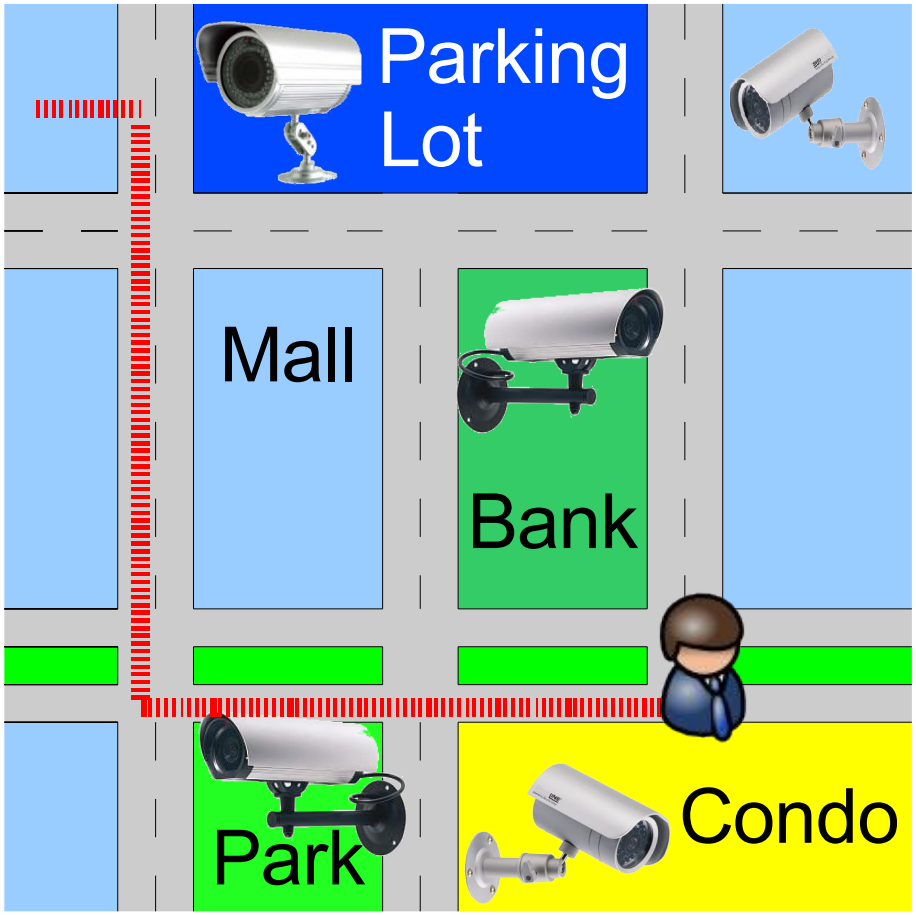
The Folksonomy of Privacy Tags

- Folksonomy contains tags from many users
  - uncritical items, urls or locations remain untagged: folksonomy converges against **social standards**
  - community **prevents misuse**, e.g., spoof tags

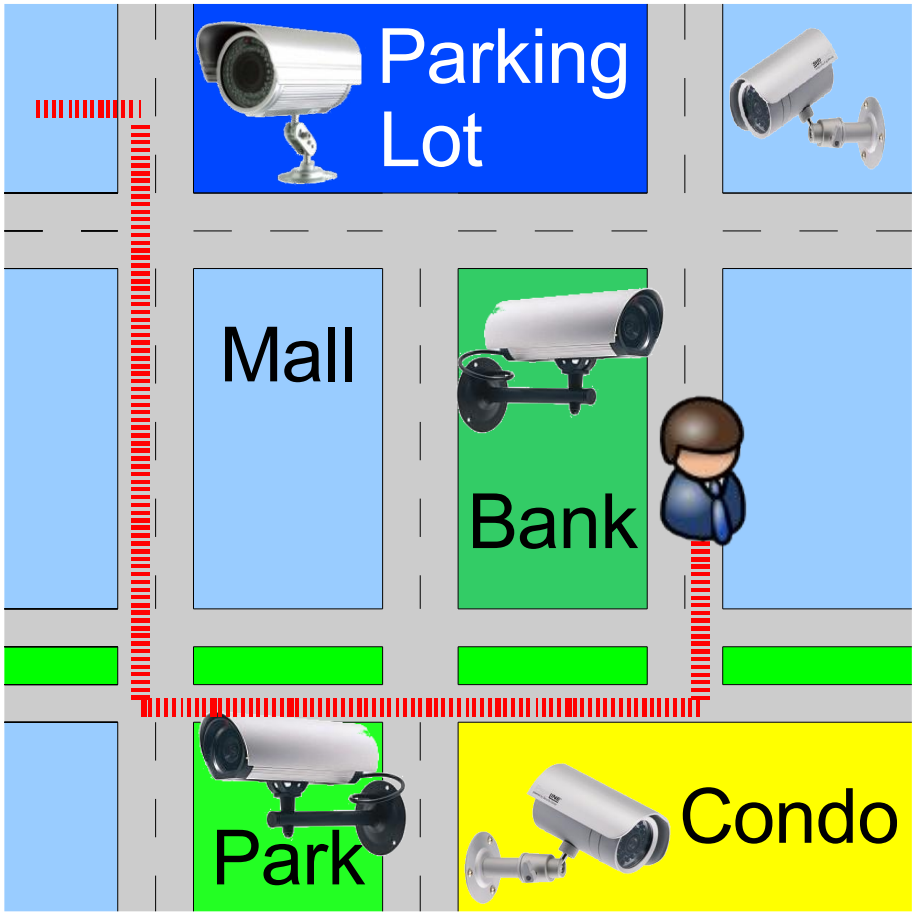
- <*tag, user, object*> tuples allow to evaluate
  - **user preferences:** tags, objects from one user
  - **quality of a threat:** semantic of the tags related to one object
  - **similar threats**: related objects, objects connnected over similar tags

- Our goal: inform the user if he has to consider threats

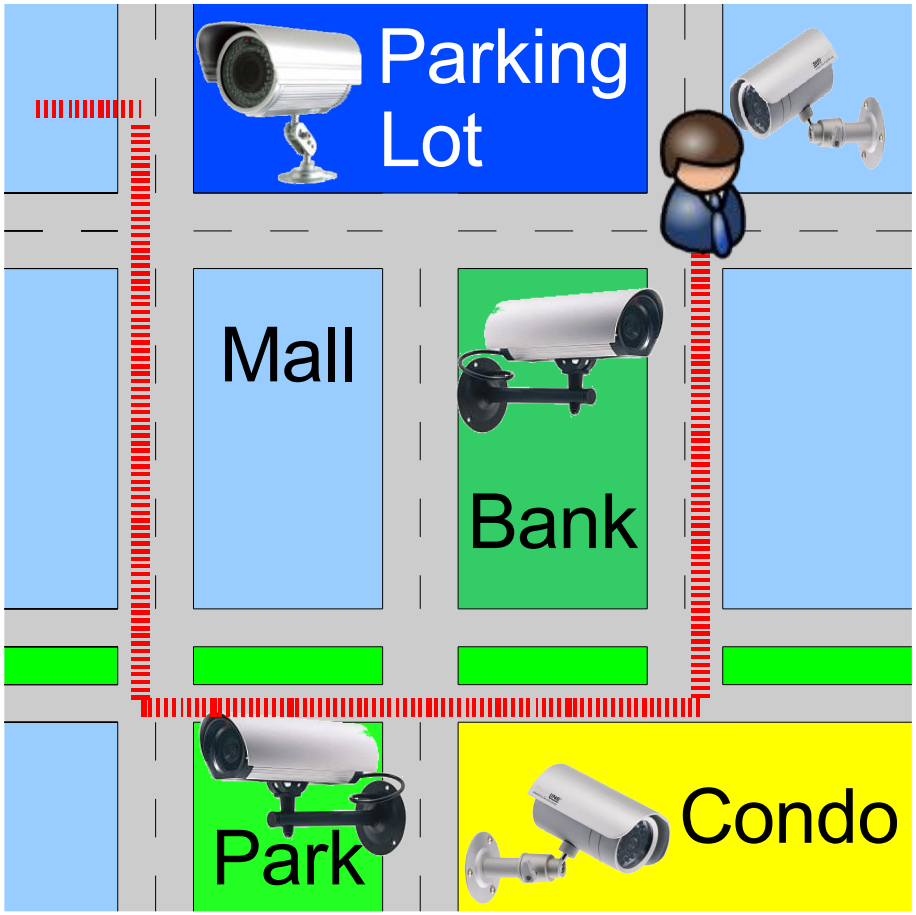
Proximity Alarm



Proximity Alarm



Proximity Alarm

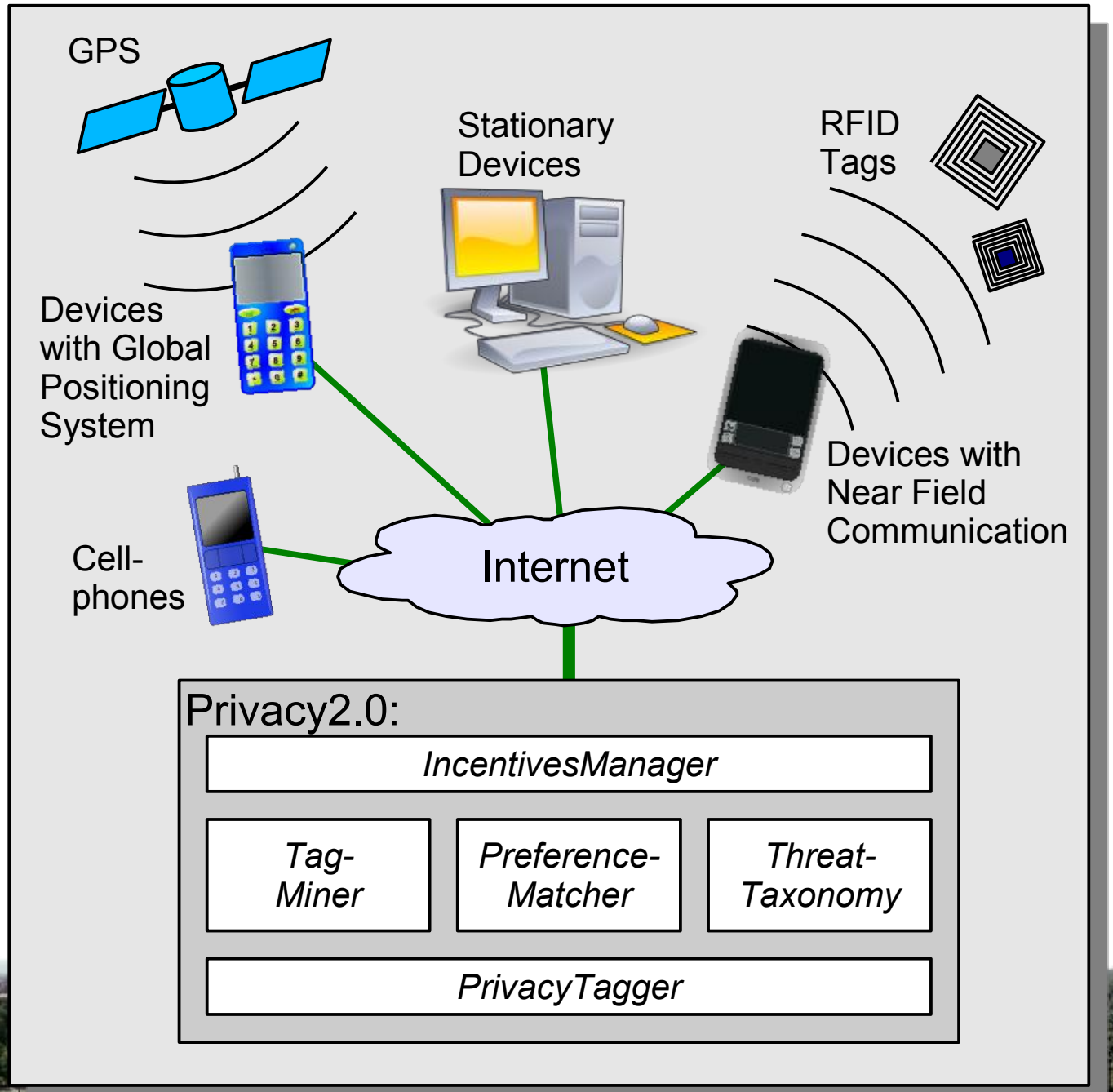


How Does it Work?

1. Collecting tags

2. Evaluating threats

- identify similar objects
- identify tag semantics
- identify similar users
- *if similar users find similar objects threatening, alert the user*



Evaluating a Query

{ , garage, {safe, great!}}

{ , park, {sneaky, cam}}

{ , house, {webcam, evil}}

{ ,Park ,{video, control, awesome!!!}}

{ ,ATM ,{observed, obscure, bank}}

{ ,Home ,{fine, home, security, camera}}

{ ,ATM ,{discreet, surveillance}}

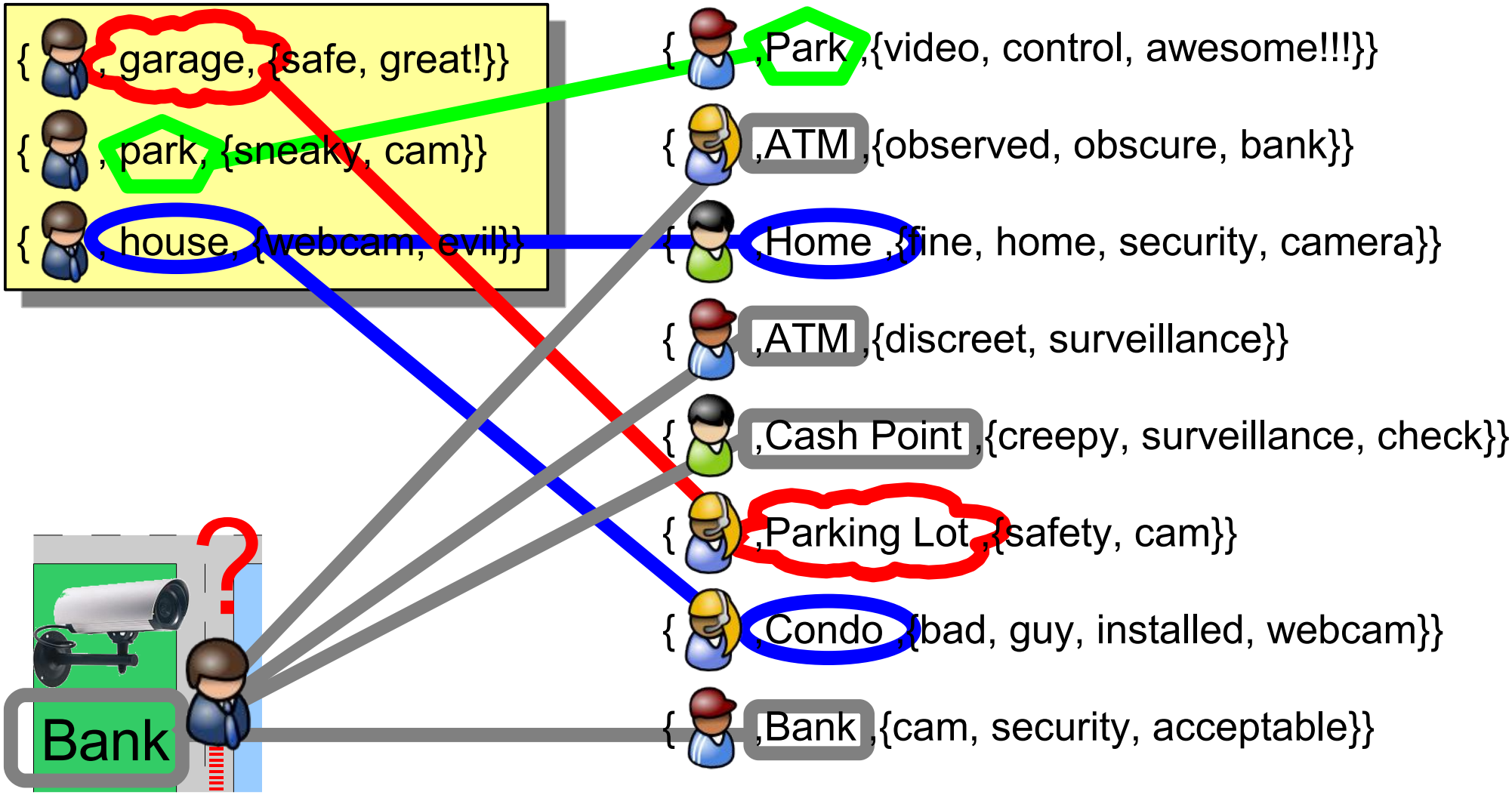
{ ,Cash Point ,{creepy, surveillance, check}}

{ ,Parking Lot ,{safety, cam}}

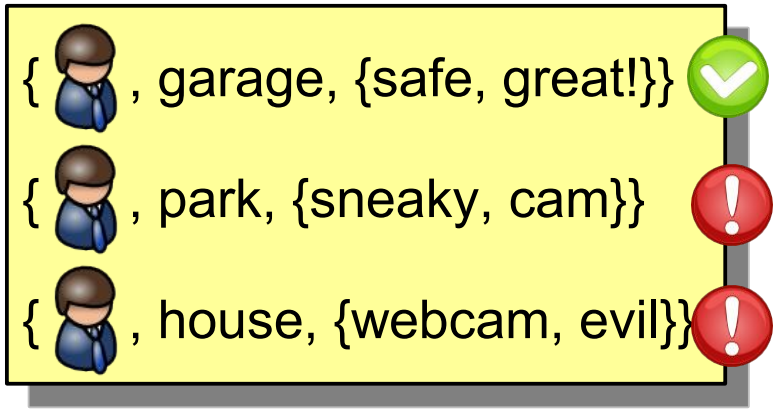
{ ,Condo ,{bad, guy, installed, webcam}}

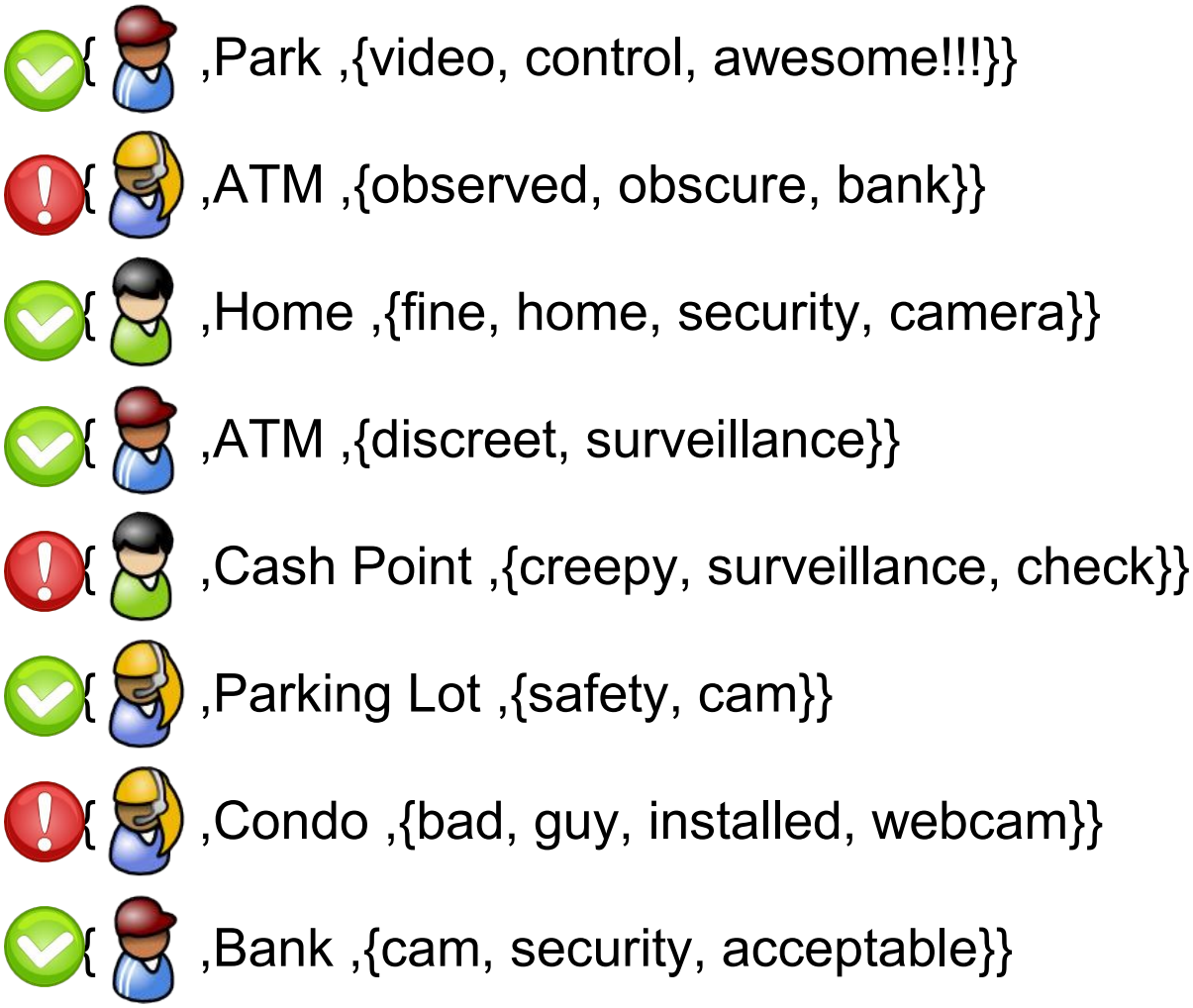
{ ,Bank ,{cam, security, acceptable}}

1. Identifying Similar Objects

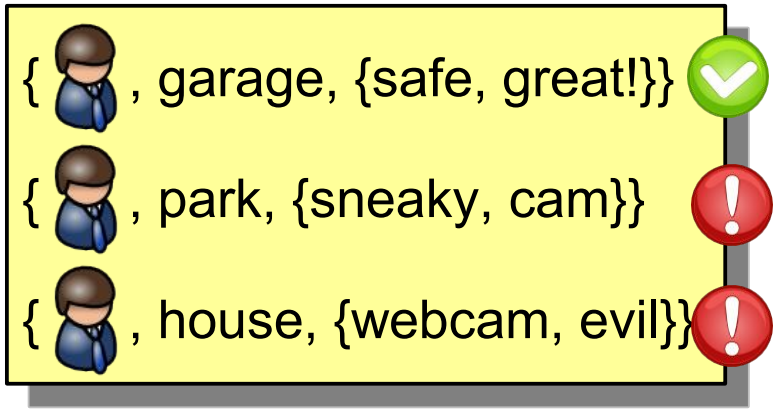


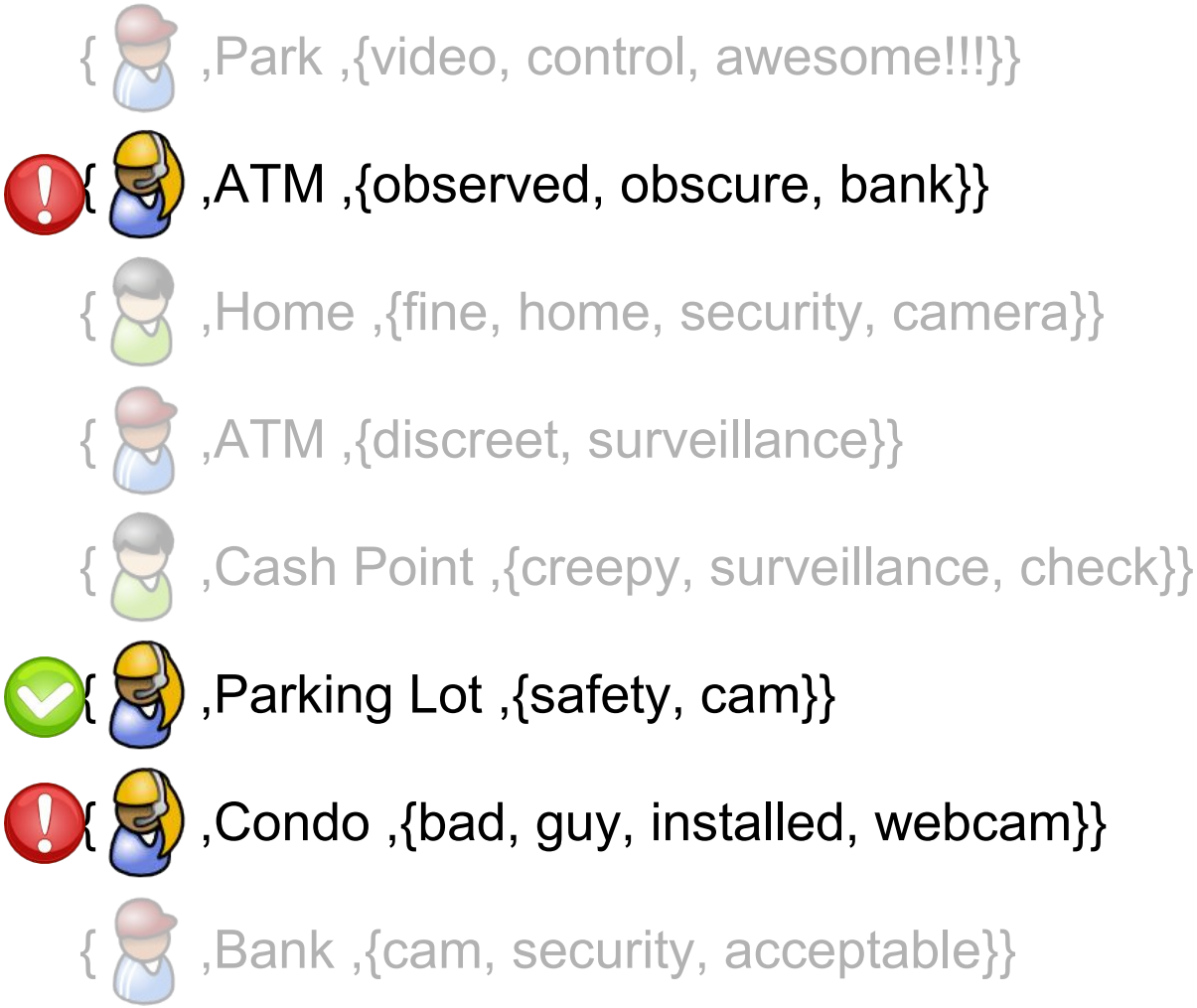
2. Identifying Tag Semantics





3. Identifying Similar Users





4. Come to a Descision

{ , garage, {safe, great!}}

{ , park, {sneaky, cam}}

{ , house, {webcam, evil}}

{ ,Park ,{video, control, awesome!!!}}

{ ,ATM ,{observed, obscure, bank}}

{ ,Home ,{fine, home, security, camera}}

{ ,ATM ,{discreet, surveillance}}

{ ,Cash Point ,{creepy, surveillance, check}}

{ ,Parking Lot ,{safety, cam}}

{ ,Condo ,{bad, guy, installed, webcam}}

{ ,Bank ,{cam, security, acceptable}}

A Vision With Many Open Challenges

- Legal aspects
  - slander, gossip, opinions without reason
    - cf. eBay reviews: many existing lawsuits
- Social issues
  - interactions of many people
    - representativeness, amplification of misjudges?
  - vulnerability against misuse?
    - existing Web2.0 approaches work fine
- Technical aspects
  - Does the system induce new privacy threats?
    - obviously yes, but we think the benefits outweigh
  - how to implement the system, performance issues

Evaluation by User Studies

- We have implemented
  - a TaXor server that allows to assign tags to URLs
  - a Firefox 3 plugin which connects to the TaXor server

- We want to know
  - how do people perceive our approach?
  - which kind of tags will be generated on privacy-relevant issues?
  - is the approach generally considered helpful w.r.t. privacy?

- *On the following slides: screenshots of our plugin*

TaXor :: Login - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://localhost:8080/taxor/login!input?login=

Google

TaXor :: Login

TaXor ALPHA

Objekt anlegen | TaXor du

Login

Login-Name:

Passwort:

TaXor Version 0.9 alpha (Build 59

Add-ons

Add-ons herunterladen | Erweiterungen | Themes | Plugins

Java Quick Starter 1.0

JavaScript Debugger 0.9.87.4
JavaScript debugger and profiler

JSONovich 0.9.2
Pretty prints JSON content. Uses json2.js to parse the JSON and google-code-prettify to ...

TaXor Privacy2.0 0.1
This extension allows to tag web sites and offers privacy enhancing technologies calculated using folksonomy data.

Einstellungen | Deaktivieren | Deinstallieren

Aktualisieren

Fertig

Burg Pyrmont ~ Übersicht - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.burg-pyrmont.de/

Burg Pyrmont ~ Übersicht

Burg Pyrmont

Burg Besichtigen Speisen Mieten Heiraten Termine Kontakt

Events, Lebensfreude &

Willkommen auf Burg Pyrmont

In einer einzigartigen Atmosphäre verbindet Burg Pyrmont das Gestern mit dem Heute.

Die Burg aus dem 13. Jahrhundert wurde in den Jahren 1963–67 von den Architekten Prof. Hentrich und Senator Petschnigg wieder aufgebaut. Sie diente mehrere Jahrzehnte als Ideenschmiede und Gästehaus für das renommierte Architekturbüro HPP in Düsseldorf. Noch heute ist sie ein Ort der Begegnung – im Geiste der Architekten.

Burg Pyrmont ist eine Burg die lebt. Bei

Tag-Eigenschaften

Privacy 2.0 Extension

Tag-Eigenschaften

Name:

-

Gefahren-Einschätzung:

1

OK Abbrechen

Die Burg ist Mittwoch bis Sonntag sowie an Feiertagen geöffnet.

- Mittwoch bis Samstag 11.00 – 16.00 Uhr

Tags:

Burg (1)

Tagger:

Fertig

heise online - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.heise.de/ rottenneighbor

heise online

heise online · c't · iX · Technology Review · Telepolis · mobil · Security · Netze · Open Source · Developer · Resale · Foto · Autos · c't-TV

Download · Stellenangebote · Preisvergleich · IT-Markt · heisetreff · Veranstaltungen · Whitepapers · Abo&Heft · Archiv

heise online

Sie sind Gast · Einloggen | Registrieren Suche

Home Newsticker 7-Tage-News News-Archiv Leserforum Newsletter News mobil RSS

heise online

Angela Merkel: Schnelles Internet für alle

In ihrer Video-Botschaft forderte die Bundeskanzlerin Breitbandanschlüsse für alle - auch für die 730.000 Haushalte, für die schnelles Internet noch nicht verfügbar sei. Mit Geldern aus dem Konjunkturpaket ließen sich die Voraussetzungen schaffen. mehr...

- Breitband-Internet bis Ende 2010 überall
- Von weißen und grauen Flecken

Die Deutsche Telekom baut um

"Die Trennung zwischen Festnetz und Mobilfunk soll aufgehoben werden. Produktentwicklung, IT und Technik

Open Source fürchtet Microsofts Patentkeule

Führende Köpfe der freien Softwareszene sehen in Microsofts Patentklage gegen

Technology Review:
Mobiles Internet
Spaß mit den Kleinen

Telepolis
Russland: Jagd auf Journalisten
"Täter dürfen sich stillschweigend ermutigt fühlen"

heise Foto
Gewinnspiel bei heise Foto
Jetzt bei unserer Foto-Galerie anmelden und einen iPod Touch gewinnen!

Neue White Date

Produk namhaf

auf heis

Wh

Tags:

Flash-Spam (1)

Tagger:

Fertig

Conclusion

- Integration of future technologies into the everyday life requres holistic, simple approaches that reflect social standards

- Vision: Web2.0 technologies for data privacy protection
  - community observes violations against privacy
  - best-effort approach, tags consider things of interest
  - ubicomp-compatible approach requires user awareness if necessary only

- Evaluation by user studies:
  - **Please register at http://experiments.ipd.uka.de**

References

- Referee: Dr.-Ing. Erik Buchmann,
  Uni Karlsruhe (TH), IPD,
  Lehrstuhl für Systeme der Informationsverwaltung
  - http://www.erikbuchmann.de
- Project Homepage
  - http://taxor.ipd.uka.de
- Experiment Homepage
  - http://experiments.ipd.uka.de
- Literature
  - Erik Buchmann, Klemens Böhm, and Oliver Raabe. Privacy2.0: Towards Collaborative Data-Privacy Protection. In Proceedings of the IFIPTM'08, 2008.