Making Privacy a Fundamental Component of Web Resources

Paper presentation at
W3C Workshop on Privacy for Advanced Web APIs
July 12/13, 2010, London

Dr. Thomas Dübendorfer
thomas.duebendorfer@google.com
Tech Lead, Privacy Engineering Team Zurich
Google Switzerland GmbH

joint work with
Christoph Renner (Google Switzerland GmbH/ETH Zurich),
Tyrone Grandison (IBM), Michael Maximilien (IBM), Mark Weitzel (IBM)

Picture sharing in social networks

[redacted]

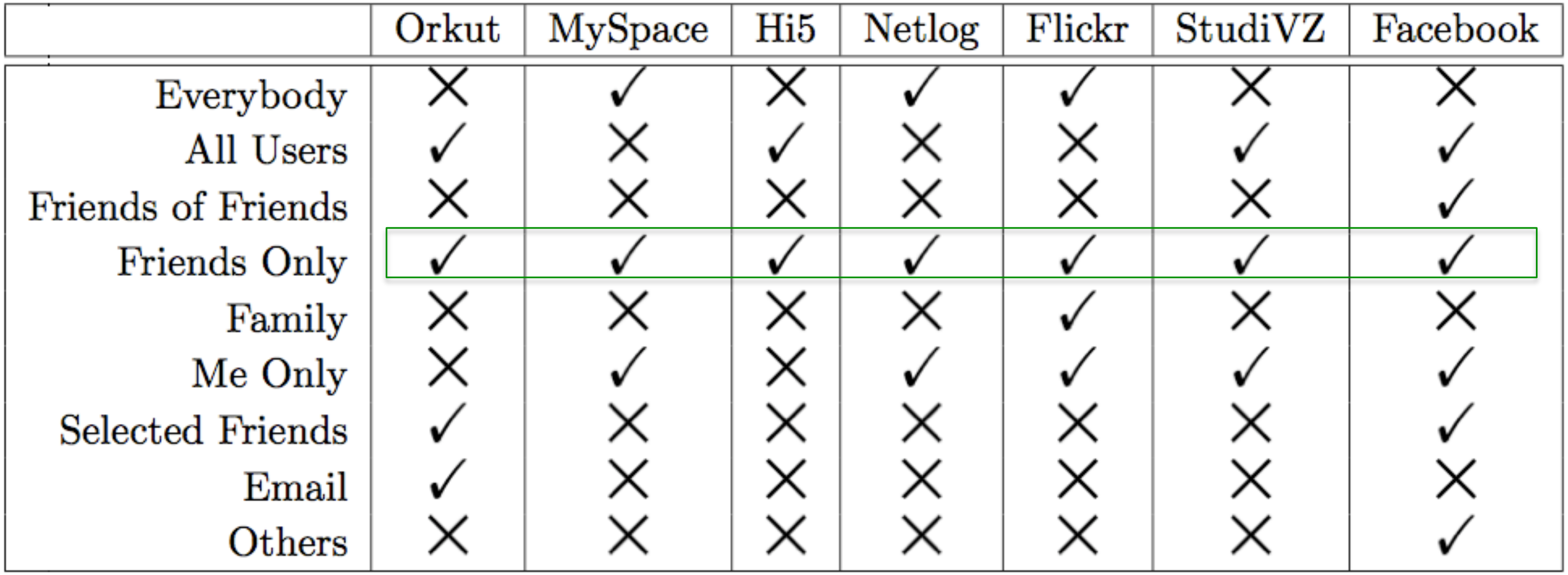
You better know who you share your pictures with!

image source: http://thebsreport.files.wordpress.com/2009/12/crazy-drunk-man-1.jpg

How to improve privacy?

- Better **transparency** on how personal data is shared on the Web
- More **control** over how personal data is shared on the Web
- Put the right security building blocks in place to build privacy features on top of them

Photo albums privacy levels in social networks (as of Nov 2009)



	Orkut	MySpace	Hi5	Netlog	Flickr	StudiVZ	Facebook
Everybody	✗	✓	✗	✓	✓	✗	✗
All Users	✓	✗	✓	✗	✗	✓	✓
Friends of Friends	✗	✗	✗	✗	✗	✗	✓
Friends Only	✓	✓	✓	✓	✓	✓	✓
Family	✗	✗	✗	✗	✓	✗	✗
Me Only	✗	✓	✗	✓	✓	✓	✓
Selected Friends	✓	✗	✗	✗	✗	✗	✓
Email	✓	✗	✗	✗	✗	✗	✗
Others	✗	✗	✗	✗	✗	✗	✓

Conclusion: Sharing granularities in social networks differ a lot!

Everybody = any Internet user, also outside the social network
All Users = any user of the social network

APIs to access photo album privacy settings in social networks

Controlling who has access to my images

- **Facebook**: Proprietary API for privacy settings
- **MySpace**: Proprietary API extensions for albums
- **OpenSocial** API (36 social networks,
  e.g. Orkut, MySpace, LinkedIn, hi5, XING):
  No API to access privacy settings up to current version 1.0 (March 2010); „default“ sharing for uploads

⇨ Clear need for a standardized way to access privacy settings across social networks!

How to give the user control over his personal data on the web?

- Define generic access control lists for shared Web resources
- Make them available in APIs
- Add privacy controls to user interfaces of apps uploading personal data to the Web

- Feb 28th, 2010: Proposal for privacy API (generic access control lists) submitted for inclusion in OpenSocial 1.1.

Generic Access Control Lists – some challenges and features

- **Entities**
  - – Finding the balance between too few and too many while keeping it extensible (CUSTOM) and simple
    - OpenSocial:
      - – USER, GROUP, EXTERNAL CONTACT
      - – Group-ID = Object-Id / "@self" (for owner) / "@friends” (networkDistance for friends of friends) / "@all" / "@everybody" / "@family”
      - – External Contact AccessorId = "MAILTO" / "PHONE" / Custom-Accessor-Type Custom-Accessor-Type = LOALPHA TEXT

Generic Access Control Lists – some challenges and features

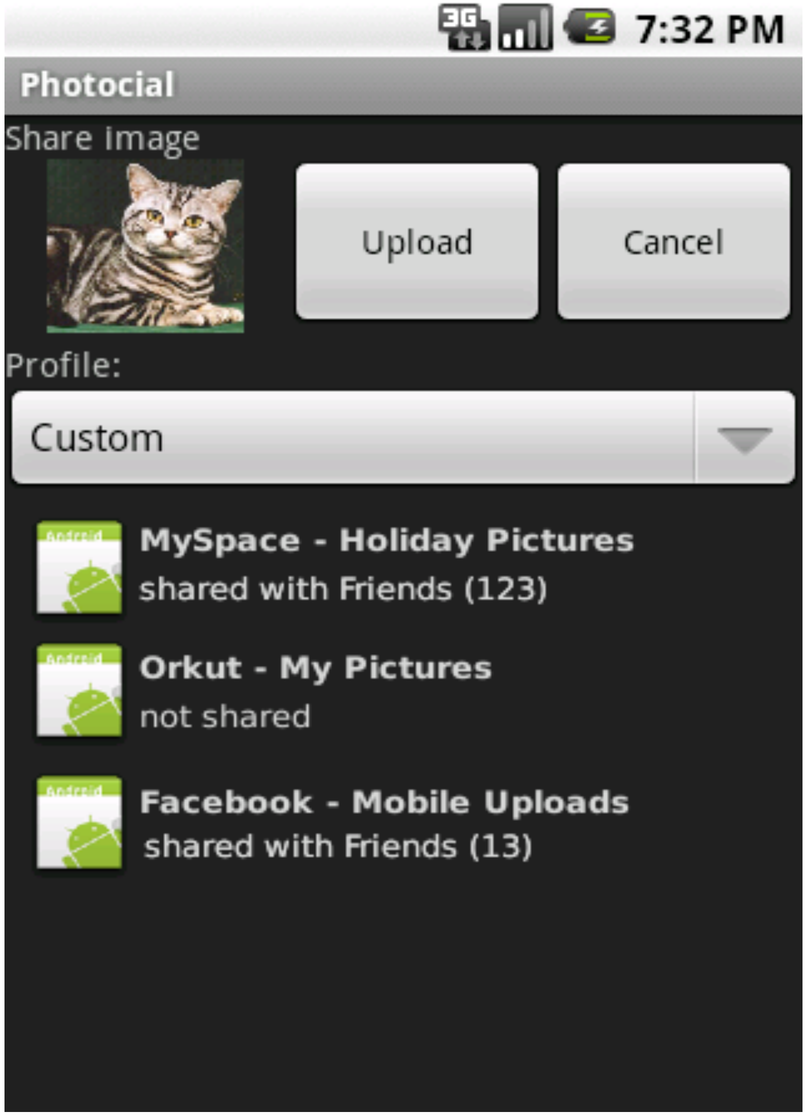
- **Rights**
  - How to define appropriate rights that can be enforced
    - OpenSocial RESTful API:
[“GET”, “POST”, “PUT”, “DELETE”]
- **Sharing model**
  - Additive (whitelist) vs. Subtractive (all but blacklist) or a combination
  - Issues with hidden memberships in large groups
  - Issues with hidden data item groupings (user profile)

Generic Access Control Lists – some challenges and features

- **Sharing with open membership groups**
  - – You share with 10 known group members today, but 1000 members tomorrow (including your boss?)
  - – Social networks might not want to share member lists
- **Privacy indicator**
  - – Number of people with read access
- **Inheritance of rights**
  - – Photo album ACL can be overriden by single image ACLs

Proof of Concept

- Generic access control lists implemented in Google’s social network “Orkut”
- Photo Sharing application “Photocial” for Android
  - Upload your picture to multiple social networks
  - User can control the privacy level per social network when uploading images



Photocial

Share image

Profile:

Custom

MySpace - Holiday Pictures
shared with Friends (123)

Orkut - My Pictures
not shared

Facebook - Mobile Uploads
shared with Friends (13)

Beyond Social Networks

- The Web becomes more and more social – why not attach ACLs to any personal Web resource?
- Issues:
  - ACLs require an accessing entity to be identified; could build on federation of social network identities
  - ACLs work only if trusted systems enforce them (server and/or client side)
  - Digital data without copy protection can be redistributed without ACLs (violation “scanner” for enforcement?)

Next Steps

- Implementation of proposed OpenSocial ACLs in Apache Shindig
- Work towards inclusion of generic ACLs in OpenSocial 1.1Next (Q1 2011)

Thanks for your attention

Presenter:

Thomas Dübendorfer, Google Switzerland GmbH

References:

- Proposal for OpenSocial Privacy API (ACLs): http://tinyurl.com/OSACL

  (includes also references to our proposals for an OpenSocial Album and MediaItem Privacy API and an OpenSocial Activity Privacy API)

- Paper: http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-26.pdf