Using Natural Language Policies for Privacy Control in Social Platforms

Juri L. De Coi¹, Philipp Kärger¹, Daniel Olmedilla², Sergej Zerr¹

¹ L3S Research Center & Leibniz University of Hannover, Germany
² Telefonica Research & Development, Madrid, Spain
Outline

1. Privacy Control in Social Platforms - Some observations
2. Semantic Web Policies
3. Controlled Natural Language
4. Controlled Natural Language Policies in Social Platforms
5. Prototype: Extending LearnWeb2.0 with Natural Language Policies
Privacy Control in Social Platforms

let’s have a look …
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who can download your stuff</td>
<td>Anyone (but no one can download the original files, because you have a free account)</td>
</tr>
<tr>
<td>Who can share your photos or video?</td>
<td>Any Flickr member</td>
</tr>
<tr>
<td>Who can print your photos</td>
<td>Only you</td>
</tr>
<tr>
<td>Who can blog your stuff</td>
<td>Any Flickr member</td>
</tr>
<tr>
<td>Hide your EXIF data</td>
<td>No</td>
</tr>
<tr>
<td>Hide your stuff from public searches</td>
<td>No</td>
</tr>
<tr>
<td>Hide your profile from public searches</td>
<td>Yes</td>
</tr>
<tr>
<td>Who can see what on your profile</td>
<td>Your profile page will be hidden from public searches (unless your email address is known, or the person who's searching for you is a contact)</td>
</tr>
</tbody>
</table>
MySpace

Interests - Visibility

This setting only controls who can view this module on your profile. Go to Privacy to control who can access your information.

Who can view this module

- Everyone
- Friends Only
- Friends in certain categories only
  - school friends
- Just me
- Apply to all modules

Apply Changes

General Privacy:

My Visitors: Turn My Visitors on

Online Now: Show people when I am online

Birthday: Show my birthday to my friends

Profile on Mobile: Choose who can view your profile on mobile (e.g., m.myspace.com, iPhone, Sidekick, Hello, Blackberry and other apps).
- Anyone can view my profile on mobile
- Anyone 18 and over can view my profile on mobile
- Only my friends can view my profile on mobile

Comments: Choose who can view your comments page.
- Anyone can view my comments page
- Anyone 18 and over can view my comments page
- Only my friends can view my comments page

Friends: Choose who can view your friends page. Mutual friends are always public.
- Anyone can view my friends page
- Anyone 18 and over can view my friends page
- Only my friends can view my friends page

Photos: Choose who can view your photos page. Set album level privacy in photos.
- Anyone can view my Photos page
- Anyone 18 and over can view my Photos page
- Only my friends can view my Photos page
- Allow my photos to be shared/mailed

Status and Mood: Choose who can view your Status and Mood page.
- Anyone can view my Status & Mood page
- Anyone 18 and over can view my Status & Mood page
- Only my friends can view my Status & Mood page

Block Users By Age: Allow users under 18 to contact me

Block Users: Block individual users by clicking "Block User" on their profile.
[View list]

Save All Changes
Current privacy settings:

• loads of combo boxes and check boxes
• a fixed set of groups or attributes of a requester
• a fine grained definition for each field in your profile
• a “closed world” for privacy decisions (no external evidences)
• no advanced evidences, such as digital credentials
No way to express privacy policies like

Only family members can see pictures geotagged at my house.

ESWC09 participants can see pictures tagged with ‘eswc09’ for two months from now.

Slides tagged with ‘lecture’ can only be accessed by users providing their digitally signed student id.

Every family member is a friend as well.
Semantic Web Policies
Semantic Web Policies

A policy is
“a (declarative) description of the behavior of a system”.

Semantic Web policies:
• have a well define semantics
• incorporate information from difference knowledge sources
• gained a lot of research effort in the last years
• several policy frameworks and policy languages are available
Semantic Web Policies: Features

- Privacy statements can be changed/updated
  - without re-coding, re-compiling, re-installing, etc.
  - in a costless manner
- Reasoning on privacy statements
- Generation of explanations
- Reusability
- Extensibility
- Context-sensitivity
- Verifiability
Protune – a policy framework

_a policy framework_ developed at L3S Research Center and Naples University provides a _logic-based, declarative_ policy language features include

- **trust negotiation**
- **external actions**
  - access to relational databases,
  - RDF stores,
  - file system requests,
  - time and location-aware packages

- **policy explanations**
  - “You cannot access because …” (in contrast to just “Access denied.”)

Getting back to the problem:

Using policies for Social Platforms …
How does a policy look like?

\[ \text{allow(access(}\text{Requester, Resource})) \leftarrow \text{friend(}\text{Requester}), \text{family}\_\text{picture(}\text{Resource}). \]

- machine-understandable
- declarative
- formal syntax
- logic-program-like semantics
- unintuitive and hard to grasp for users
A natural language representation of policies

\[\text{allow(access(Requester, Resource))} \leftarrow \text{friend(Requester), family\_picture(Resource)}.\]

If the requester is a friend and the resource is a family-picture then the requester can access the resource.
Controlled Natural Languages
Controlled Natural Language (CNL)

- is a subset of natural language (NL)
- CNLs have a formal, machine-understandable semantics that is unambiguous:

  "Bob sees the girl with the telescope."

  "Bob and John are friends. He is my friend, too."

are always given the same semantics.
ProACE – a controlled natural policy language

• a subset of the controlled natural language ACE
• each ProACE can be translated into a Protune policy
• still a subset of natural language (not every sentence is possible)

“If the requester is older than 18 and she is Bob’s friend then she can access everything which is in ‘adult-content-folder’.”

“If the company of a credit-card is “VISA” then the credit-card is accepted.”
Again, getting back to the problem:

Using Natural Language Policies for Privacy Control in Social Platforms

- allows the user the create arbitrary conditions for access of resources or profile
  → not restricted to predefined groups or attributes
- may access external information about the requestors outside the social platform
  → e.g., if he is enrolled at your university
- natural language policies are more intuitive to the user
  → more than formal syntax
Prototype: CNL Policies for LearnWeb2.0
Implementation: Privacy policies in LearnWeb2.0

LearnWeb2.0
• a platform for sharing, tagging, commenting resources
• intended for collaborative learning
• meta-platform that wraps several Web2.0 platforms
<table>
<thead>
<tr>
<th>Title of the policy</th>
<th>Policy text</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family photos and videos rule</td>
<td>Everyone who is a relative can see everything which is a photo. Everyone who is a relative can see everything which is a video.</td>
<td>Edit Delete</td>
</tr>
<tr>
<td>Work documents</td>
<td>If a file is related to &quot;job&quot; then everyone who is a colleague can access the file.</td>
<td>Edit Delete</td>
</tr>
<tr>
<td>Student rule</td>
<td>If a document is protected then if the requester sends a student-id and the student-id’s issuer is &quot;uni hannover&quot; then the requester can access the document.</td>
<td>Edit Delete</td>
</tr>
<tr>
<td>Employee rule</td>
<td>Every requester can access everything which is an employee-credential.</td>
<td>Edit Delete</td>
</tr>
</tbody>
</table>
Every requester

can access every

Alice
Bob
John
Mary

certifies
sees
accesses
certifies
contains
retrieves
sees
sends

certifies
retrieves
sends

X
Y
Z
is
an
can
of
some

OK  Cancel
Summary

• Privacy settings on social platforms are too strict

• (Semantic Web) Policies are more expressive

• Controlled Natural Language is a way to make them available to common users

• CNL policies are more handy than loads of combo boxes
Thanks for your attention.

Philipp Kärger
L3S Research Center
kaerger@L3S.de
www.L3S.de/~kaerger