Out of the Wild: On Generating Default Policies in Social Ecosystems

Imrul Kayes, Adriana Iamnitchi
Bank worker fired for Facebook post comparing her £7-an-hour wage to Lloyds boss's £4,000-an-hour salary

Francesca's CFO fired over use of social media

More than once, the chief financial officer of Houston-based Francesca's Holdings Corp. wondered in a tongue-in-cheek Twitter post whether his days at the company might be numbered.

Turns out, they were. On Monday, the women's boutique chain announced it was terminating CFO Gene Morphis - not, the company claims, because of his handling of company finances, but over his use of social media.

The statement from Francesca's did not reveal what specific comment or comments online caused the company to fire Morphis, but it did refer to "improperly communicated company information through social media."

An investigation was launched after Francesca's officials discovered the activity on May 11, according to the statement. The company declined to comment further, and efforts to reach Morphis were not successful.

Morphis links to his Twitter account, personal website and blog from a LinkedIn profile. He also has a Facebook account.
Why Does This Happen?

• (Permissive) Default privacy settings by OSN provider
  • Because they can
  • Lack of universal framework that establishes what is right and wrong
• Users do not change default settings
  • 99% Twitter users
  • >80% Facebook users
  • When they do, they get it wrong
Evolution Towards Social Ecosystems

Privacy in Social Ecosystems

• Social Ecosystems amplify privacy concerns
  – Aggregated data from different contexts of activity
  – A more complete (uncomfortable?) digital recording of a person’s life
  – Social applications from different contexts of activity

• Default privacy settings become critical
Privacy as Contextual Integrity

• The right to appropriate flow of personal information
• Based on two life facts:
  – transfer of personal information happens in a social context
  – people alter behavior to correspond with the norms of the context
• Two norms:
  – Norms of appropriateness
  – Norms of distribution

Our Solution

• Ontology-based social ecosystem data model to capture user online data semantics
  – Model social spheres
  – Model user roles
• Generate default privacy from social data based on Nisseembaum’s contextual integrity framework
• Extensible, fine-grained default policy customizable by users
Social Ecosystems Data Model

Ontology-based data model
- set of entities, instances, functions, relations and axioms
- a vocabulary for social ecosystems
- provides formal and structured representation of user’s data and social spheres
- gives semantic interoperability
- high-level logic inference is possible
System Model

1. There is an unrestricted set of disjoint social contexts;
2. A user belongs to only one social context at any time;
3. A user can have one or more roles in every social context;
4. Each piece of data (resource) is initially assigned (created) to only one context; sharing a resource with other users means replication in each of the other users’ current contexts;
5. A request for a resource is made on behalf of the requester’s role in the context in which the requester is when request is made;
6. A request specifies an action, which could be read, write, delete or replicate to another user’s ownership.
Architecture

Socially-aware Applications

Policy Enforcer
Policy Extractor
Contextual Policy Definer
Policy Repository
User Defined
Default

SEKB
Ontology
Social Data Extractor
Social Data Management Layer

Privacy Management Layer

Policy Editor

Architectural Components:
- Social Data Acquisition & Aggregation Layer
- SEKB
- Ontology
- User Defined
- Default
- Policy Repository
- User Defined
- Contextual Policy Definer
- Policy Extractor
- Policy Editor
- Policy Enforcer

Diagram Elements:
- A1
- A2
- A3
- S1
- S2
- S3
- S4
- Bluetooth
- YouTube
- Reddit
- Facebook
- Netflix
- SEKB
- Ontology
- Privacy Management Layer
- Socially-aware Applications
Policy Specification

• A policy is defined as a set of RDF statements
• Policies obey the two information norms of CI

Norms of appropriateness: Bob’s colleagues can read his professional groups in the Professional context

<Policy>
ASK
where {
p:read p:performedOn Bob.
?req se:isColleagueOf Bob.
Bob se:professionalMember ?group.}
Norms of distribution: policy restricts the access to Bob’s photos if they are shared

```xml
<Policy>
ASK
where {
p:read p:performedOn Bob.
?req se:isFriendOf Bob.
Bob se:hasPhoto ?photo.
?photo se:status se:notShared}
```
Prototype Implementation

• Implemented the prototype in Java Platform Standard Edition 6 (Java SE 6)
• Knowledge base: Jena’s APIs for RDF data management
• Ontology: Jena’s API API for handling OWL ontologies
• SPARQL: Jena’s query engine
Prototype Implementation

- 3 datasets: Slashdot, BlogCatalog, Facebook
- Performance results show solution is practical
Summary

• Proposed an ontology-based social ecosystem data model to capture user social data
• Employ semantic web technologies to generate default privacy policies based on Nissembaum’s contextual integrity theory
• Provide an architecture and prototype implementation of privacy model
Thank you!

Out of the Wild: On Generating Default Policies in Social Ecosystems

Imrul Kayes, Adriana Iamnitchi
http://www.cse.usf.edu/dsg/