Shared Content Risk in Social Networks and Access Control

Panagiotis Ilia

Institute of Computer Science
Foundation for Research and Technology – Hellas (FORTH)

<pilia@ics.forth.gr>

iSocial

FORTH
Institute of Computer Science

MARIE CURIE ACTIONS
PEOPLE

Online Social Networks

- **Facebook**: More than **1.2b** users currently

   More than **350m** photos uploaded daily.

Success of OSNs due to their **human-centric design:**

- **Users create their digital counterparts**

- **Connect and communicate with others**

- **Create and share their own original content**

Concerns regarding user privacy

o   Most users don't care about their privacy

o   Access control mechanisms are complicated

o   Users are unaware of the **"true visibility"** of **published content.**

However, according to OSN design:

➢   The **uploader** is considered as **the owner**.

➢   Users can **control** only **self-disclosed information**.

❑   Users **cannot** control **shared content** published by others

Conflict of interests

➢ The will of the uploader goes against the will of the depicted users.

➢ The privacy settings of a user are overridden by those of another user.

Scenario: The Sober Tagger

• Alice uploads photo - Bob request removal - Alice does not remove it.

Scenario: The Silent Tagger

• Alice does not tag Bob, thus Bob is never notified about the photo.

Scenario: The Group Photographer

- Bob set the photo as **"private"** – Alice set it as **"public"**
- **18%** allow friends-of-friends, **26%** public [Liu, IMC 11]

Scenario: The Accidental Over-sharer

- Users accidentally over-share content due to complex privacy settings.
- Sharing photos with much larger audience than they intended.
- **63%** of photos - wrong settings, **51%** of them public [Liu, IMC 11]

Scenario: The Friendly Stranger

- Both Alice and Bob set their privacy settings as **"friends".**
- If their social graphs do not overlap, "strangers" can access the photo.

Contributions of this work

➢ Conduct a user study about the tagging behaviour of the users.

- Identify the risk users face due to conflicting privacy settings.

➢ Design a new fine-grained access control mechanism.

- Enforce **face-level** access control (according to user's access-list).
- Handles effectively the **conflicting visibility settings** of the users.
- Can **inter-operate** with the existing access control mechanisms.

➢ Proof-of-concept application.

- Demonstrate applicability of the approach within OSN infrastructure.

User study on photo-tagging behaviour

➢   FB application for collecting user data and photos.

- **Photos and tags** both from the user and his friends.

- Friend-list of the users

➢   Collected data from 128 users

- About **4m** photos containing **4.6m** tags

➢   Average number of friends **344**

- **7% - less than 100 friends**

- **3% - more than 1000 friends (hubs)**

User study on photo-tagging behaviour

➢   Each user and his friends as a group

- Average number of photos per group **31753**

- **20%** of groups have more than **44700** photos

- **4%** of groups have more than **100000** photos

  (1 every 3 photos is accidentally public)

➢   Tags within a photo collection (group)

- Average: each group has **36102 tags** and **250 tagged users**

- **20%** of groups have over **340** unique tagged users and over **50k photos**

iSocial

Silent uploader scenario

Tags - Faces	1	2	3	4	5	6+
Photos (# of Faces)	15.2% (304)	32.5% (651)	17.9% (359)	10.7% (214)	8.3% (166)	15.3% (306)
Photos (# of Tags)	87.6% (1753)	9.9% (199)	1.6% (33)	0.3% (7)	0.25% (5)	0.15% (3)

Total of **7,244** faces → **3.62 faces per photo**

2,331 faces have been tagged → **1.16 tags per photo**

At least 4 depicted faces in 34% of the photos

FORTH
Institute of Computer Science

User study on photo-tagging behaviour

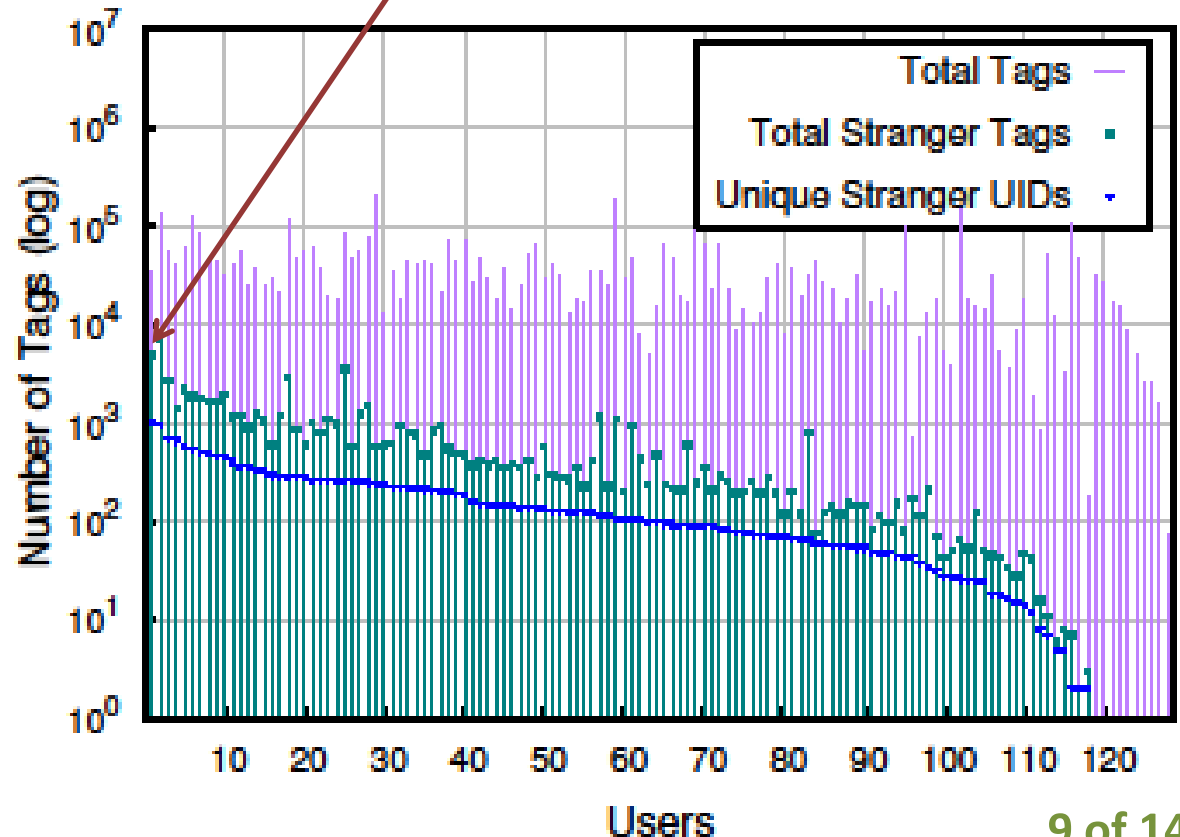*Friendly stranger scenario*

Users as "Adversaries"

Access to photos containing stranger's information

92% of users have access to photos that contain tag of a stranger (non-friend).
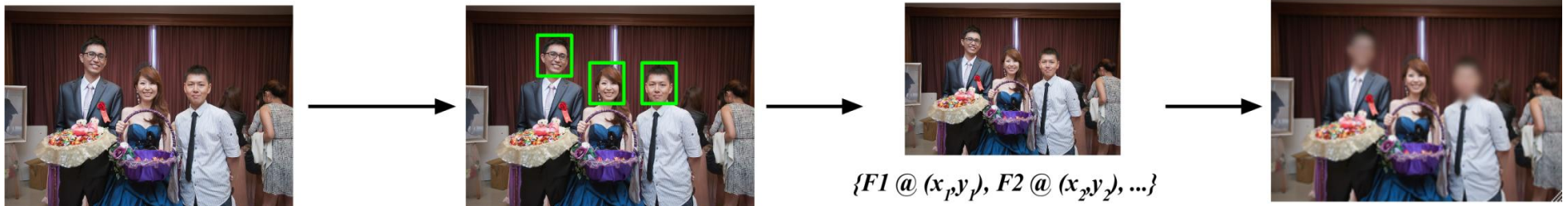
Average: access to **647** photos of **169** different users (strangers)

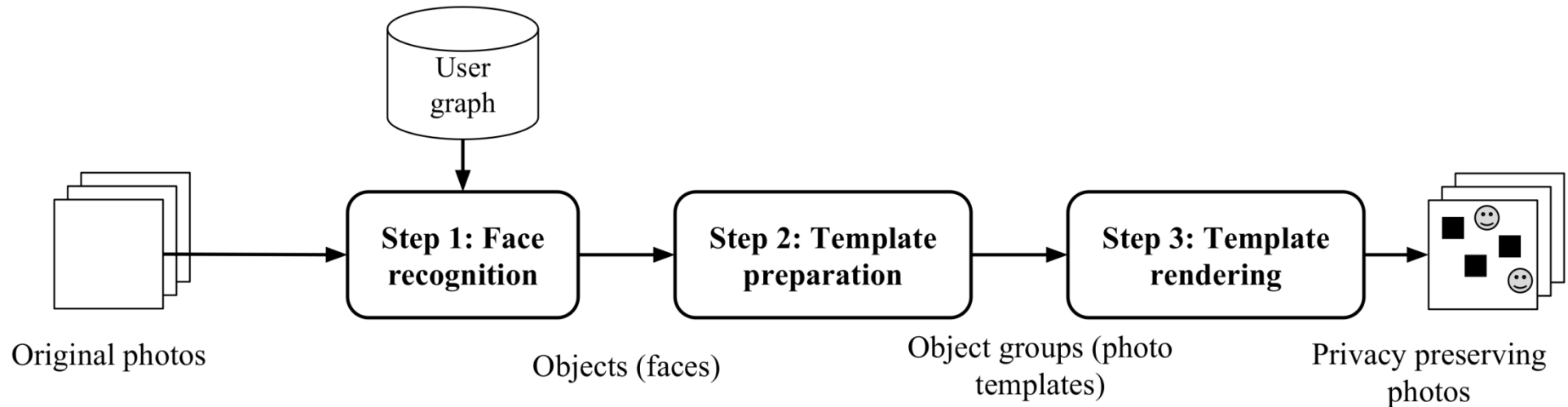Almost **1900** photos containing **1100** strangers

Proposed Access Control Mechanism

- Each user's face is considered as PII.

- **Switches the granularity** of the access control ...

  ... from the level of a **photo** to that of users' **faces**.

- User's privacy settings are not overridden by others.

$$\{F1 @ (x_1, y_1), F2 @ (x_2, y_2), ...\}$$

Proposed Access Control Mechanism

Step 1: Face Recognition

Step 2: Template Preparation

- Auto-tagging the identified faces - face verification.
- The users are automatically notified to verify the face validity.

Overview of the access control approach

Step 2: Template Preparation (cont)

- Each tagged user defines face-level privacy settings.

- For each tagged face a layer is created (face is hidden/blurred out).

- Photo template consisted from original photo and the created layers.

Step 3: Template Rendering

- Determine in constant time the hidden faces (access control matrix)

- The photo is rendered selectively according to who is viewing it.

- The requested photo is created "**on the fly**".

- Superimposing the required layers, on top of the original photo.

However,

This approach can be used **only on shared photos**

It affects the user experience as the presented photos are modified.

Thus,

- We study new approaches for collaborative access control

- The rules are defined and enforced collectively.

- A more generic model, not only for photos.

FORTH
Institute of Computer Science

Summary

- **Tagged users affect the visibility** of the photos

Conflict of interests

➢ The will of the uploader goes against the will of the depicted users.

➢ The privacy settings of a user are overridden by those of another user.

We propose a new fine-grained access control mechanism.

- Enforce **face-level** access control (according to user's access-list).
- Handles effectively the **conflicting visibility settings** of the users.
- Can **inter-operate** with the existing access control mechanisms of SNs.

Previous work

o   Survey on user behaviour, ownership and privacy issues.   **[Besmer, SOUPS 08]**

o   A "negotiation" mechanism.   Out-of-band request to the uploader to hide the photo.

o   Does not effectively solve conflict of interests.   **[Besmer, SIGCHI 10]**

Rule-based access control

o   Users annotate photos with custom descriptive tags. AC rules according to these tags.

o   Access control on photo-level .   **[Klemperer, SIGCHI 12]**

Rule-based mechanism / similar to recommendation systems

o   AC policy according to rules.   Classifies new photos and predicts an acceptable rule.

         [Squicciarini, HT' 11]

Security rules for content-based access control

o   Uses the SWRL language. The owner sets complex Positive and Negative rules.

o   Mechanism for resolving conflicting rules. Depends on the owner to set attributes /rules

         [Al Bouna, SITIS 12]

FORTH
Institute of Computer Science

User study on photo-tagging behaviour

Silent uploader scenario

- Randomly select 2000 photos

- The set is good representative