Computing and Informatics, Vol. 28, 2000, 747–762

EXTENSION OF IMAGENOTION TO ALLOW PRIVACY-AWARE IMAGE SHARING

Andreas Walter

FZI Research Center for Information Technologies
Information Process Engineering
Haid-und-Neu-Straße 10-14
76131 Karlsruhe
Germany
e-mail: awalter@fzi.de

Gabor Nagypal

disy Informationssysteme GmbH
Erbprinzenstr. 4-12, Eingang B
76133 Karlsruhe, Germany
Germany
e-mail: nagypal@disy.net

Revised manuscript received 19 January 2009

Abstract. A growing number of users in Web 2.0 based social network sites and photo sharing portals upload millions of images per day. In many cases, this leads to serious privacy threats. The images reveal not only the personal relationships and attitudes of the user who uploads the images, but those of other persons displayed in the images as well. In this paper, we propose a system architecture for privacy-aware image sharing. Our approach is based on the ImageNotion application, which combines automated processes to create high-quality semantic image annotations.

Keywords: Social network sites, collaboration, semantic image annotation, privacy, ImageNotion, face detection, face recognition, person detection

1 INTRODUCTION

Users have already uploaded a lot of images to many different image platforms, e.g., to Flickr or Facebook. For example, in Facebook, 60 million users upload more than 14 million images per day [1]. People upload photos from holidays with their family, parties with friends or company events with their colleagues.

From the perspective of privacy, this is alarming: Publicly visible images often show people in compromising situations without the consent or even the knowledge of the individuals on the pictures. Recent Web 2.0 platforms, e.g., social networking sites (SNS) like Facebook or photo sharing platforms (PSP) like Flickr, make this problem even more serious. Such platforms allow the users to link photos to individuals, and to provide tags describing the persons on a photo and the situation it was taken. In order to enable people to manage their representations on the Internet as envisioned by data protection regulations [2], it is important to let concerned individuals become aware of images showing them.

Because many people are not aware about privacy problems while they upload new images, we propose to use automated processes for the detection and recognition of persons on images. This may help other users, who do not want to be displayed on image contents, or who want to know who provides images showing them.

Using semantic image annotations, it is possible for machines and algorithms to automatically execute queries for images and to "understand" the image contents [3]. For example, agents can search for images showing a specific person together with female persons, and they will know who the displayed persons on the images are. This is based on the available background information in semantic elements, such as the gender or profession of a person.

Since state-of-the-art systems use textual image annotations, a system is required that is capable of creating semantic image annotations, of transforming textual annotations to semantic annotations, and of creating semantic annotations on image parts. The ImageNotion application [4] provides a visual methodology that supports collaborative, work-integrated ontology development. ImageNotion allows for semantic search and for the navigation through image archives based on the available image annotations. As the creation of semantic annotations is very time consuming, ImageNotion automates the generation of semantic annotations to the maximum possible extent by combining a number of different automated processes.

In this paper, we first analyze the requirements for privacy-aware image sharing from many different image sharing platforms. Then, we give an overview on the ImageNotion application. Based on ImageNotion, we introduce the PRIMO (PRivacy for IMage Objects) system architecture. PRIMO benefits from features of ImageNotion, such as person and face detection and face recognition to identify the individuals on the published images. PRIMO allows the users to train the system with images showing their face. Also, it is possible to specify privacy rules, which are evaluated for each individual identified on a picture. Example rules include "inform me when someone publishes a photo of me with my girlfriend" or "block the publication of images showing me". Based on these training data and rules, PRIMO

loads publicly available images from different sources and scans them. Each time an image contains an already known face, the user is alerted based on his/her predefined rules. This allows the user to react on this image if it harms his/her privacy, e.g. by asking the provider of the image to remove it.

The paper is structured as follows: in Section 2, we discuss related work. Section 3 discusses privacy aspects of image sharing on Web 2.0 platforms and the requirements for privacy aware image sharing on the Web. Section 4 gives an overview about the features of ImageNotion. These features include collaborative and work integrated ontology development and the combination of the results of automated processes to improve the quality of generated metadata. We introduce the PRIMO architecture in Section 5. Section 6 concludes the paper.

2 RELATED WORK

In this section, we report on related work that is relevant to our goal to extend ImageNotion to a mashup service for privacy-aware image sharing.

Data integration from image platforms: For our mashup, the integration of image metadata from image platforms is necessary. Image platforms include portals (such as the German fotomarktplatz[1] portal for professional photographers and image agencies), images displayed on web pages (e.g., crawled by Google), photo sharing platforms (e.g., MySpace, Flickr and Riya) and social network sites (e.g. Facebook, studiVZ or LinkedIn). We give an overview on possible data integration techniques for these image platforms.

One possibility is to use the OpenSocial API [11]. It defines a set of commonly used, standardized methods for social network sites. Thus, it allows for interchanging and linking among other profile data, friend lists and even images from various sources supporting this standard. E.g., images from MySpace [19] can be accessed this way. Currently, most sites, such as Flickr, Facebook and Riya, do not support OpenSocial but they provide proprietary APIs and proprietary data exchange formats. For such services, a wrapper is needed. The APIs allow either to retrieve all publicly available images or images of a given user where the the user agreed exchanging data with the service using the API. Via the APIs, it is possible to read the existing image annotations and also to retrieve the images themselves. Image platforms supporting the annotation of image parts, such as Riya or Facebook, also support the retrieval of image part annotations [18].

Integrating automated processes: Creating image annotations, and especially annotations for image parts, is very time consuming. This process should be automatized as much as possible. We give an overview how automated processes are used in other image platforms. Tag4you[2] uses the Flickr API to allow

[1] `www.fotomarktplatz.de`

[2] `www.tag4you.com`

face detection in Flickr images. The system automatically marks the areas of detected faces and also allows adding tags to those areas manually. The tags are then automatically written back to Flickr. Riya offers face detection and recognition algorithms. Text recognition based on OCR in images is also provided. The face detection and recognition algorithm of Fraunhofer IIS [5] (we use it in ImageNotion) also supports gender classification and can detect moods like happy, angry, sad or surprised.

Semantic image annotation: RDFPic [7] and PhotoStuff [6] allow for the generation of semantic image annotations using imported domain ontologies. Both applications are only available as desktop applications and offer do not offer support for collaborative ontology development and semantic annotation.

Privacy mechanisms for images in SNS: Existing privacy-enhancing technologies (PETs) can be categorized into two classes [8]. The first class focuses on the *awareness* and *control* of Internet users. One example is the browser plugin MozPET [9] that helps users protocol personal data they disclose while surfing the Web. The second class addresses the *transparency* of privacy practices of providers, e.g., P3P [10]. Focusing on the classical provider-consumer paradigm, neither classes support for Web 2.0 applications where users provide the content and do not consider private information revealed by other persons.

3 PRIVACY-AWARE IMAGE SHARING

According to [12], "privacy is the claim of individuals to determine for themselves when, how and to what extend information about them is communicated to others". In the context of images, each person should be able to control the publication and distribution of all images where s/he is identifiable.

This is challenging. Problems occur by information individuals publish about themselves as well by information they disclose about others. People tend to forget about "who knows what" [8], e.g., they publish personal images to various providers, portals and services in the first place, but do not delete them later on. Further, people forget that intimate communication at such platforms is publicly visible [13]. A typical example is a user who uploads party pictures to a photo portal, makes the virtual album publicly visible, shows the link to some friends, and forgets the album after some time. Forgotten images can contradict the self-representation of the uploader, e.g., when a photo reveals former attitudes and habits. As the photos might show other party guests as well, this affects not only the self-representation of the uploader, but also the privacy of others.

In Web 2.0 applications like Facebook, photos can be assigned with tags describing background information or the people shown. Photos can be linked with personal profiles or other descriptive resources, and the cross-references among the users reveal their social relationships. Person search engines like `123people.com` use this information to generate comprehensive personality profiles. Thus, in the

context of Web 2.0, privacy-aware image sharing becomes an even more serious issue as compared to classical photo sharing portals. Uncontrolled disclosure of private information has already cost the jobs of several people [14].

Due to the huge number of images uploaded every day, users require an automated system for managing their privacy while sharing images on the Web. In the following, we compile the requirements for such a system.

Definition of privacy rules. A user should be able to define privacy rules for images. The simplest rule a user can specify is to get informed if another person uploads images showing his/her face. More complex rules take the context into account, i.e., the uploading user as well as the users having access to the uploaded images. As an example, a rule could notify a user if a friend uploads a compromising image.

Semantic annotations. Semantic annotation of images supports the definition of more complex privacy rules. Based on semantic annotations it is possible to take semantic information into account, e.g., the gender. For example, this allows for a rule of a female user "send a notification if there are images showing me together with a male person" to avoid misunderstandings like having cheated the partner or a rule "send a notification if there are images showing me angry".

Automated face and person detection and face recognition. Because of the huge number of images uploaded every day, automated processes are required to identify the individuals concerned. Therefore, person and face detection and face recognition techniques are mandatory. Person detection algrithms can detect areas where complete persons are displayed. Face detection identifies the areas of a photo which show faces and may also derive semantic information like the gender of the displayed person. Face recognition identifies the person displayed in such an area. Face recognition requires training. For example, the Fraunhofer IIS face recognizer [5] needs at least five images of a person to allow a reliable recognition of him or her.

Automated conflict detection. Based on the defined privacy rules, the system must detect images which are not conform to these rules. Therefore, the system has to analyze new images on Web 2.0 applications, detect faces, check privacy rules and inform the users, e.g., via email, for all images which cause conflicts.

Interoperability. Due to the large number of Web 2.0 applications that share photos, interoperability is required to detect images which probably cause privacy problems. For example, two photos at Flickr and Facebook uploaded from different users might show the same person in the same compromising situation. Thus, a system for privacy-aware image sharing has to include APIs to as many popular SNS and PSP as possible.

4 THE IMAGENOTION APPLICATION

ImageNotion automates the generation of semantic annotations to the maximum possible extent by combining a number of different automated processes. In this section, we give a brief overview on the ImageNotion application. For further details refer to [4, 15]. A demo of the ImageNotion application is publicly available at `http://www.imagenotion.com`.

We will use ImageNotion as the core system to build an architecture for a privacy-aware image sharing system. ImageNotion will thereby fulfil the requirements "Semantic annotations" and "Automated face and person detection and face recognition".

4.1 Collaborative and Work-Integrated Ontology Development

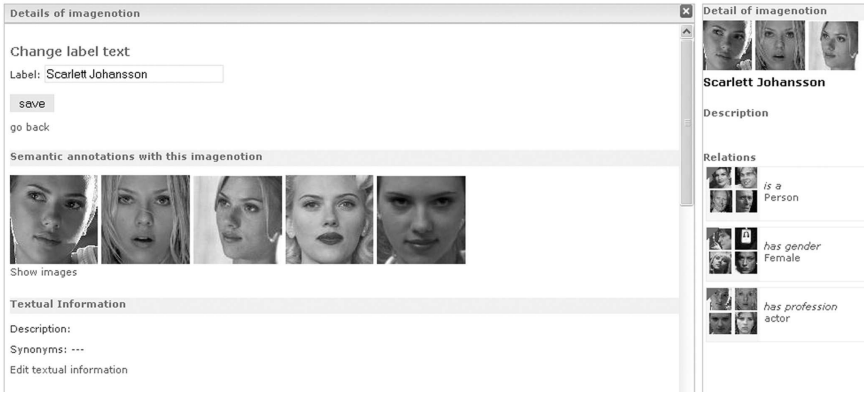

Fig. 1. Editing the imagenotion for Scarlett Johansson

We call our ontology elements (concepts and instances) *imagenotions*, formed from the words image and notion. An imagenotion visually represents an ontology element through corresponding images. Imagenotions may represent concrete things, e.g. the specific person "Scarlett Johansson", or abstract things, e.g. the profession "actor" (see Figure 1). The visual representation of ontology elements helps image annotators get a better understanding of their meaning.

Based on the ontology maturing process model [17], a collaborative and work integrated ontology development methodology is implemented in ImageNotion. New imagenotions may be added by users in the first phase. In the next step, imagenotions are consolidated in communities of users. In this phase, a stable definition of the concept emerges as users communicate with each other, or work on the same concept definition. In the third phase, it is possible to add named relations between imagenotions. Figure 1 shows the imagenotion for the actor "Scarlett Johansson" and the already added relations to describe this actor "is-a" "person", "has-gender"

"female" and "has-profession" "actor". Imagenotions from each maturing grade may be used for semantic image annotations immediately after creation.

The ImageNotion methodology allows to start the development of a new ontology either from scratch or by reusing existing ontologies or parts of these. A community may then collaboratively add further ontology elements. Automated processes may also add new imagenotions they require to describe the images with semantic annotations.

4.2 Combining Automated Processes in ImageNotion

For the generation of semantic annotations, ImageNotion combines the results of automated processes. The integrated face detection algorithms (from Fraunhofer IIS, [5]) can detect the parts on images showing faces and in addition the gender and the emotion of the displayed person.

The face recognition engine (from Fraunhofer IIS, [5]) recognizes already known faces in the archive. To provide acceptable results, the face recognition algorithm needs training images for each person that should be recognized by the algorithm. In addition, object and person detection algorithms can detect objects such as cars and airplanes and person detection (from NTUA, [16]) detects the areas displaying persons on images. Finally, text mining algorithms, such as text recognition algorithms, detect semantic elements in available textual annotations and converts them to semantic annotations for the complete image. The generated semantic annotations use the existing imagenotions in the ontology.

To create a privacy-aware image sharing platform, the recognition of persons and faces is needed. We therefore now give an overview how the combination of algorithms works to achieve this goal.

4.2.1 Combination of Face Detection and Face Recognition

Fig. 2. Combination of face detection and face recognition in ImageNotion

In ImageNotion, the training of new faces for the face recognition functionality is based on the combination of face detection and face recognition as follows.

1. A user uploads images. One or more faces on these images are unknown for the system or although the faces are known, they cannot be recognized correctly for some reasons. The face detection algorithm that operates very reliably, determines the bounding boxes also for such faces. The system notices that the face recognition algorithm failed to recognize the person because the recognition score is too low.
2. If a new face is detected, gender and mood detection is additionally executed and relations to the imagenotions of the categories "gender" and "person" and of the category "mood" such as "happy", "sad", "angry" or "surprised" are added automatically.
3. If the person was not recognized by the face recognition, a new imagenotion for this face is created and named with "unknown person x" (where x increases). The gender information is automatically added to this new imagenotion. The image part showing the face is added as the first training image of this new face.
4. The web user interface asks the user, who is the person. The user may associate the bounding box with an existing imagenotion of a person or may set the correct name of the person in the "unknown person x" imagenotion.

In Figure 2, the system has recognized a person a so far unknown to the system, and created a new imagenotion with the label "Unknown person 70" and assigned the relations "has-gender" "male" and "is-a" "person" automatically. In total, four images in the archive were identified which contains this person. In the web interface, the user may now correct the name of this person from "Unknown person 70" to "Harrison Ford".

4.2.2 Combination of Text and Face Recognition

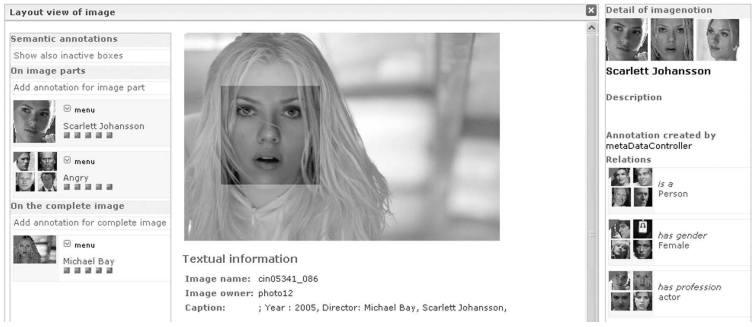

Fig. 3. Combination of text and face recognition in ImageNotion

If an image already contains textual description text, this text is analyzed by text recognition algorithms in ImageNotion. One component of the text recognition allows to detect names in the text and in addition to specify the gender associated

with the first name. In the image caption "Year : 2005, Director: Michael Bay, Scarlett Johansson" of the image shown in Figure 3, the text recognition algorithm has detected two names: "Michael Bay" and "Scarlett Johansson". Moreover, for "Scarlett Johansson" the gender "female" and for "Michael Bay" the gender "male" was detected correctly, too. Finally, this algorithm creates two image annotations for the complete image.

After text recognition, the face detection and identification algorithm is executed. In our example in Figure 3, the face detection algorithm has detected one female person on the image and generated the corresponding semantic image annotation for this image part. Even if the face recognition did not recognize the face, the controller of the automated processes can merge this annotation with the annotation on the whole image that also represents a female, i.e., with "Scarlett Johansson". Consequently, it was possible to add a new training image for "Scarlett Johansson". In big image archives, this enables completely automated training of the face recognition algorithm with correct training images.

4.2.3 Combination of Face and Person Detection

With the combination of face detection and person detection, it is possible to get a higher score for the correctness of the generated semantic image annotation. If the person detection detects a complete person on the image and the face detection detects a face in this area, both information are merged together. The annotation for the person is removed and the score for the face detection is set to a high value (0.9, which means there is a face with 90 percent certainty).

4.3 Building a Mashup With ImageNotion

ImageNotion can either annotate images which are stored in a local file system or images which are stored on the Web, e.g., on image sharing platforms. In this case, ImageNotion operates as a service and provides a web service interface for adding images or searching images via semantic search requests. This interface is used in the next section to build a privacy-aware image sharing platform.

5 THE PRIMO MASHUP

In this section we introduce the components of the PRIMO architecture (Figure 4) and show how they fulfill our requirements. Also, we present a prototypical implementation. The PRIMO application is built as an extension of ImageNotion. It uses the service interface to communicate with ImageNotion in order to get semantic image annotations for images send to the service.

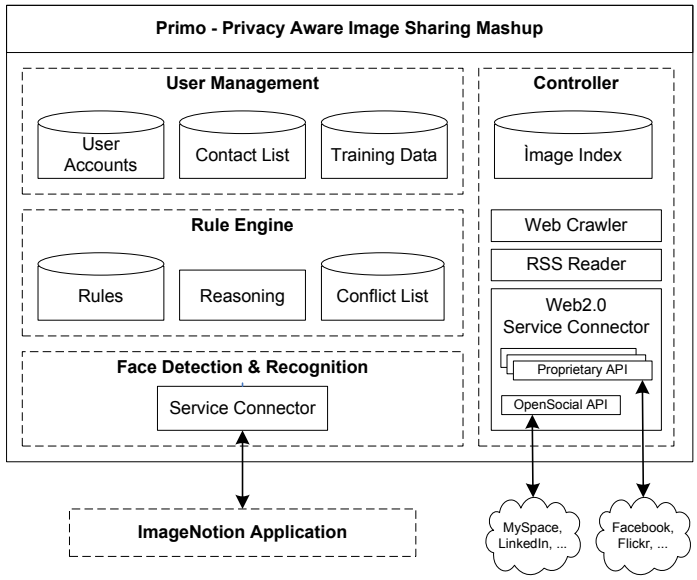

Fig. 4. PRIMO System Architecture

5.1 System Architecture of PRIMO

User Management. This component stores the *user account*, the *contact list* and *training data* for each user. The user account contains user name, password and email-address for notifications. The contact list holds all information about personal contacts of a user, whether or not they are friends. Interfaces to Web 2.0 applications normally allow to query and to import these data. Since the face recognition in ImageNotion requires training data, the user has to upload images of his/her face.

Controller. The controller fulfills the requirement for "interoperability". Therefore, a *Web 2.0 service connector* loads images from SNS and PSP. PRIMO supports the OpenSocial standard to connect to SNS and PSP like MySpace or LinkedIn. In addition, proprietary APIs can be included, e.g., from Flickr or Facebook. The Controller lets users decide if images should be made public, kept private or shared with friends. Furthermore, the controller allows users to make their training information for the face recognition service public in order to increase the detection rate of the face recognition algorithm. The controller stores the source, id and signature of the image in the *image index*.

Detection and recognition. The detection and recognition component supports the requirements "automated face detection and recognition" and "semantic annotation". This component uses a *service connector* to interoperate with the ImageNotion application. In the first step, this component *detects* faces and

persons on images and automatically creates semantic annotation boxes for each identified face and person.

In the second step, the face recognition algorithm *recognizes* the persons in the image using the training data of the User Management component.

After these steps, ImageNotion creates semantic annotations by linking the annotation boxes with semantic elements. More precisely, it assigns the faces in the picture with corresponding imagenotions in the ImageNotion system, such as "male" or "Andreas Walter".

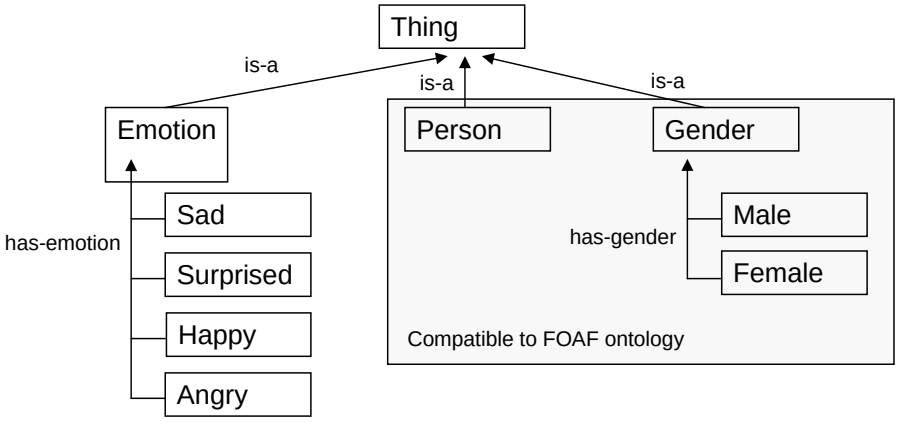

Fig. 5. Core ontology required by PRIMO

Ontology setup. Figure 5 shows the parts of the core ontology which are used for semantic image annotation in PRIMO. The emotions "Sad", "Surprised", "Happy" and "Angry" are used to describe the emotions of the displayed persons. In ImageNotion, the emotion detection algorithm will automatically detect the emotions of faces displayed on images and will use these ontology elements to create semantic annotations. The two gender elements "male" and "female" are used by gender detection in ImageNotion to set the gender of the recognized faces on images. The person detection algorithm uses the semantic element "person" to annotate the parts on images showing complete faces. If new faces are added for face recognition, a new semantic element is created for each person. The relations to the semantic elements "gender" and "person" are then assigned automatically. Using these semantic annotations, it is possible to define privacy rules.

Rule engine. The rule engine fulfills the requirements "definition of privacy rules" and "automated conflict detection". It allows the users to define privacy rules for all images showing their faces. The rules are stored in the rules database. Rules consist of a *Context* and a *Reaction* on this context, i.e,
`Rule := if Context then Reaction`.

The Context defines

i) who is uploading an image
ii) who is displayed on that image, and
iii) who may access the image.

If the person displayed is not known to PRIMO, the system can still rely on semantic information that can be derived from the image. i) and iii) can be obtained from metadata of SNS or PSP. The *reasoner* uses this information together with the contact list from the user management component to evaluate rules like "If a friend from my contact list is uploading a publicly visible image that displays me with a girl then notify me". For every image or new rule, the rule engine has to reason if one of the rules fires. Fired rules are recorded on the *conflict list*.

A *notification* is the simplest reaction which a user can specify for the case that his face is detected on an image. In case of integrating PRIMO into a SNS, three further mechanisms are possible: *blocking* of the publication, *opt-in* or *opt-out*. Opt-in means that persons are asked for their consent before the publication of an image. Blocking prohibits the publication without asking the user. Opt-out allows the persons to decline after the publication took place. If an image displays several persons with contradicting rules, the most restrictive rule is applied for the image, i.e., *Block* > *Opt-In* > *Opt-Out* > *Notification*.

5.2 Implementation and Example Scenario

For a prototype of our PRIMO system, we implemented interfaces to MySpace, Facebook and Flickr in the Web 2.0 service connector. MySpace uses the OpenSocial standard, while Facebook and Flickr offer proprietary interfaces.

Fig. 6. User management component

Currently, our rule engine supports three rules of different complexity. The rule "notify me if a friend uploads an image showing persons" requires face detection and the contact list, and does not depend on identifiable faces on the picture. The rule "notify me for images showing me with other users not having my gender" requires face recognition based on the training set in the user management component, and depends on face detection and semantic image annotations to identify the gender of further persons on an image. The third rule, "notify me for all images showing me with persons that are not my friends", depends on face detection and recognition for all individuals on the image, and uses the contact list to identify friends. For semantic search requests of images showing these contacts, we access the ImageNotion application.

Fig. 7. Reasoning result of rule engine

To demonstrate how our PRIMO prototype works, we now briefly describe an example scenario. First, PRIMO scans images from SNS and PSP and creates the image index containing the signatures of all faces detected. Now Andreas, a new user, creates an account in PRIMO. In order to provide the system with the training data required, Andreas uploads several images of his face (see Figure 6). After that, he imports his friend lists from Facebook and Flickr. Finally, Andreas specifies a privacy rule so that he receives an email if an image showing him with a stranger is detected. PRIMO then scans the image index for signatures of Andreas' face, and invokes the rule engine with the semantic annotations from the images found. It does the same for each photo that will be uploaded in the future. As Figure 7 shows, PRIMO eventually detects an image on Flickr, which meets the criteria of Andreas' privacy rule.

6 CONCLUSIONS

In this work we have introduced PRIMO, an approach for privacy-aware image sharing that helps users to get back control over images showing them on social network sites or photo portals, even if they are uploaded by strangers. Based on automatically created semantic image annotations by the ImageNotion system, PRIMO detects and recognizes the persons shown on images. It lets users specify rules to filter images that might harm their privacy.

PRIMO is a big step toward privacy aware image sharing. Obviously, it follows a best effort approach, i.e., it offers no guarantees to find all compromising images. Three factors influence the effectiveness of PRIMO:

1. The face detection and recognition mechanism. This is a hot topic in research. Recent proposals combine multiple algorithms to increase the detection rate.
2. The quality of the images used for training.
3. The availability of standardized APIs to PSP and SNS. Here, the OpenSocial API is an important step towards unified SNS.

Currently, PRIMO is an operational prototype. Next, we will fine-tune the prototype to evaluate our approach by extensive user studies.

REFERENCES

[1] Web-Strategist: Knowledge and Belief: `http://www.webstrategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunionjan-2008/`, 2008.

[2] European Parliament: Directive 95/46/EC of the European Parliament and of the Council, Knowledge and Belief: `http://ec.europa.eu/justicehome/fsj/privacy/docs/95-46-ce/dir1995-46part1en.pdf`, 2008.

[3] Bashir, A.—Latifur, K.: A Framework for Image Annotation Using Semantic Web. MSW2004, 10th International ACM SIGKDD Conference on Knowledge Discovery and Data Mining KDD 2004, 2004, Seattle (WA),USA.

[4] Walter, A.—Nagypal, G.: ImageNotion – Methodology, Tool Support and Evaluation. GADA/DOA/CoopIS/ODBASE 2007 Confederated International Conferences DOA, CoopIS and ODBASE, Proceedings, LNCS. Springer 2007.

[5] Kűblbeck, C.—Ernst, A.: Face Detection and Tracking in Video Sequences Using the Modified Census Transformation. Image and Vision Computing, K. D. Baker (Ed.), Issue No. 6, Elsevier, 2006.

[6] Ossenbruggen, J.—Troncy, R.—Stamou, G.—Pan, J.: Image Annotation on the Semantic Web. W3C, `http://www.w3.org/TR/2006/WD-swbp-imageannotation-20060322/`, 2006.

[7] Lavon, Y.–Boss, B.: Describing and Retrieving Photos Using RDF and HTTP. W3C, `http://www.w3.org/TR/photo-rdf/`, 2002.

[8] Burghardt, T.—Buchmann, E.—Bőhm, K.: Why do Privacy-Enhancement Mechanisms Fail After All? W2Trust, 2008.

[9] Brűckner, L.—Voss, M.—Brűckner, L.—Voss, M.: PST, 2005.

[10] Marchiori, M.: The Platform for Privacy Preferences 1.0 Specification. W3C Proposed Recommendation, `http://www.w3.org/P3P`, 2002.

[11] OpenSocial: `http://code.google.com/apis/opensocial/`, 2008.

[12] Turner, E.—Dasgupta, S.: Privacy on the Web: An Examination of User Concerns, Technology and Implications for Business Organizations and Individuals. Information Systems Management, Volume 20, 2003.

[13] Rosenblum, D.: What Anyone Can Know: The Privacy Risks of Social Networking Sites. Journal of Security and Privacy, 2007.

[14] Warren, J: Self-Imposed Violations of Privacy in Virtual Communities. University of Texas, 2008.

[15] Walter, A.—Nagypal, G.—Nagi, K.: Evaluating Semantic Techniques for the Exploration of Image Archives on the Example Of the ImageNotion System. Alexandria Engineering Journal (AEJ), Vol. 47, No. 4, ISSN 1110-0168, Springer 2008.

[16] Kapsalas, P.—Rapantzikos, K.—Sofou,A.—Avrithis,Y.: Regions of Interest for Accurate Object Detection. Proc. of Sixth International Workshop on Content-Based Multimedia Indexing (CBMI 2008), London, UK, 2008.

[17] Braun, S.—Schmidt, A.—Walter, A.—Nagypal, G.—Zacharias, V.: Ontology Maturing: A Collaborative Web 2.0 Approach to Ontology Engineering. Proceedings of the Workshop on Social and Collaborative Construction of Structured Knowledge at the 16th International World WideWeb Conference (WWW '07), Banff, Canada, 2007.

[18] Riya API: `http://www.riya.com/riyaAPI`, 2008.

[19] MySpace: MySpace Specific Extensions on OpenSocial, `http://tinyurl.com/ytpfgl`, 2008.

Andreas Walter works as Ph. D. student at the FZI Research Center for Information Technologies in Karlsruhe, Germany. He has long-time experience with image management applications, grid applications and semantic technologies.

Gabor Nagypal has received his Ph. D. degree at the University of Karlsruhe in 2007 and now works for disy Informationssysteme GmbH where he leads web application development projects. His research interests include using semantic technologies for effective information retrieval. He was the technical and scientific coordinator of the EU-IST project IMAGINATION (`http://www.imagination-project.org`).