# PrivacyTag: A Community-Based Method for Protecting Privacy of Photographed Subjects in Online Social Networks

Shimon Machida, Adrian Dabrowski, Edgar Weippl, Isao Echizen

▶ **To cite this version:**

Shimon Machida, Adrian Dabrowski, Edgar Weippl, Isao Echizen. PrivacyTag: A Community-Based Method for Protecting Privacy of Photographed Subjects in Online Social Networks. 16th Conference on e-Business, e-Services and e-Society (I3E), Nov 2017, Delhi, India. pp.261-275, 10.1007/978-3-319-68557-1_24 . hal-01768504

**HAL Id: hal-01768504**
**https://inria.hal.science/hal-01768504**

Submitted on 17 Apr 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

# PrivacyTag: A Community-based Method for Protecting Privacy of Photographed Subjects in Online Social Networks

Shimon Machida[1], Adrian Dabrowski[2], Edgar Weippl[2], Isao Echizen[3]

[1] SAP Japan,
shimon.machida@sap.com
[2] SBA Research
[adabrowski, eweippl]@sba-research.org
[3] National Institute of Informatics,
iechizen@nii.ac.jp

**Abstract.** Online social networks, such as Facebook, have become popular with people of all ages, and online communication with friends and acquaintances via messages that include photos has become very common. With the increasing ease with which users can take and post photos, the unintentional disclosure of sensitive information of various kinds through mistakes made while posting has become a problem. In this work, we focused on the privacy of people appearing in photos and developed a method called "PrivacyTag" for adaptively blurring their facial area in accordance with the communities to which they belong by using tags embedded with community-based privacy policies. We also evaluated a newly designed privacy tag and developed a prototype application for Facebook that uses this tag.

**Keywords:** photo privacy, privacy tag, online social network

## 1 Introduction

Online social networks (OSNs), such as Facebook and Instagram, have become popular with people of all ages, and online communication with friends and acquaintances via messages that include photos and videos has become very common.

As it has become very easy for users to take and post photos, the inadvertent disclosure of sensitive information through mistakes made while posting has become a problem [1]. A message containing sensitive information can be passed along by the user or by the user's friends to acquaintances and strangers. Disclosure of such information can trigger unexpected problems such as loss of credibility. In a survey on awareness of information security ethics in Japan [4], researchers found that 70% of the respondents were not aware of the problems related to posting in OSNs photos containing other people. In response to this situation, and in order to avoid unnecessary trouble when making OSN posts [5], it was recommended that photos be processed before posting, specifically by (1) deleting location and other metadata, (2)

obtaining permission from subjects before posting, and (3) preventing the identification of people that are unnecessarily included in the photos. However, since it is complicated to carry out all these measures every time a post is made, there is a need for a procedure that can be implemented easily.

People have different policies regarding privacy in daily life. Additionally, one person might have different policies depending on the communities to which he or she belongs [6]. Similarly, OSN users have subjective judgment criteria corresponding to the contents of the message being posted [8]. Moreover, they can belong to multiple OSN communities, which are created using social access control lists (SACLs) that classify friends into subsets that are used to determine which messages they can see. When posting a message or photo, the user can choose the target community appropriate for the situation and content of the post [7]. Users can share their posts more effectively by using SACLs to control disclosure to the particular individuals or communities that they think would be interested in the post [8, 9]. However, users are sometimes unhappy about unintentional people such as different community people on the SACL and people not on the SACL seeing their photos or finding out about their activities and other information included in the post, which can happen if a post is unintentionally or unthinkingly shared with a certain community [10]. Many people are sensitive about privacy and believe that they always make correct privacy-related decisions. However, it is not easy to make the right choice for every situation. For example, users tend to make wrong decisions about posting when undergoing changes in feelings and emotions [14], meaning that it is difficult to always make correct decisions when posting in OSNs. Therefore, a function is needed that can easily reflect privacy policies matching the user's communities or situation instead of merely relying on the user's subjective decision criteria. While there are several kinds of sensitive information that a user may unintentionally disclose in a posted message or photo, this study focused on protecting the privacy of people appearing in photos that are to be posted.

We have developed a method (PrivacyTag) for adaptively protecting (blurring) the facial area of people appearing in photos to be posted within and outside the communities to which they belong by using tags embedded with community-based privacy policies. The application of this method enables the protection of privacy based on the privacy policy of the photographed subject instead of relying on the subjective judgment of the OSN poster or photographer.

## 2 Related work

### 2.1 OSN user privacy

OSNs offer various privacy settings and functions to prevent the disclosure of users' sensitive information. However, privacy management is not only complicated, maintaining it requires a lot of effort [7]. This has prompted many studies on information disclosure boundaries, including proposals for access control for posts [7,11,12]. However, many of these studies focused on the privacy of the poster while ignoring the privacy of others in a photo. In fact, problems resulting from posting personally

identifiable photos without permission have been reported in case studies about regrets of OSN users after posting [8,13,14], showing that there is a need to also consider the privacy of everyone appearing in photos posted in OSNs. Therefore, we developed a method for reflecting the privacy policies of the subjects rather than protecting privacy only on the basis of the judgment criteria of the poster.

### 2.2 Privacy protection for photographed subjects

Before the privacy policy of a subject can be respected, the policy first has to be determined. This can be achieved by methods that use (1) facial recognition, (2) radio frequency identification, or (3) tag recognition. Methods that use facial recognition involve linking facial features and privacy policies in advance, conducting facial recognition when a user posts photos, and applying and notifying the user of the subject's privacy policy [15,16]. While these measures have the benefit of working without always having to wear tags, they require potential subjects to register their facial features and other physical characteristics to the system, which may be rejected due to privacy concerns [17]. With methods that use radio frequency identification, a person who is a candidate for privacy protection carries an RFID tag containing his privacy policy. When an RFID tracking system detects the person, he is anonymized on the basis of the privacy policy [3, 24]. These methods need to integrate unified tag specifications so that the RFID readers can recognize any tag. The tag recognition methods require wearing tags that show one's policies, conducting tag analysis when photos are to be posted, and applying the policies of the photographed subjects. In a previous study, Dabrowski et al. [2] proposed using a personal photo policy framework based on a simplified symbol/accessory or button with a 2D barcode containing the subject's privacy policy. Pallas et al. [18] proposed wearing and displaying simplified tags that can be easily distinguished by people as well as machines. Other proposed methods control privacy by embedding many different kinds of policies in QR codes [6,19]. Bo et al. [6] proposed using a QR-code-based tag (Privacy.Tag) embedding the subject's flexible privacy policy including allowed and disallowed domains. However, since such simplified tags cannot contain a large amount of information, it is difficult to use them to express varying community-based privacy policies. Conversely, with QR codes and other complex tags that contain large amounts of information, there are problems with detection accuracy and analysis depending on the distance to the photographed subject. Thus, none of these methods are practical for OSN application.

Also, in the method that uses tag recognition, when a person wears a policy tag, that person displays their policy to people around them. Since that policy can also be considered sensitive information, some people believe it should be hidden. Making them visible to people taking photos, however, promotes respect for the subject's policy [16]. Thus, in our proposal, we adopted a method that uses tag recognition, does not require the registration of physical attributes into the system, and applies policies acquired from tags worn by photographed subjects.

## 3 Method overview

Our PrivacyTag method protects the privacy of people appearing in photos by adaptively blurring their facial area in photos to be posted within and outside the community to which that person belongs by using tags embedded with the community-based privacy policies. This method makes it possible to detect and analyze tags worn by individuals appearing in a photo and to blur and anonymize their facial areas in accordance with the policies acquired through analysis of the tags. Additionally, users can define to which communities they belong, and users can be assigned to those communities by using community information included in the tags. This enables subjects to wear tags that contain policies that differ for each community and to implement different privacy policies depending on the situation. Further, by specifying a particular community as the intended audience of a post, the user can restrict access to posted messages and thereby prevent inadvertent disclosure of sensitive information.

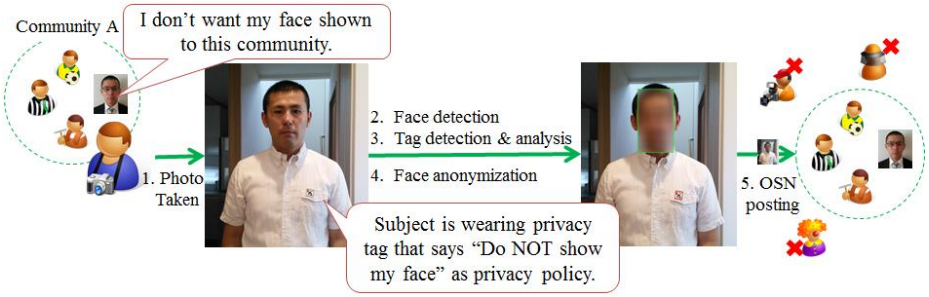



**Fig. 1.** Simple example of how proposed method works

Figure 1 shows a simple example of how the proposed method works when the subject has a policy for only one community. In this case, he does not want his face shown to the community members, so he wears a privacy tag containing "Do not show my face" as his privacy policy. If a photographer using our smartphone application takes a photo of him, the application detects the subject's face and the tag being worn and analyzes the embedded policy. It then blurs his facial area in accordance with the policy and publishes a message including this photo in an OSN. The community members who are friends of the photographer can see the message with the anonymized photo. Other community members such as acquaintances and strangers cannot even see the message.

This method is composed of three main functions: (1) Privacy Tag, (2) Photo Privacy Realizer, and (3) Privacy Wall. The following sub-sections explain these functions and the flow of the proposed method.

### 3.1 Privacy Tag

A privacy tag contains the wearer's privacy policy for each community to which she belongs. The tag is worn as a fashion accessory and displays the wearer's privacy

policy. The design, analysis algorithm, and evaluation of the privacy tag are explained in Chapter 4.

### 3.2 Photo Privacy Realizer

The Photo Privacy Realizer (PPR) is a Web application that detects a person in a photo being posted in an OSN, detects and analyzes the privacy tag that the person is wearing, and performs protection measures for the facial area of the person in accordance with the policy acquired through the tag analysis. It is designed for use on smartphones and other devices and consists of two functions: (1) community management and (2) photo taking and anonymization. The PPR blurs the facial area on the basis of the acquired policy to anonymize the subject. It then posts the anonymized photo and message in the OSN, and they are visible only to the community members. Chapter 5 discusses a prototype PPR.

### 3.3 Privacy Wall

Privacy Wall is a function for protecting the privacy of a subject wearing a privacy tag in photos taken with ordinary digital cameras and devices that do not have the PPR installed. It is to be configured as a function offered by OSN providers. When a post is made, it detects the privacy tags and anonymizes the facial areas in accordance with the tags being worn. This function is only a proposal at the moment; it will be addressed in a future study.

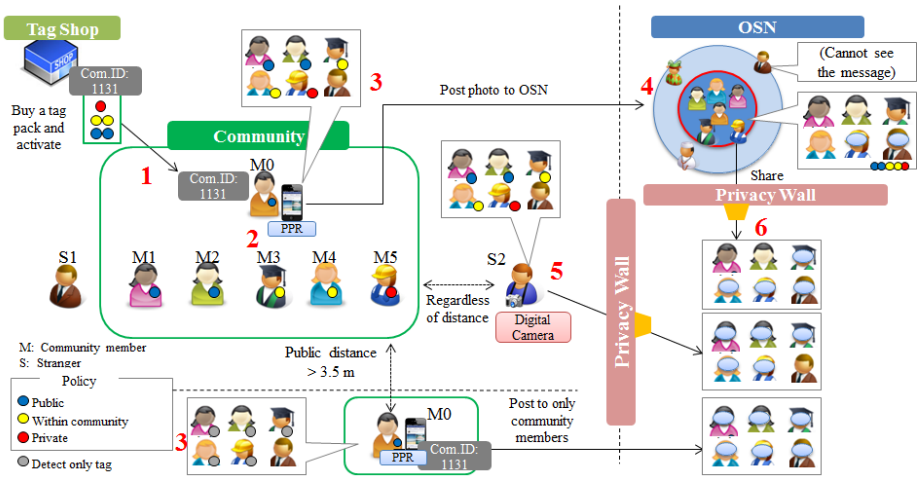



**Fig. 2.** Process flow of proposed method

### 3.4 Process flow

Figure 2 shows the process flow of the proposed method. The numbers in red correspond to the following steps.

**1) Tag acquisition:** Tags are bought from participating stores in a pack with three types of tags: public, private, and within community that include common community IDs. The user can also print her own tags.

**2) Tag activation and community registration:** After purchasing the tags, the user uses the PPR to activate a tag and register a new community. She can then select the members of the community from her OSN friend list. All community members are asked to wear a tag with their own privacy policy.

**3) Photo taking and anonymization:** A photo is taken using the PPR, which analyzes the tags worn by the subjects. If a subject is wearing a tag with a "private" policy, his facial area is blurred (Fig. 2, M5). Moreover, if people who are not members of the community appear in the photo, they are also anonymized to respect their privacy even though their policy cannot be acquired since they are not wearing tags (Fig. 2, S1). Likewise, if a tag is detected for someone but cannot be analyzed due to distance or other reasons, that person is anonymized as well.

**4) OSN Posting:** After processing the photo to protect the privacy of the subjects, the user posts the photo in the OSN along with a message. The post is restricted to members of the community and they can see the anonymized photo.

**5) Taking photos and posting from non-PPR devices:** If a person outside the community posts a photo taken using a device or application without the PPR, the Privacy Wall of the OSN provider detects only the presence of tags and anonymizes all subjects wearing tags.

**6) Reposting outside the community:** When messages already posted are shared in the community or reposted outside the community, the privacy policies are acquired from the photo metadata, and anonymization is carried out on the basis of those policies.

### 3.5 Effect of distance from photographer

Protection of the facial area of the subject depends on (1) the distance between the photographer and subject and (2) whether the device used to take the photo was equipped with the PPR. According to a classification of photos posted on Instagram [20], photos fall into eight categories such as selfies, food, and pets. Selfies and group

photos with two or more friends comprised 46.6% of the photos posted. To determine the distance within which tag detection and analysis should be accurate, we referred to the classification of personal space by Hall [21]. As shown in Table 1, he defined four distance categories. Since many of the photos posted on Instagram are either selfies or group photos with two or more friends, we assumed that many of the photos posted in OSNs fall into the categories of intimate, personal, and social. This means that the detection and analysis of tags should work accurately up to a distance of 350 cm from the photographer.

**Table 1.** Personal space classification by Hall

| Distance Category | Description | Distance |
|---|---|---|
| Intimate | Distance where only very close people are permitted | 0 – 45 cm |
| Personal | Distance when talking to friends | 45 – 120 cm |
| Social | Distance when talking to acquaintances and unrelated people | 120 – 350 cm |
| Public | Distance in public intercourse | 350 – 750 cm |

# 4 Tag realization

This section explains the design and the detection and analysis algorithm of the privacy tag we are proposing. We also compare our proposed tag with a QR-code-based tag used in conventional methods and demonstrate improvements in detection and analysis accuracy, which was previously limited by the distance to the subject.

## 4.1 Preliminary evaluation

The design of the privacy tag takes into account the method used for tag detection and analysis. We created a frame to enclose the tag and assumed the following steps: detection of the frame, reading of the bit pattern inside the frame, and determining whether it is a privacy tag or not. On the basis of these assumptions, we performed a preliminary evaluation of (1) detection accuracy based on frame line width and distance and (2) accuracy of reading bit patterns depending on distance. For both tests, we used 5 × 5 cm tags and took photos of them with a digital camera (resolution of 20.9 megapixels). Photo taking was considered successful when the frame or bit outline was clearly captured in the photo.

Figure 3 compares detection accuracy for different frame line widths (1 mm to 5 mm) and distances (in 1.5 m increments up to 12 m). For a frame line width of 2 mm or less, the farther the subject from the photographer, the more difficult it was to detect the frame outline. A frame line width of 3 mm or more could be detected up to a distance of 12 m. Figure 4 shows the results for reading bit patterns with 7 bits/surface. The bit patterns were mostly readable at distances of 6 m or less from the

photographer. The tags were designed on the basis of these results, as discussed in the next section.

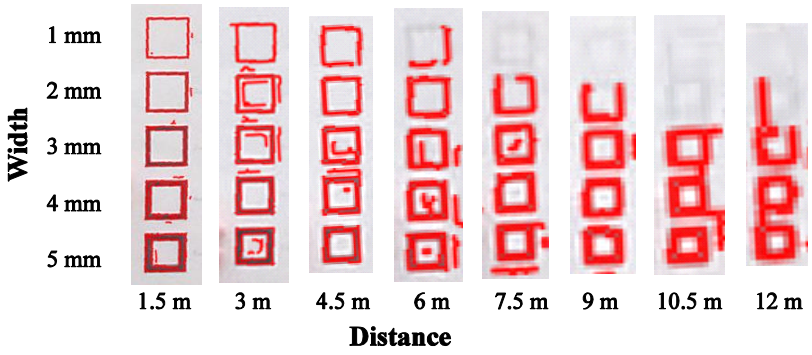



**Fig. 3.** Comparison of 5 × 5 cm outline detection for different frame line widths and distance

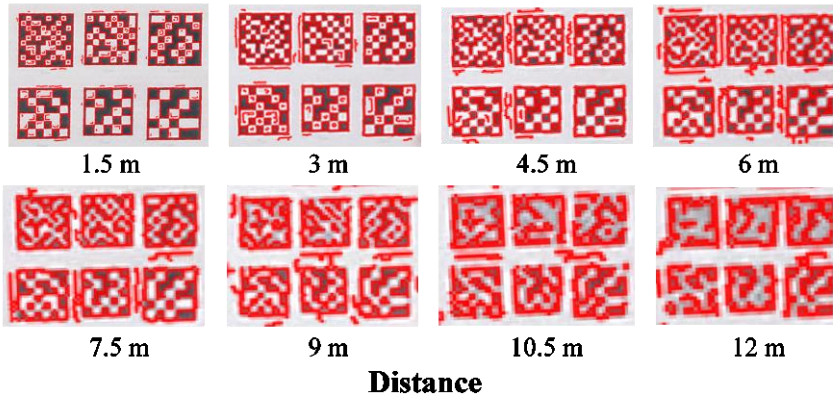



**Fig. 4.** Comparison of 5 × 5 cm bit pattern reading at different distances

**Table 2.** Disclosure policies

| Disclosure Policy | Description |
|---|---|
| Private | Do not show facial area either within or outside community |
| Within community | Show facial area within particular community |
| Public | Show facial area regardless of community |

### 4.2 Disclosure policy design

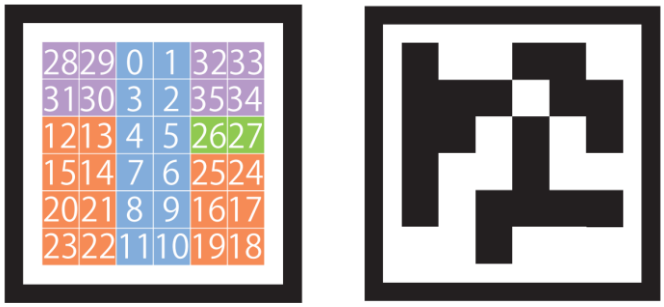
Preventing inadvertent disclosure of sensitive information in photos does not require complex settings, so it is possible to carry out protection using only a few bits for

expressing face information, tags, and disclosure/non-disclosure of location, etc. [22]. As shown in Table 2, we defined three privacy policies: (1) private, (2) within community, and (3) public.

### 4.3 Bit pattern design

The pattern of the bits in the tag used to store the disclosure policy and applicable community information was designed as shown in Fig. 5 (a). A sample tag is shown in Fig. 5 (b).

Two requirements were set: (1) the bits should be readable regardless of tag orientation, and (2) error correction should be carried out based on burst error. To meet these requirements, we assumed that burst errors occur within the tag in the following order of likelihood: upper left/right → lower left/right → middle area. In accordance with these assumptions, we placed the bit pattern indicating the tag orientation as the header part in the two center columns to enable the system to quickly detect the tag and determine its orientation (Fig. 5 (a), bits 0-11). Next, we placed the community ID and the disclosure policy, i.e., the privacy policy, in the central and lower part on the left and right sides (Fig. 5 (a), bits 12-25, 26-27). We use the Reed-Solomon Code as the error-correcting code, meaning that error correction is possible for each symbol (= 4 bits). The header part is excluded from error correction. The error-correcting code is located in the upper left and right corners (Fig. 5 (a), bits 28-34).




(a) Bit pattern (b) Sample tag

**Fig. 5.** Privacy Tag

### 4.4 Detection and analysis

As shown in Fig. 6, tag detection/analysis and face detection are carried out in parallel. The first step in tag detection/analysis is to detect the tag frame. Next, image correction is carried out to adjust the tag orientation, after which the bit pattern inside the tag is read. Finally, the decision of whether it is a privacy tag is made on the basis of matching with the header part, which indicates the orientation of the tag. For face detection, we use a method based on the Viola-Jones face detection algorithm [23].

The error-correction code is used to complement bits that cannot be read, if there are any.

After tag detection and analysis, the system identifies the subject wearing a tag. Matching is carried out under the assumptions that the subject is wearing the tag on the upper part of his or her body directly under the face and that the tag is three times the width and four times the height of the detected face (3W × 4H). Finally, the facial area is blurred or not blurred in accordance with the policy embedded in the tag. Moreover, if several faces are detected in a photo, the process can find a suitable tag for each one and blur the faces in accordance with the acquired policies.

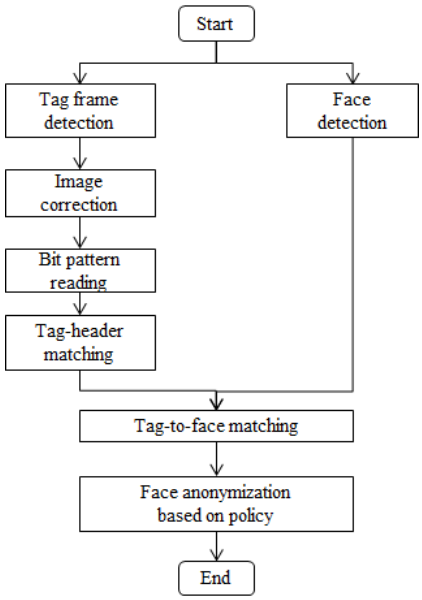



**Fig. 6.** Flow of tag detection and analysis

### 4.5 Experimental evaluation

To compare the performance of our proposed tag with that of QR-code-based tags used in conventional methods, we first measured the accuracy of tag detection and analysis for tags with a width and height of 2 cm to 10 cm at distances of 45 cm to 1050 cm from the photographer. We used a version-1 QR code and a digital camera with a resolution of 20.9 megapixels. The photos were taken outdoors in sunny conditions. Photos of a person wearing the QR-code-based tag and the proposed tag are shown in Fig. 7. As shown in Fig, 8, for tags 5 × 5 cm or smaller, which is considered to be a realistic size with regards to wearability, our tag could be detected and analyzed at a greater distance. For sizes between 2 and 5 cm, the QR code could be read from 120 cm up to a maximum of 350 cm while our proposed tag could be read up to 450 cm. As shown in Fig. 7 (b), the bits in the proposed tag (3 cm in size) were clear and could be read at 350 cm while those in the QR code tag were blurred and could

not be read. As discussed above, the intended scope of privacy protection ranges up to the social distance (350 cm), and these results show that it is possible to detect and analyze reasonably sized tags within the social distance. Furthermore, as shown by the photos of someone wearing a 10 cm tag in Fig. 7 (a), a practical size for the tag is 5 cm or less.

(a) 10 cm; 350 cm (b) 3 cm; 350 cm

**Fig. 7.** Photos showing wearing of proposed tag (left phots) and QR code tag (right photos)

**Proposed tag** (cm)

| Size/Dist. | 45 | 82.5 | 120 | 235 | 350 | 450 | 550 | 650 | 750 | 850 | 950 | 1050 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND | ND | ND |
| 3 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND | ND |
| 5 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND | ND |
| 7.5 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✠ | ND | ND | ND | ND | ND |
| 10 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND |

Intimate Distance | Personal Distance | Social Distance | Public Distance

✔ - Tag detection & analysis
✠ - Tag detection
ND - No detection

**QR code tag** (cm)

| Size/Dist. | 45 | 82.5 | 120 | 235 | 350 | 450 | 550 | 650 | 750 | 850 | 950 | 1050 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 cm | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND | ND | ND | ND | ND |
| 3 cm | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND | ND | ND | ND |
| 5 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND | ND | ND |
| 7.5 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND | ND |
| 10 cm | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ND | ND | ND | ND |

**Fig. 8.** Results of comparison of the proposed tag and QR code tag

# 5 Application implementation

In this section, we present a high-level application of our proposed Photo Privacy Realizer (PPR) and a prototype implementation.

## 5.1 Overview

The purpose of the PPR is to reflect a photographed subject's privacy policy acquired through analysis of the subject's privacy tag before publishing an original photo in an OSN. Figure 9 shows the PPR process flow.

The PPR is composed of two modules: (1) community management and (2) photo taking and anonymization. The community management module creates a community and assigns OSN users to the community. First, the photographer activates a tag and creates a community. The PPR sets an expiration date for the tag automatically. The photographer then assigns users to the created community by using his OSN friend list. The PPR can create and manage several communities. After the community is activated, the photo-taking and anonymization module is used to take a photo and reflect the subject's privacy policy in accordance with the result of analyzing the privacy tag. Finally, the PPR is used to publish a message with the anonymized photo only to community members.

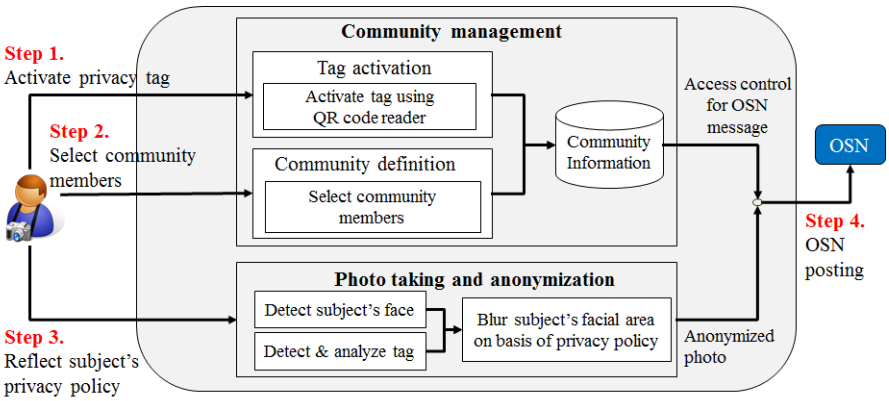
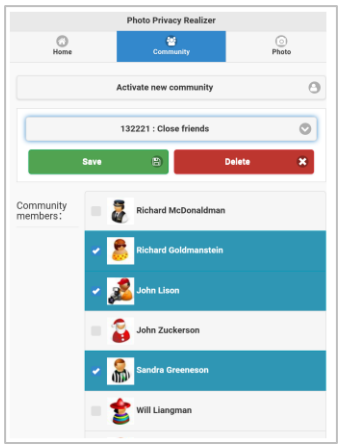
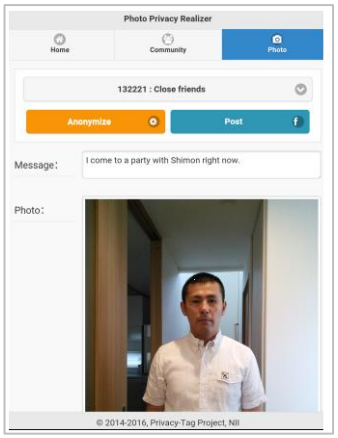


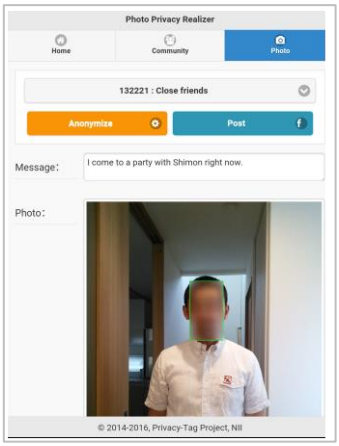

**Fig. 9.** Photo Privacy Realizer process flow




(a) Community management




(b) Photo taking




(c) Facial area blurring


(d) Posting to community

**Fig. 10.** Flow of operation

## 5.2 Prototype implementation

We developed a prototype implementation of the PPR designed for Facebook. The user interface is shown in Figure 10, and the operation flow is as follows.

**Community management:** The community management function of the PPR is used to activate a community and assign users to the community. The user first logs into her Facebook account through the PPR interface (Fig. 10 (a)). After the user has logged in, her Facebook friend list is displayed. To activate (create) a community, the user presses the "Activate new community" button and registers the community ID

attached to the purchased tag pack. After registering the community, the user then selects users to be included in the community by tapping on the respective friends' names. Users can be deleted from the community in the same way. After adding members, the user saves the community information. The community pull-down menu can be used to switch between communities and manage friends belonging to different communities.

**Photo taking and anonymization:** This function detects faces in new or old photos, detects and analyzes tags, and blurs faces depending on the acquired policies and the community specified in the PPR. First, the user inputs the message and takes the photo (Fig. 10 (b)); at this point, the tag has not yet been detected or analyzed). Next, the user presses the "Anonymize" button to analyze the tags in the photo, and anonymization is performed in accordance with the results of the analysis. Anonymization is also carried out when communities in the tags do not match. Finally, the user presses the "Post" button to post the message and the anonymized photo in the OSN (Fig. 10 (c)). They are visible only to members of the selected community (Fig. 10 (d)).

## 6 Conclusions and future work

We have developed a method called "PrivacyTag" for adaptively blurring the facial area of a photographed subject in accordance with the communities to which the subject belongs by using privacy tags embedded with community-based privacy policies. We also evaluated the tag used for this by performing a preliminary evaluation of tag frame detection and bit reading and comparing the performance of our proposed tag with a QR-code-based tag for different tag sizes and distances from the photographer. We were able to demonstrate improved detection and analysis accuracy, which was previously limited by the distance to the subject. Furthermore, we created a prototype application (Photo Privacy Realizer) designed for Facebook using the proposed tag that can be used to publish an OSN message with an anonymized photo to only community members.

One open question is whether blurring the subject's face is sufficient for protecting the subject's privacy because a person who knows the subject may be able to recognize him or her from the subject's clothing or another simple factor. Another question regarding anonymization is whether, if all the subjects in a photo have a tag, is there is a possibility of blurring all the faces. If so, no one may want to post photos in OSNs. However, the basic concept of our method is that maximum safety measures are taken in cases where the subject's policy cannot be acquired and applied.

Also, we compared the performance of the proposed privacy tag with that of a QR-code-based tag in terms of detection and analysis accuracy for tags of various sizes and at various distances. Since the comparison with QR code tags was limited, future work includes more evaluation to improve the tag design. Finally, we showed as a first step that our method can protect the privacy of people appearing in phots without relying on subjective decisions by OSN posters and photographers.

## Acknowledgment

This work was supported by JSPS KAKENHI Grants (JP16H06302 and JP15H01686).

## References

1. B. Bosker: The Twitter Typo That Exposed Anthony Weiner, http://www.huffingtonpost.com/2011/06/07/anthony-weiner-twitter-dm_n_872590.html, last accessed 2017/05/10.
2. A. Dabrowski, E.R. Weippl, I. Echizen: Framework based on Privacy Policy Hiding for Preventing Unauthorized Face Image Processing. In Proceedings of 2013 IEEE International Conference on Systems, Man and Cybernetics, pp. 455-461 (2013).
3. J. Wickramasuriya, M. Datt, S. Mehrotra, N. Venkatasubramanian: Privacy Protecting Data Collection in Media Spaces. In Proceedings of the 12th annual ACM international conference on Multimedia pp. 48-55 (2004).
4. Survey research regarding ethics of information security in 2014 (in Japanese), https://www.ipa.go.jp/files/000044094.pdf, last accessed 2017/05/10.
5. Be careful when you post a photo during your vacation (in Japanese), http://www.ipa.go.jp/security/txt/2015/05outline.html, last accessed 2017/05/10.
6. C. Bo, G. Shen, J. Liu, X.-Y. Li, Y. Zhang, F. Zhao: Privacy.tag: privacy concern expressed and respected. In Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, pp. 163-176 (2014).
7. M. Mondal, Y. Liu, B. Viswanath, K.P. Gummadi, A. Mislove: Understanding and Specifying Social Access Control Lists. In Proceedings of the Tenth Symposium On Usable Privacy and Security, pp. 271-283 (2014).
8. M. Sleeper, R. Balebako, S. Das, A.L. McConahy, J. Wiese, L.F. Cranor: The post that wasn't: exploring self-censorship on facebook. In Proceedings of the 2013 conference on Computer supported cooperative work, pp. 793-802 (2013).
9. A. Besmer, H.R. Lipford: Privacy Perceptions of Photo Sharing in Facebook. In Proceedings of the Fourth Symposium on Usable Privacy and Security (2008).
10. P. Kumar, S. Schoenebeck: The Modern Day Baby Book: Enacting Good Mothering and Stewarding Privacy on Facebook. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, pp. 1302-1312 (2015).
11. S. Egelman, A. Oates, S. Krishnamurthi: Oops, I did it again: mitigating repeated access control errors on facebook. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2295-2304 (2011).
12. S. Machida, T. Kajiyama, S. Shigeru, I. Echizen: Analysis of Facebook Friends Using Disclosure Level. In Proceedings of the Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 471-474 (2014).
13. M. Sleeper, J. Cranshaw, P.G. Kelley, B. Ur, A. Acquisti, L.F. Cranor, N. Sadeh: "I read my Twitter the next morning and was astonished": a conversational perspective on Twitter regrets. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3277-3286 (2013).
14. Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P.G. Leon, L.F. Cranor: "I regretted the minute I pressed share": a qualitative study of regrets on Facebook. In Proceedings of the Seventh Symposium on Usable Privacy and Security, pp. 10 (2011).

15. B. Henne, C. Szongott, M. Smith: SnapMe if you can: privacy threats of other peoples' geo-tagged media and what we can do about it. In Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, pp. 95-106 (2013).
16. P. Pappachan, R. Yus, P.K. Das, T. Finin, E. Mena, A. Joshi: A semantic context-aware privacy model for faceblock. In Proceedings of the 2nd International Conference on Society, Privacy and the Semantic Web - Policy and Technology, pp. 64-72 (2014).
17. Y. Li, K. Xu, Q. Yan, Y. Li, R.H. Deng: Understanding OSN-based facial disclosure against face authentication systems. In Proceedings of the 9th ACM symposium on Information, computer and communications security, pp. 413-424 (2014).
18. F. Pallas, M.-R. Ulbricht, L. Jaume-Palasí, U. Höppner: Offlinetags: a novel privacy approach to online photo sharing. In Proceedings of CHI '14 Extended Abstracts on Human Factors in Computing Systems, pp. 2179-2184 (2014).
19. A. Cammozzo: TagMeNot, http://tagmenot.info/, last accessed 2017/05/10.
20. Y. Hu, L. Manikonda, S. Kambhampati: What We Instagram: A First Analysis of Instagram Photo Content and User Types. In Proceedings of the 8th International AAAI Conference on Weblogs and Social Media (2014).
21. ET. Hall: The hidden dimension. New York: Anchor Books/Doubleday (1966).
22. A. Ashok, V. Nguyen, M. Gruteser, N. Mandayam, W. Yuan, K. Dana: Do not share!: invisible light beacons for signaling preferences to privacy-respecting cameras. In Proceedings of the 1st ACM MobiCom workshop on Visible light communication systems, pp. 39-44 (2014).
23. P. Viola, M.J. Jones: Robust Real-Time Face Detection. International Journal of Computer Vision, vol. 57, issue 2, pp. 137-154. Springer (2004).
24. S.-C.S. Cheung, M.V. Venkatesh, J.K. Paruchuri, J. Zhao, T. Nguyen: Protecting and Managing Privacy Information in Video Surveillance Systems. Protecting Privacy in Video Surveillance, pp. 11-33 (2009).