Faceless Person Recognition: Privacy Implications in Social Media

Seong Joon Oh(✉), Rodrigo Benenson, Mario Fritz, and Bernt Schiele

Max-Planck Institute for Informatics, Saarbrücken, Germany
{joon,benenson,mfritz,schiele}@mpi-inf.mpg.de

Abstract. As we shift more of our lives into the virtual domain, the volume of data shared on the web keeps increasing and presents a threat to our privacy. This works contributes to the understanding of privacy implications of such data sharing by analysing how well people are recognisable in social media data. To facilitate a systematic study we define a number of scenarios considering factors such as how many heads of a person are tagged and if those heads are obfuscated or not. We propose a robust person recognition system that can handle large variations in pose and clothing, and can be trained with few training samples. Our results indicate that a handful of images is enough to threaten users' privacy, even in the presence of obfuscation. We show detailed experimental results, and discuss their implications.

Keywords: Privacy · Person recognition · Social media

1 Introduction

With the growth of the internet, more and more people share and disseminate large amounts of personal data be it on webpages, in social networks, or through personal communication. The steadily growing computation power, advances in

Person A training samples. Is this person A ?

Fig. 1. An illustration of one of the scenarios considered: can a vision system recognise that the person in the right image is the same as the tagged person in the left images, even when the head is obfuscated?

Electronic supplementary material The online version of this chapter (doi:10.1007/978-3-319-46487-9_2) contains supplementary material, which is available to authorized users.

© Springer International Publishing AG 2016
B. Leibe et al. (Eds.): ECCV 2016, Part III, LNCS 9907, pp. 19–35, 2016.
DOI: 10.1007/978-3-319-46487-9_2

machine learning, and the growth of the internet economy, have created strong revenue streams and a thriving industry built on monetising user data. It is clear that visual data contains private information, yet the privacy implications of this data dissemination are unclear, even for computer vision experts. We are aiming for a transparent and quantifiable understanding of the loss in privacy incurred by sharing personal data online, both for the uploader and other users who appear in the data.

In this work, we investigate the privacy implications of disseminating photos of people through social media. Although social media data allows to identify a person via different data types (timeline, geolocation, language, user profile, etc.) [1], we focus on the pixel content of an image. We want to know how well a vision system can recognise a person in social photos (using the image content only), and how well users can control their privacy when limiting the number of tagged images or when adding varying degrees of obfuscation (see Fig. 1) to their heads.

An important component to extract maximal information out of visual data in social networks is to fuse different data and provide a joint analysis. We propose our new Faceless Person Recogniser (described in Sect. 5), which not only reasons about individual images, but uses graph inference to deduce identities in a group of non-tagged images. We study the performance of our system on multiple privacy sensitive user scenarios (described in Sect. 3), analyse the main results in Sect. 6, and discuss implications and future work in Sect. 7. Since we focus on the image content itself, our results are a lower-bound on the privacy loss resulting from sharing such images.

Our contributions are:

- We discuss dimensions that affect the privacy of online photos, and define a set of scenarios to study the question of privacy loss when social media images are aggregated and processed by a vision system.
- We propose our new Faceless Person Recogniser, which uses convnet features in a graphical model for joint inference over identities.
- We study the interplay and effectiveness of obfuscation techniques with regard of our vision system.

2 Related Work

Nowadays, essentially all online activities can be potentially used to identify an internet user [1]. Privacy of users in social network is a well studied topic in the security community [1–4]. There are works which consider the relationship between privacy and photo sharing activities [5,6], yet they do not perform quantitative studies.

Camera Recognition. Some works have shown that it is possible to identify the camera taking the photos (and thus link photos and events via the photographer), either from the file itself [7] or from recognisable sensing noise [8,9]. In this work we focus exclusively on the image content, and leave the exploitation of image content together with other forms of privacy cues (e.g. additional meta-data from the social network) for future work.

Image Types. Most previous work on person recognition in images has focused either on face images [10] (mainly frontal head) or on the surveillance scenario [11,12], where the full body is visible, usually in low resolution. Like other areas of computer vision, the last years have seen a shift from classifiers based on hand-crafted features and metric learning approaches [13–19] towards methods based on deep learning [20–27]. Different from face recognition and surveillance scenarios, the social network images studied here tend to show a diverse range of poses, activities, points of view, scenes (indoors, outdoors), and illumination. This increased diversity makes recognition more challenging and only a handful of works have addressed explicitly this scenario [28–30]. We construct our experiments on top of the recently introduced PIPA dataset [29], discussed in Sect. 4.

Recognition Tasks. The notion of "person recognition" encompasses multiple related problems [31]. Typical "person recognition" considers a few training samples over many different identities, and a large test set. It is thus akin to fine grained categorization. When only one training sample is available and many test images (typical for face recognition and surveillance scenarios [10,12,32]), the problem is usually named "re-identification", and it becomes akin to metric learning or ranking problems. Other related tasks are, for example, face clustering [26,33], finding important people [34], or associating names in text to faces in images [35,36]. In this work we focus on person recognition with on average 10 training samples per identity (and hundreds of identities), as in typical social network scenario.

Cues. Given a rough bounding box locating a person, different cues can be used to recognise a person. Much work has focused on the face itself ([20–27,37] to name a few recent ones). Pose-independent descriptors have been explored for the body region [28–30,38,39]. Various other cues have been explored, for example: attributes classification [40,41], social context [42,43], relative camera positions [44], space-time priors [45], and photo-album priors [46]. In this work, we build upon [30] which fuses multiple convnet cues from head, body, and the full scene. As we will discuss in the following sections, we will also indirectly use photo-album information.

Identify Obfuscation. Some previous works have considered the challenges of detection and recognition under obfuscation (e.g. see Fig. 1). Recently, [47] quantified the decrease in Facebook face detection accuracy with respect to different types of obfuscation, e.g. blur, blacking-out, swirl, and dark spots. However, on principle, obfuscation patterns can expose faces at a higher risk of detection by a fine-tuned detector (e.g. blur detector). Unlike their work, we consider the *identification* problem with a system *adapted* to obfuscation patterns. Similarly, a few other works studied face recognition under blur [48,49]. However, to the best of our knowledge, we are the first to consider person recognition under head obfuscation using a trainable system that leverages full-body cues.

3 Privacy Scenarios

Fig. 2. Obfuscation types considered.

We consider a hypothetical social photo sharing service user. The user has a set of photos of herself and others in her account. Some of these photos have identity tags and the others do not have such identity tags. We assume that all heads on the test photos have been detected, either by an automatic detection system, or because a user is querying the identity of a specific head. Note that we do not assume that the faces are visible nor that persons are in a frontal-upstanding pose. A "tag" is an association between a given head and a unique identifier linked to a specific identity (social media user profile).

Goal. The task of our recognition system is to identify a person of interest (marked via its head bounding box), by leveraging all the photos available (both with and without identity tags). In this work, we want to explore how effective different strategies are to protect the user identity.

We consider four different dimensions that affect how hard or easy it is to recognise a user:

Number of Tagged Heads. We vary the number of tagged images available per identity. The more tagged images available, the easier it should be to recognise someone in new photos. In the experiments of Sects. 5 and 6 we consider that 1∼10 tagged images are available per person.

Obfuscation Type. Users concerned with their privacy might take protective measures by blurring or masking their heads. Other than the fully visible case (non-obfuscated), we consider three other obfuscations types, shown in Fig. 2. We consider both black and white, since [47] showed that commercial systems might react differently to these. The blurring parameters are chosen to resemble the YouTube face blur feature.

Amount of Obfuscation. Depending on the user's activities (and her friends posting photos of her), not all photos might be obfuscated. We consider a variable fraction of these.

Domain Shift. For the recognition task, there is a difference if all photos belong to the same event, where the appearance of people change little; or if the set of photos without tags correspond to a different event than the ones with identity tags. Recognising a person when the clothing, context, and illumination have changed ("across events") is more challenging than when they have not ("within events").

Table 1. Privacy scenarios considered. Each row in the table can be applied for the "across events" and "within events" case, and over different obfuscation types. See text Sect. 3. The obfuscation fraction indicates $^{\text{tagged}}/_{\text{non-tagged}}$ heads. Bold abbreviations are reused in follow-up figures. In scenario S_1^τ, $\tau \in \{1.25, 2.5, 5, 10\}$.

Abbreviation	Brief description	Amount of tagged heads	Amount of obfuscated heads
S_0	Privacy indifferent	100 %	0 %
$\mathbf{S_1^\tau}$	Some of my images are tagged	τ instances	0 %
$\mathbf{S_2}$	One non-tagged head is obfuscated	10 instances	0 %/1 instance
$\mathbf{S_3}$	All my heads are obfuscated	10 instances	100 %
S_3'	All tagged heads are obfuscated	10 instances	100 %/0 %
S_3''	All non-tagged heads are obfuscated	10 instances	0 %/100 %

Based on these four dimensions, we discuss a set of scenarios, summarised in Table 1. Clearly, these only cover a subset of all possible combinations along the mentioned four dimensions. However, we argue that this subset covers important and relevant aspects for our exploration on privacy implications.

Scenario S_0. Here all heads are fully visible and tagged. Since all heads are tagged, the user is fully identifiable. This is the classic case without any privacy.

Scenario S_1. There is no obfuscation but not all images are tagged. This is the scenario commonly considered for person recognition, e.g. [28–30]. Unless otherwise specified we use S_1^{10}, where an average of 10 instances of the person are tagged (average across all identities). This is a common scenario for social media users, where some pictures are tagged, but many are not.

Scenario S_2. Here the user has all of her heads visible, except for the one non-tagged head being queried. This would model the case where the user wants to conceal her identity in one particular published photo.

Scenario S_3. The user aims at protecting her identity by obfuscating all her heads (using any obfuscation type, see Fig. 2). Both tagged and non-tagged heads are obfuscated. This scenario models a privacy concerned user. Note that the body is still visible and thus usable to recognise the user.

Scenarios S_3'&S_3''. These consider the case of a user that inconsistently uses the obfuscation tactic to protect her identity. Albeit on the surface these seems like different scenarios, if the visual information of the heads cannot be propagated from/to the tagged/non-tagged heads, then these are functionally equivalent to S_3.

Each of these scenarios can be applied for the "across/within events" dimension. In the following sections we will build a system able to recognise persons across these different scenarios, and quantify the effect of each dimension on the recognition capabilities (and thus their implication on privacy). For our system, the tagged heads become training data, while the non-tagged heads are used as test data.

4 Experimental Setup

We investigate the scenarios proposed in Sect. 3 through a set of controlled experiments on a recently introduced social media dataset: PIPA (People In Photo Albums) [29]. In this section, we project the scenarios in Sect. 3 onto specific aspects of the PIPA dataset, describing how much realism can be achieved and what are possible limitations.

PIPA Dataset. The PIPA dataset [29] consists of annotated social media photos on Flickr. It contains ∼40k images over ∼2k identities, and captures subjects appearing in diverse social groups (e.g. friends, colleagues, family) and events (e.g. conference, vacation, wedding). Compared to previous social media datasets, such as [28] (∼600 images, 32 identities), PIPA presents a leap both in size and diversity. The heads are annotated with a bounding box and an identity tag. The individuals appear in diverse poses, point of view, activities, sceneries, and thus cover an interesting slice of the real world. See examples in [29,30], as well as Figs. 1 and 10.

One possible limitation of the dataset, is that only repeating identities have been annotated (i.e. a subset of all persons appearing in the images). However, with a test set covering ∼13k instances over ∼600 identities (∼20 instances/identity), it still presents a large enough set of identities to enable an interesting study and derive relevant conclusions. We believe PIPA is currently the best public dataset for studying questions regarding privacy in social media photos.

Albums. From the Flickr website, each photo is associated with an album identifier. The ∼13k test instances are grouped in ∼8k photos belonging to ∼350 albums. We use the photo album information indirectly during our graph inference (Sect. 5.3).

Protocol. The PIPA dataset defines train, validation, and test partitions (∼17k, ∼5k, ∼8k photos respectively), each containing disjoint sets of identities [29]. The train partition is used for convnet training. The validation data is used for component-wise evaluation of our system, and the test set for drawing final conclusions. The validation and test partitions are further divided into split_0 and split_1. Each $\text{split}_{0/1}$ contains half of the instances for each identity in the validation and test sets (∼10 instances/identity per split, on average).

Splits. When instantiating the scenarios from Sect. 3, the tagged faces are all part of split_0. In S_1, S_2, and S_3, split_1 is never tagged. The task of our Faceless Person Recognition System is to recognise every query instance from split_1, possibly leveraging other non-tagged instances in split_1.

Domain Shift. Other than the one split defined in [29,30] proposed additional splits with increasing recognition difficulty. We use the "Original" split as a good proxy for the "within events" case, and the "Day" split for "across events". In the day split, split_0 and split_1 contain images of a given person across different days.

5 Faceless Recognition System

In this section, we introduce the Faceless Recognition System to study the effectiveness of privacy protective measures in Sect. 3. We choose to build our own baseline system, as opposed to using an existing system as in [47], for adaptibility of the system to obfuscation and reproducibility for future research.

Our system does joint recognition employing a conditional random field (CRF) model. CRF often used for joint recognition problems in computer vision [42,43,50,51]. It enables the communication of information across instances, strengthening weak individual cues. Our CRF model is formulated as follows:

$$\arg\max_{Y} \frac{1}{|V|}\sum_{i\in V}\phi_\theta(Y_i|X_i) + \frac{\alpha}{|E|}\sum_{(i,\,j)\in E} 1_{[Y_i=Y_j]}\psi_{\tilde{\theta}}(X_i,\,X_j) \tag{1}$$

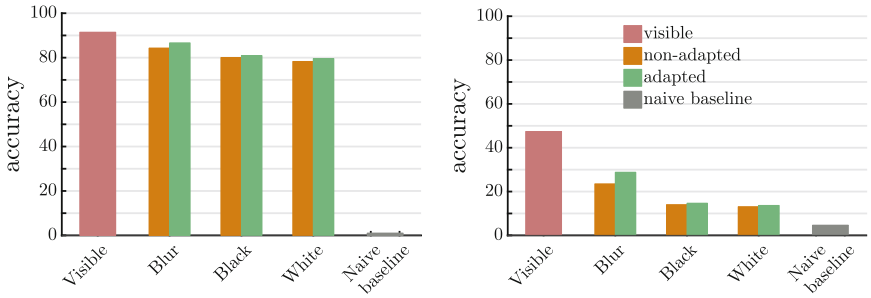
with observations X_i, identities Y_i and unary potentials $\phi_\theta(Y_i|X_i)$ defined on each node $i \in V$ (detailed in Sect. 5.1) as well as pairwise potentials $\psi_{\tilde{\theta}}(X_i,\,X_j)$ defined on each edge $(i,\,j) \in E$ (detailed in Sect. 5.2). $1_{[.]}$ is the indicator function, and $\alpha > 0$ controls the unary-pairwise balance.

Unary. We build our unary ϕ_θ upon a state of the art, publicly available person recognition system, `naeil` [30]. The system was shown to be robust to decreasing number of tagged examples. It uses not only the face but also context (e.g. body and scene) as cues. Here, we also explore its robustness to obfuscation, see Sect. 5.1.

Pairwise. By adding pairwise terms over the unaries, we expect that the system to propagate predictions across nodes (instances). When a unary prediction is weak (e.g. obfuscated head), the system aggregates information from connected nodes with possibly stronger predictions (e.g. visible face), and thus deduce the query identity. Our pairwise term $\psi_{\tilde{\theta}}$ is a siamese network build on top of the unary features, see Sect. 5.2.

Experiments on the validation set indicate that, for all scenarios, the performance improves with increasing values of α, and reaches the plateau around $\alpha = 10^2$. We use this value for all the experiments and analysis.

In the rest of the section, we provide a detailed description of the different parts and evaluate our system component-wise.



(a) Within events (b) Across events

Fig. 3. Impact of head obfuscation on our unary term. Compared to visible (unobfuscated) case, it struggles on obfuscations (blur, black, and white); nonetheless, it is still far better than the naive baseline classifier that blindly predicts the most popular class. "Adapted" means CNN models are trained for the corresponding obfuscation type. (Color figure Online)

5.1 Single Person Recognition

We build our single person recogniser (the unary potential ϕ_θ of the CRF model) upon the state of the art person recognition system `naeil` [30].

First, 17 AlexNet [52] cues are extracted and concatenated from multiple regions (head, body, and scene) defined relative to the ground truth head boxes. We then train per-identity logistic regression models on top of the resulting 4096×17 dimensional feature vector, which constitute the $\phi_\theta(\cdot|X_i)$ vector.

The AlexNet models are trained on the PIPA train set, while the logistic regression weights are trained on the tagged examples (split_0). For each obfuscation case, we also train new AlexNet models over obfuscated images (referred to as "adapted" in Fig. 3). We assume that at test time the obfuscation can be easily detected, and the appropriate model is used. We always use the "adapted" model unless otherwise stated.

Figures 3 and 4 evaluate our unary term over the PIPA validation set, under different obfuscation, within/across events, and with varying number of training tags. In the following, we discuss our main findings on how single person recognition is affected by these measures.

Adapted Models Are Effective for Blur. When comparing "adapted" to "non-adapted" in Fig. 3, we see that adaptation of the convnet models is overall positive. It makes minor differences for black or white fill-in, but provides a good boost in recognition accuracy for the blur case, especially in the across events case (5+ percent points gain).

Robustness to Obfuscation. After applying black obfuscation in the within events case, our unary performs only slightly worse (from "visible" 91.5 % to "black adapted" 80.9 %). This is 80 times better than a naive baseline classifier (1.04 %)

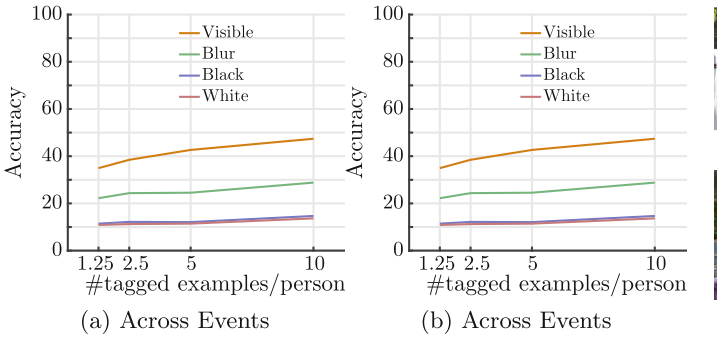


Fig. 4. Single person recogniser at different tag rates.

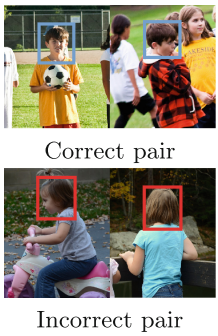


Fig. 5. Matching in social media

that blindly predicts the most popular class. In the across events case, the "visible" performance drops from 47.4 % to 14.7 %, after black obfuscation, which is still more than 3 times accurate than the naive baseline (4.65 %).

Black and White Fill-In Have Similar Effects. [47] suggests that white fill-in confuses a detection system more than does the black. In our recognition setting, black and white fill-in have similar effects: 80.9 % and 79.6 % respectively, for within events, adapted case (see Fig. 3). Thus, we omit the experiments for white fill-in obfuscation in the next sections.

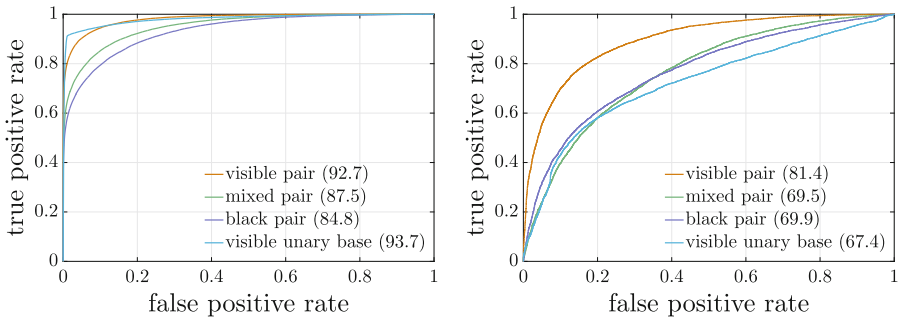
The System Is Robust to Small Number of Tags. As shown in Fig. 4 the single person recogniser is robust to a small number of identity tags. For example, in the within events, visible case, it performs at 69.9 % accuracy even at 1.25 instances/identity tag rate, while using 10 instances/identity it achieves 91.5 %.

5.2 Person Pair Matching

In this section, we introduce a method for predicting matches between a pair of persons based on head and body cues. This is the pairwise term in our CRF formulation (Eq. 1). Note that person pair matching in social media context is challenging due to clothing changes and varying poses (see Fig. 5).

We build a Siamese neural network to compute the match probability $\psi_{\tilde{\theta}}(X_i, X_j)$. A pair of instances are given as input, whose head and body features are then computed using the single person recogniser (Sect. 5.1), resulting in a $2 \times (2 \times 4096)$ dimensional feature vector. These features are passed through three fully connected layers with ReLU activations with a binary prediction at the end (match, no-match).

We first train the siamese network on the PIPA train set, and then fine-tune it over split_0, the set of tagged samples. We train three types of models: one for visible pairs, one for obfuscated pairs, and one for mixed pairs. Like for the unary



(a) Within events (b) Across events

Fig. 6. Person pair matching on the set of pairs in photo albums. The numbers in parentheses are the equal error rates (EER). The "visible unary base" refers to the baseline where only unaries are used to determine match.

term, we assume that obfuscation is detected at test time, so that the appropriate model is used. Further details can be found in the supplementary materials.

Evaluation. Figure 6 shows the matching performance. We evaluate on the set of pairs within albums (used for graph inference in Sect. 5.3). The performance is evaluated in the equal error rate (EER), the accuracy at the score threshold where false positive and false negative rates meet. The three obfuscation type models are evaluated on the corresponding obfuscation pairs.

Fine-Tuning on split$_0$ is Crucial. By fine-tuning on the tagged examples of query identities, matching performance improves significantly. For the visible pair model, EER improves from 79.1 % to 92.7 % in the within events setting, and from 74.5 % to 81.4 % in across events.

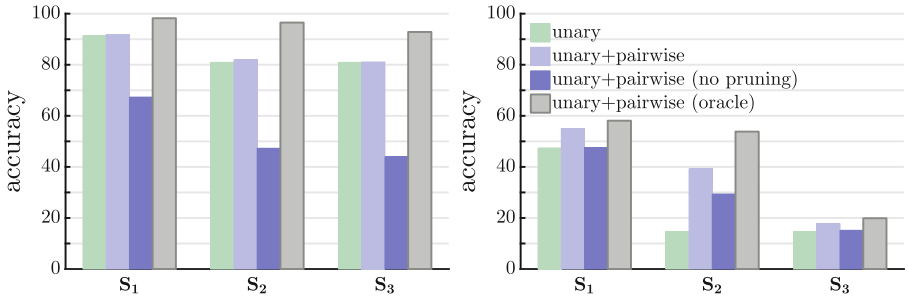
Unary Baseline. In order to evaluate whether the matching network has learned to predict match better than its initialisation model, we consider the unary baseline. See "visible unary base" in Fig. 6. It first compares the unary prediction (argmax) for a given pair, and then determines its confidence using the prediction entropies. See supplementary materials for more detail.

The unary baseline performs marginally better than the visible pair model under the within events: 93.7 % versus 92.7 %. Under the across events, on the other hand, the visible pair model beats the baseline by a large margin: 81.4 % versus 67.4 % (Fig. 6). In practice, the system has no information whether the query image is from within or across events. The system thus uses the pairwise trained model (visible pair model), which performs better on average.

General Comments. The matching network performs better under the within events setting than across events, and better for the visible pairs than for mixed or black pairs. See Fig. 6.

5.3 Graph Inference

Given the unaries from Sect. 5.1 and pairwise from Sect. 5.2, we perform a joint inference to perform more robust recognition. The graph inference is implemented via PyStruct [53]. The results of the joint inference (for the black obfuscation case) are presented in Fig. 7, and discussed in the next paragraphs.



(a) Within events (b) Across events

Fig. 7. Validation performance of the CRF joint inference in three scenarios, S_1, S_2, and S_3 (see Sect. 3), under black fill-in obfuscation. After graph pruning, joint inference provides a gain over the unary in all scenarios.

Across-Album Edge Pruning. We introduce some graph pruning strategies which make the inference tractible and more robust to noisy predictions. Some of the scenarios considered (e.g. S_2) require running inference for each instance in the test set (∼6k for within events). In order to lower down the computational cost from days to hours, we prune all edges across albums. The resulting graph only has fully connected cliques within albums. The across-album edge pruning reduces the number of edges by two orders of magnitude.

Negative Edge Pruning. As can be seen in Fig. 7, simply adding pairwise terms ("unary+pairwise (no pruning)") can hurt the unaries only performance. This happens because many pairwise terms are erroneous. This can be mitigated by only selecting confident (high quality, low recall) predictions from $\psi_{\tilde{\theta}}$. We found that selecting positive pairs $\psi_{\tilde{\theta}}(X_i, X_j) \geq 0.5$ works best (any threshold in the range [0.4, 0.7] works equally fine). These are the "unary+pairwise" results in Fig. 7, which show an improvement over the unary case, especially for the across events setting. The main gain is observed for S_2 (one obfuscated head) across events, where the pairwise term brings a jump from 15 % to 39 %.

Oracle Pairwise. To put in context the gains from the graph inference, we build an oracle case that assumes perfect pairwise potentials ($\psi_{\tilde{\theta}}(X_i, X_j) = 1_{[Y_i = Y_j]}$, where $1_{[\cdot]}$ is the indicator function and Y are the ground truth identities). We do not perform negative edge pruning here. The unaries are the same as for the other cases in Fig. 7. We can see that the "unary+pairwise" results are within

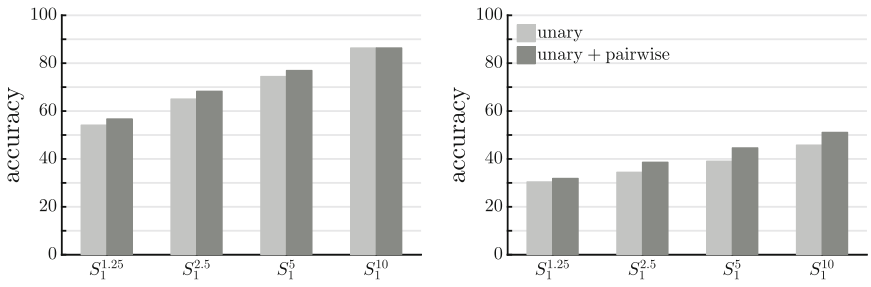
70 %+ of the oracle case "(oracle)", indicating that the pairwise potential $\psi_{\widetilde{\theta}}$ is rather strong. The cases where the oracle perform poorly (e.g. S_3 across events), indicate that stronger unaries or better graph inference is needed. Finally, even if no negative edge is pruned, adding oracle pairwise improves the performance, indicating that negative edge pruning is needed only when pairwise is imperfect.

Recognition Rates Are Far from Chance Level. After graph inference, all scenarios in the within event case reach recognition rates above 80 % (Fig. 7a). When across events, both S_1 and S_2 are above 35 % (Fig. 7b). These are recognition far above the chance level (1 %/5 % within/across events, shown in Fig. 3). Only S_3 (all user heads with black obfuscation) show a dreadful drop in recognition rate, where neither the unaries nor the pairwise terms bring much help. See supplementary materials for more details in this section.

6 Test Set Results and Analysis

Following the experimental protocol in Sect. 4, we now evaluate our Faceless Recognition System on the PIPA test set. The main results are summarised in Figs. 8 and 9. We observe the same trends as the validation set results discussed in Sect. 5. Figure 10 shows some qualitative results over the test set. We organize the results along the same privacy sensitive dimensions that we defined in Sect. 3 in order to build our study scenarios.

Amount of Tagged Heads. Figure 8 shows that even with only 1.25 tagged photos per person on average, the system can recognise users far better than chance level (naive baseline; best guess before looking at the image). Even with such little amount of training data, the system predicts 56.8 % of the instances correctly within events and 31.9 % across events; which is 73× and 16× higher than chance level, respectively. We see that even few tags provide a threat for privacy and thus users concerned with their privacy should avoid having (any of) their photos tagged.



(a) Within events (b) Across events

Fig. 8. Impact of number of tagged examples: $S_1^{1.25}$, $S_1^{2.5}$, S_1^{5}, and S_1^{10}.

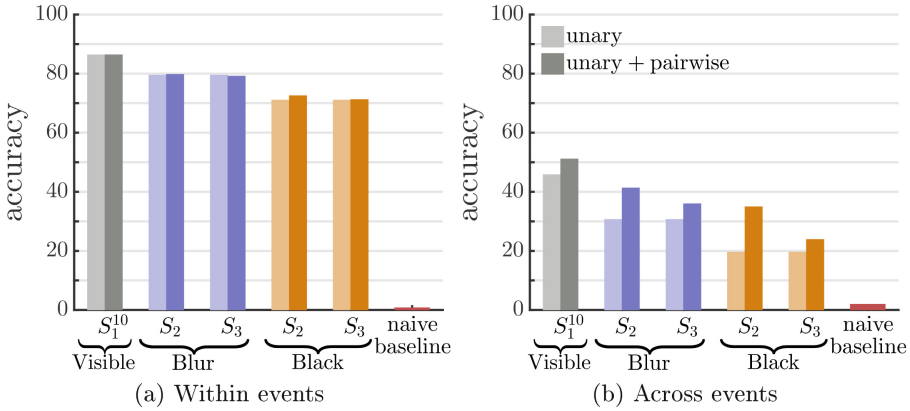


Fig. 9. Co-recognition results for scenarios S_1^{10}, S_2, and S_3 with black fill-in and Gaussian blur obfuscations (white fill-in match black results). (Color figure Online)

Fig. 10. Examples of queries in across events setting, not identified using only tagged (red boxes) samples, but successfully identified by the Faceless Recognition System via joint prediction of the query and non-tagged (white boxes) examples. A subset of both tagged and non-tagged examples are shown; there are ∼10 tagged and non-tagged examples originally. Non-tagged examples are ordered in the match score against the query (closest match on the left). (Color figure online)

Obfuscation Type. For both scenario S_2 and S_3, Fig. 9 (and the results from Sect. 5.1) indicates the same privacy protection ranking for the different obfuscation types. From higher protection to lower protection, we have Black ≈ White > Blur > Visible. Albeit blurring does provide some protection, the machine learning algorithm still extracts useful information from that region. When our full Faceless Recognition System is in use, one can see that (Fig. 9) obfuscation helps, but only to a limited degree: e.g. 86.4 % (S_1) to 71.3 % (S_3) under within events and 51.1 % (S_1) to 23.9 % (S_3) under across events.

Amount of Obfuscation. We cover three scenarios: every head fully visible (S_1), only the test head obfuscated (S_2), and every head fully obfuscated (S_3). Figure 9

shows that within events obfuscating either one (S_2) or all (S_3) heads is not very effective, compared to the across events case, where one can see larger drops for $S_1 \rightarrow S_2$ and $S_2 \rightarrow S_3$. Notice that unary performances are identical for S_2 and S_3 in all settings, but using the full system raises the recognition accuracy for S_2 (since seeing the other heads allow to rule-out identities for the obfuscated head). We conclude that within events head obfuscation has only limited effectiveness, across events only blacking out all heads seems truly effective (S_3 black).

Domain Shift. In all scenarios, the recognition accuracy is significantly worse in the across events case than within events (about $\sim$50 % drop in accuracy across all other dimensions). For a user, it is a better privacy policy to make sure no tagged heads exist for the same event, than blacking out all his heads in the event.

7 Discussion and Conclusion

Within the limitation of any study based on public data, we believe the results presented here are a fresh view on the capabilities of machine learning to enable person recognition in social media under adversarial condition. From a privacy perspective, the results presented here should raise concern. We show that, when using state of the art techniques, blurring a head has limited effect. We also show that only a handful of tagged heads are enough to enable recognition, even across different events (different day, clothes, poses, point of view). In the most aggressive scenario considered (all user heads blacked-out, tagged images from a different event), the recognition accuracy of our system is 12$\times$ higher than chance level. It is very probable that undisclosed systems similar to the ones described here already operate online. We believe it is the responsibility of the computer vision community to quantify, and disseminate the privacy implications of the images users share online. This work is a first step in this direction. We conclude by discussing some future challenges and directions on privacy implications of social visual media.

Lower Bound on Privacy Threat. The current results focused singularly on the photo content itself and therefore a lower bound of the privacy implication of posting such photos. It remains as future work to explore an integrated system that will also exploit the images' meta-data (timestamp, geolocation, camera identifier, related user comments, etc.). In the context of the era of "selfie" photos, meta-data can be as effective as head tags. Younger users also tend to cross-post across multiple social media, and make a larger use of video (e.g. Vine). Using these data-form will require developing new techniques.

Training and Test Data Bounds. The performance of recent techniques of feature learning and inference are strongly coupled with the amount of available training data. Person recognition systems like [20,26,27] all rely on undisclosed training data in the order of millions of training samples. Similarly, the evaluation of privacy issues in social networks requires access to sensitive data, which

is often not available to the public research community (for good reasons [1]). The used PIPA dataset [29] serves as good proxy, but has its limitations. It is an emerging challenge to keep representative data in the public domain in order to model privacy implications of social media and keep up with the rapidly evolving technology that is enabled by such sources.

From Analysing to Enabling. In this work, we focus on the analysis aspect of person recognition in social media. In the future, one would like to translate such analyses to actionable systems that enable users to control their privacy while still enabling communication via visual media exchanges.

Acknowledgements. This research was supported by the German Research Foundation (DFG CRC 1223).

References

1. Narayanan, A., Shmatikov, V.: Myths and fallacies of personally identifiable information. Commun. ACM **53**(6), 24–26 (2010)
2. Narayanan, A., Shmatikov, V.: De-anonymizing social networks. In: IEEE Symposium on Security and Privacy (2009)
3. Zheleva, E., Getoor, L.: To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In: International Conference on World Wide Web (2009)
4. Mislove, A., Viswanath, B., Gummadi, K.P., Druschel, P.: You are who you know: inferring user profiles in online social networks. In: International Conference on Web Search and Data Mining (2010)
5. Ahern, S., Eckles, D., Good, N.S., King, S., Naaman, M., Nair, R.: Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (2007)
6. Besmer, A., Richter Lipford, H.: Moving beyond untagging: photo privacy in a tagged world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1563–1572. ACM (2010)
7. Kee, E., Johnson, M.K., Farid, H.: Digital image authentication from JPEG headers. Trans. Inf. Forensics Secur. **6**(3), 1066–1075 (2011)
8. Dirik, A.E., Sencar, H.T., Memon, N.: Digital single lens reflex camera identification from traces of sensor dust. Trans. Inf. Forensics Secur. **3**, 539–552 (2008)
9. Chen, M., Fridrich, J., Goljan, M., Lukáš, J.: Determining image origin and integrity using sensor noise. Trans. Inf. Forensics Secur. **3**, 74–90 (2008)
10. Huang, G.B., Ramesh, M., Berg, T., Learned-Miller, E.: Labeled faces in the wild: a database for studying face recognition in unconstrained environments. Technical report, UMass (2007)
11. Benfold, B., Reid, I.: Guiding visual surveillance by tracking human attention. In: BMVC (2009)
12. Bedagkar-Gala, A., Shah, S.K.: A survey of approaches and trends in person re-identification. Image Vis. Comput. **32**, 270–286 (2014)
13. Guillaumin, M., Verbeek, J., Schmid, C.: Is that you? Metric learning approaches for face identification. In: ICCV (2009)

14. Chen, D., Cao, X., Wen, F., Sun, J.: Blessing of dimensionality: high-dimensional feature and its efficient compression for face verification. In: CVPR (2013)
15. Cao, X., Wipf, D., Wen, F., Duan, G.: A practical transfer learning algorithm for face verification. In: ICCV (2013)
16. Lu, C., Tang, X.: Surpassing human-level face verification performance on lfw with gaussianface. arXiv (2014)
17. Li, W., Wang, X.: Locally aligned feature transforms across views. In: CVPR (2013)
18. Zhao, R., Ouyang, W., Wang, X.: Person re-identification by salience matching. In: ICCV (2013)
19. Bak, S., Kumar, R., Bremond, F.: Brownian descriptor: a rich meta-feature for appearance matching. In: WACV (2014)
20. Taigman, Y., Yang, M., Ranzato, M., Wolf, L.: Deepface: closing the gap to human-level performance in face verification. In: CVPR (2014)
21. Li, W., Zhao, R., Xiao, T., Wang, X.: DeepReID: deep filter pairing neural network for person re-identification. In: CVPR (2014)
22. Yi, D., Lei, Z., Li, S.Z.: Deep metric learning for practical person re-identification. In: ICPR (2014)
23. Hu, Y., Yi, D., Liao, S., Lei, Z., Li, S.Z.: Cross dataset person re-identification. In: Shan, S., Jawahar, C.V., Jawahar, C.V. (eds.) ACCV 2014 Workshops. LNCS, vol. 9010, pp. 650–664. Springer, Heidelberg (2015)
24. Zhou, E., Cao, Z., Yin, Q.: Naive-deep face recognition: touching the limit of lfw benchmark or not? arXiv (2015)
25. Parkhi, O.M., Vedaldi, A., Zisserman, A.: Deep face recognition. BMVC **1**(3), 6 (2015)
26. Schroff, F., Kalenichenko, D., Philbin, J.: Facenet: a unified embedding for face recognition and clustering. In: CVPR (2015)
27. Sun, Y., Wang, X., Tang, X.: Deeply learned face representations are sparse, selective, and robust. In: CVPR (2015)
28. Gallagher, A., Chen, T.: Clothing cosegmentation for recognizing people. In: CVPR (2008)
29. Zhang, N., Paluri, M., Taigman, Y., Fergus, R., Bourdev, L.: Beyond frontal faces: improving person recognition using multiple cues. In: CVPR (2015)
30. Oh, S.J., Benenson, R., Fritz, M., Schiele, B.: Person recognition in personal photo collections. In: ICCV (2015)
31. Gong, S., Cristani, M., Yan, S., Loy, C.C. (eds.): Person Re-identification. Springer, Heidelberg (2014)
32. Wu, L., Shen, C., van den Hengel, A.: Personnet: person re-identification with deep convolutional neural networks. In: arXiv (2016)
33. Cui, J., Wen, F., Xiao, R., Tian, Y., Tang, X.: Easyalbum: an interactive photo annotation system based on face clustering and re-ranking. In: SIGCHI (2007)
34. Mathialagan, C.S., Gallagher, A.C., Batra, D.: VIP: finding important people in images. In: CVPR (2015)
35. Everingham, M., Sivic, J., Zisserman, A.: Hello! My name is... buffy-automatic naming of characters in TV video. In: BMVC (2006)
36. Everingham, M., Sivic, J., Zisserman, A.: Taking the bite out of automated naming of characters in TV video. IVC **27**, 545–559 (2009)
37. Ding, C., Tao, D.: A comprehensive survey on pose-invariant face recognition. In: arXiv (2015)
38. Cheng, D.S., Cristani, M., Stoppa, M., Bazzani, L., Murino, V.: Custom pictorial structures for re-identification. In: BMVC (2011)

39. Gandhi, V., Ronfard, R.: Detecting and naming actors in movies using generative appearance models. In: CVPR (2013)
40. Kumar, N., Berg, A.C., Belhumeur, P.N., Nayar, S.K.: Attribute and simile classifiers for face verification. In: CVPR (2009)
41. Layne, R., Hospedales, T.M., Gong, S., Mary, Q.: Person re-identification by attributes. In: BMVC (2012)
42. Gallagher, A.C., Chen, T.: Using group prior to identify people in consumer images. In: CVPR (2007)
43. Stone, Z., Zickler, T., Darrell, T.: Autotagging facebook: social network context improves photo annotation. In: CVPR Workshops (2008)
44. Garg, R., Seitz, S.M., Ramanan, D., Snavely, N.: Where's waldo: matching people in images of crowds. In: CVPR (2011)
45. Lin, D., Kapoor, A., Hua, G., Baker, S.: Joint people, event, and location recognition in personal photo collections using cross-domain context. In: Daniilidis, K., Maragos, P., Paragios, N. (eds.) ECCV 2010, Part I. LNCS, vol. 6311, pp. 243–256. Springer, Heidelberg (2010)
46. Shi, J., Liao, R., Jia, J.: Codel: a human co-detection and labeling framework. In: ICCV (2013)
47. Wilber, M.J., Shmatikov, V., Belongie, S.J.: Can we still avoid automatic face detection? arXiv (2016)
48. Gopalan, R., Taheri, S., Turaga, P., Chellappa, R.: A blur-robust descriptor with applications to face recognition. PAMI **34**, 1220–1226 (2012)
49. Punnappurath, A., Rajagopalan, A.N., Taheri, S., Chellappa, R., Seetharaman, G.: Face recognition across non-uniform motion blur, illumination, and pose. IEEE Trans. Image Process. **24**, 2067–2082 (2015)
50. Vu, T., Osokin, A., Laptev, I.: Context-aware CNNs for person head detection. In: International Conference on Computer Vision (ICCV) (2015)
51. Hayder, Z., He, X., Salzmann, M.: Structural kernel learning for large scale multiclass object co-detection. In: 2015 IEEE International Conference on Computer Vision (ICCV), pp. 2632–2640. IEEE (2015)
52. Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. In: NIPS (2012)
53. Müller, A.C., Behnke, S.: PyStruct – learning structured prediction in python. J. Mach. Learn. Res. **15**, 2055–2060 (2014)