Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos

YIFANG LI, Clemson University, USA
NISHANT VISHWAMITRA, Clemson University, USA
BART P. KNIJNENBURG, Clemson University, USA
HONGXIN HU, Clemson University, USA
KELLY CAINE, Clemson University, USA

Current collaborative photo privacy protection solutions can be categorized into two approaches: controlling the recipient, which restricts certain viewers' access to the photo, and controlling the content, which protects all or part of the photo from being viewed. Focusing on the latter approach, we introduce privacy-enhancing obfuscations for photos and conduct an online experiment with 271 participants to evaluate their effectiveness against human recognition and how they affect the viewing experience. Results indicate the two most common obfuscations, *blurring* and *pixelating*, are ineffective. On the other hand, *inpainting*, which removes an object or person entirely, and *avatar*, which replaces content with a graphical representation are effective. From a viewer experience perspective, *blurring*, *pixelating*, *inpainting*, and *avatar* are preferable. Based on these results, we suggest *inpainting* and *avatar* may be useful as privacy-enhancing technologies for photos, because they are both effective at increasing privacy for elements of a photo and provide a good viewer experience.

CCS Concepts: • **Security and privacy → Privacy protections**; **Usability in security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**; *Collaborative and social computing*;

Additional Key Words and Phrases: Privacy, security, Online Social Network, image obfuscation, image redaction, user experience

ACM Reference Format:
Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos. *Proc. ACM Hum.-Comput. Interact.* 1, 2, Article 67 (November 2017), 24 pages. https://doi.org/10.1145/3134702

1 INTRODUCTION

Preserving privacy is a critical task in online environments [82]. Revealing personal information may lead to identification, inference attacks, sensitive information leakage, location leakage, and cross-profiling [27]. However, privacy is often hard to achieve due to the unpredictability of the online context [53] and the lack of usable tools [23]. Descriptive investigations of privacy-enhancing

This work is supported by the National Science Foundation, under grant IIS-1527421.
Authors' addresses: Yifang Li, Clemson University, School of Computing, Clemson, SC, 29634, USA; Nishant Vishwamitra, Clemson University, School of Computing, Clemson, SC, 29634, USA; Bart P. Knijnenburg, Clemson University, School of Computing, Clemson, SC, 29634, USA; Hongxin Hu, Clemson University, School of Computing, Clemson, SC, 29634, USA; Kelly Caine, Clemson University, School of Computing, Clemson, SC, 29634, USA.

2573-0142/2017/11-ART67 $15.00
https://doi.org/10.1145/3134702

behaviors both online and offline identify two approaches to protecting privacy: controlling recipients and controlling information content [16]. In the context of online photo privacy protection, the approach of controlling recipients has been studied extensively [7, 34, 74]. This approach provides some privacy protection, but has a number of drawbacks. Of particular importance to the CSCW community, controlling the recipient is insufficient to enable multi-party privacy conflicts [7, 20, 76].

The goal of this work is to investigate controlling content instead of recipient as a means to protect users' privacy. We chose the context of photo privacy in OSNs as an exemplar setting where there is a tension between sharing and privacy [7]. While some prior work has investigated methods to hide elements of photos to be shared online, it has been limited to a few approaches, most notably blurring and pixelating [35, 78], which are ineffective at preventing human and machine identification [46, 55].

Recognizing the need for more effective photo privacy-enhancing obfuscations, we identified silhouette [60], box masking [85], avatar [65], point-light [17], bar [85], and inpainting [60, 85]. Moreover, recognizing that the audience for online photos is human beings, we investigated human (vs. machine) perception of these options (in terms of photo satisfaction, perceived photo information sufficiency, photo enjoyment, social presence, obfuscation likability and preference), as well as their ability to identify content in the photos. To our knowledge, there is no existing research that addresses both effectiveness against human recognition and users' perceptions of obfuscations as privacy-enhancing tools.

Our results show that even though people are generally satisfied with *blurring* and *pixelating*—the two most investigated and widely-adopted obfuscation methods—these methods do not enhance privacy. When developing collaborative privacy management systems, researchers should consider alternative privacy-enhancing obfuscations, such as *inpainting* and *avatar*, which are both effective and likable. Though our findings focus on face and body, they can be further applied to other PII, such as object and location.

2 BACKGROUND AND RELATED WORK

2.1 A Simplified Privacy Framework: Recipient and Content

While a review of the extensive and growing literature on privacy in HCI and CSCW is outside of the scope of this paper, we do want to situate our work in the larger theoretical work on privacy that is particularly relevant to our approach.

Contextual integrity suggests that we achieve privacy if the flow of information follows the context-relative informational norm, which includes several key parameters such as subject, sender, recipient, type of information, and transmission principles while acknowledging that in digital media and online environments the context becomes more complicated and unpredictable [57]. For example, the recipients or the goal of the information content may change outside the awareness of the user [58]. The networked privacy model extends contextual integrity by emphasizing that by passing information through the network, one user's privacy can be violated by any other users who connect to this user [53]. The complexity of the network determines that the widely adopted access-control list scheme on OSNs may not be effective [53].

Separately, but in line with these and prior approaches [3, 57, 81], others have identified two fundamental elements at play in privacy: information type and recipient [16]. In the online photo sharing domain, recipient is the viewer of a photo and information type can be interpreted as photo content or elements. In this study, we adopt this simplified framework for privacy [16], and organize the remainder of our review of related work around these elements (recipient and content).

2.2 Controlling Recipient

A primary strategy for protecting users' privacy is controlling the recipient [7, 79]. For example, the "Restrict Others" tool allows each stakeholder depicted in a photo on Facebook to negotiate with the uploader to hide the photo from certain viewers [7]. However, this solution may cause social tension between the uploader and other stakeholders [7], and the final decision of sharing a photo is still in the hands of the uploader. Moreover, privacy conflicts often occur among multiple users, further complicating the privacy negotiation [20, 76].

Some collaborative access control schemes for OSNs have been developed to address potential conflicts. One approach is to consider stakeholder preferences to determine which photos are shared [74]. However, only the friends at the intersection of the privacy preferences of all stakeholders have access to the photo, resulting in large sharing losses when any of the stakeholders desires privacy. Some of these losses may be avoided by using a conflict resolution mechanism that asks users to manually input a trust level for the audience with potential access to the photo, the sensitivity level of the photo, and their privacy preferences. Based on the preference of each stakeholder, the system can determine who should and should not get access to the photo [34]. Although these systems solve some privacy conflicts, they do not effectively address the privacy preferences of all the stakeholders, especially when the stakeholders have conflicting preferences. Furthermore, they may not address interactional privacy and relational needs [51].

2.3 Controlling Content

An alternative strategy for protecting users' privacy is through controlling information content. For example, since most YouTube videos are public by default, it is hard to regulate the information recipients. Instead, YouTube uses a blurring obfuscation to hide faces and objects in certain videos [10]. Similarly, life-logging devices may reveal excessive details about wearers and bystanders. Thus, researchers have employed automatic screen detection to hide any information presented on screens that are visible in photos or videos taken by life-logging devices [38]. In the home environment two privacy-preserving mechanisms (blob tracker and point-light) have been used to protect elements of users' identities [17]. Google Street View blurs faces and license plates in an attempt to avoid identification [29]. After the fact, users may delete content [2] or, a platform may "default to ephemerality" by deleting content automatically [83]. To protect OSNs photo privacy, Face/off system enables blurring person's face in a group photo [35], rather than recipient.

Various potentially sensitive photo elements influence users' sharing decisions, including the people in the photo, the background setting, visible objects, and visible private information [33] which can be summarized as three photo content variables that affect privacy concerns: the subject's identity, the environment in the photo, and the activity the subject is performing [17]. Hiding or changing one or a combination of these variables may offset privacy concerns. For example, imagine that Bob's friend uploads a group photo to Facebook that depicts several people drinking in a bar, including Bob. Bob may worry that his colleagues will see the photo, because the uploader and Bob have mutual friends. Bob's concerns can be reduced by hiding his identity (e.g., by obscuring his face and body), changing the activity (e.g., switching his beer can to a Coke can), and/or changing the environment (e.g., from a bar to a home party). In this work, we focus on the first variable: hiding the identity of a person in a photo.

Ideally, on OSNs, controlling recipient and controlling content can be combined to provide better collaborative photo privacy management. Indeed, some prior work has investigated controlling both the recipient and the content (e.g., for protecting the privacy of crowd-workers [18], in the health domain [15]), and specifically in photo sharing [35]. In the work on photo sharing, participants were given the ability hide their identity from certain recipients of the photo by blurring their face. The evaluation showed that users were not able to recognize their friends in 82.7% of the blurred photos. However, this approach has limitations, for example, comparing to hiding the entire body, only protecting the user's face is less effective [19].

Blurring is the most commonly used obfuscation to control information content disclosure both in research and in practice [6, 35]. However, blurring may not provide sufficient privacy protection [11]. In video surveillance, blurring is less effective than solid masking in terms of preventing people from recognizing the obscured individual [40, 50]. In addition to human recognition, blurring is also susceptible to reversal by machine identification; researchers have used generative adversarial networks to refine image details [46], trained artificial neural networks to perform re-identification [55], and automated "faceless recognition" using clothes and/or pose [59].

Redaction tools from video surveillance can be applied to privacy-preserving online photo sharing, since both of these applications attempt to protect a subject's identity by hiding the subject's visual information. However, most of these focus on the effectiveness of these redaction tools against automatic recognition software. To the best of our knowledge, none of these tools have been used to enhance privacy for photos shared via OSNs. In particular, we have seen no work that investigates their effectiveness against human re-identification, especially in relation to users' attitudes towards these tools.

3 METHOD

3.1 Overview

We conducted an experiment with 271 participants to understand how type of obfuscation and region the obfuscation is applied to influenced effectiveness and users' perceptions (satisfaction, perceived information sufficiency, photo enjoyment, social presence, and likability).

3.2 Participants

Three hundred and forty seven participants from United States were recruited via the Amazon Mechanical Turk. While imperfect, it is considered one of the better sampling strategies because Turkers are relatively more diverse than the samples collected by other means (e.g., U.S. college samples) [12]. We paid participants $1.50 to complete the study [66]. To ensure the data quality, we set restrictions to only include MTurk workers with high reputation (above 95% approval ratings), and with the number of HIT approved being greater than 1000 [62]. Excluding the data of participants who failed more than one attention check questions, the final sample size is 271 (131 men and 140 women). Fifty-seven participants were from the Midwest region; 99 were from the South; 66 were from the West, and 49 were from the Northeast [14] . Forty-three percent ranged in age from 25 to 34; twenty percent ranged from 35 to 44; and forty-eight percent is was from 45 to 54. Seventy-six percent was White. Ninety-eight percent of participants used Internet most of the day or several times a day; and 72% visited OSNs most of the day or several times a day.

3.3 Experimental Design

We used a 8 (privacy-enhancing obfuscation) by 2 (body region) experimental design. The eight obfuscation methods were: *blurring*, *pixelating*, *silhouette*, *avatar*, *point-light*, *masking*, *bar*, and *inpainting*. The two regions were face and body. Please see below sections for descriptions of why we chose them.

3.3.1 Regions. Different elements in an image can be considered sensitive: for example, people, personal belongings, affiliation, and privacy information [33, 78]. For this study, we decided to study the recognizability of people for a variety of reasons, but one very compelling reason was because of prior work on human recognition of faces [8, 24, 39], machine recognition of faces [46, 55], and obfuscation of humans in video [11, 41]. We chose two regions to obfuscate: face and body (which includes the face). Masking the face is the most common strategy for hiding the identity of a person in photos or videos [10, 29, 35]. The face also has special meaning and significance in the human visual system. The perceptual process in facial recognition is different from the process in recognizing non-facial stimuli, that faces are recognized at the individual level [25]. However, prior work on video surveillance suggests that masking only the face is ineffective: obscuring the entire body is more effective than obscuring only the face [19].

3.3.2 Obfuscation Methods. We chose eight redaction tools from previous work on online photo privacy, video surveillance, and video monitoring [17, 60, 70, 85]. We did not investigate some tools that were less applicable to photo redaction. For example, "see-through (translucent) [85]" and "monotone [85]" are excluded because the semitransparent or monochrome subjects may not be identified accurately in videos where they are dynamic, while in a photo, people can easily identify a static subject. Generally, we excluded the tools that were either ineffective or overlapping. The eight redaction tools we studied are listed in Table 1.

We also tested the baseline condition of no obfuscation (*as is*). We left out three region by obfuscation combinations resulting in 14 total conditions (including *as is*; see obfuscation methods Table 1 and its caption). We did not test the following obfuscations for face: *inpainting*, *point-light* and *bar* because we anticipated these might make viewers uncomfortable. For example, *inpainting* just the face would have resulted in what appeared to be a headless person, which we anticipated might be jarring to view.

3.4 Stimuli

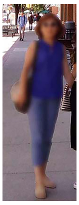
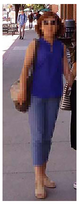
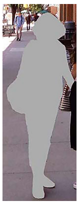
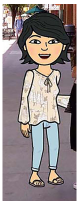
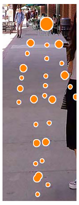
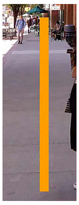
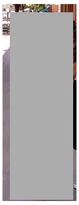
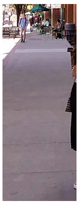
3.4.1 Targets. Target is the person in a photo who needs to be identified. We selected targets from racial categories broadly representing the racial makeup of the United States [13] including white, African American, Asian, and Hispanic and Latino, who were unknown to participants. The target photos were taken by our lab and researchers. We applied each of the 14 obfuscations to all targets with 2 different backgrounds resulting in 392 unique images.

3.4.2 Backgrounds. We selected the backgrounds and background people photos online which had licenses that allowed for reuse and modify, and photos taken by our lab and researchers, cut them out, and reassembled them to include the target person (Figure 1). Each photo has the same number of background people (three people) and similar background (campus building etc.).

3.4.3 Photo Creation. We used Photoshop to create photos so they would be consistent, except for elements we intentionally varied (e.g., target or obfuscation). Each photo consists of the target with an obfuscation applied, three non-target people, and a background (Figure 1). To generate a complete set of experimental stimuli, we created an image of each target/obfuscation pair and overlaid these on each background. The experiment platform randomly selected the combination of target, obfuscation condition and background. In total, the stimuli set has 392 unique photos (14 targets * 14 obfuscations * 2 backgrounds).

3.4.4 ID Photo. For each target we collected one ID photo (e.g., the second person from the left in Figure 1), and three ID photos of similar looking people. A similar looking person might be the same gender, have a similar hair style, skin color, body shape and/or height (see the right two people in Figure 1).

Table 1. Eight obfuscation methods. In the example figures, we applied the methods on body. They were also applied on face in the study, yielding in 14 conditions (We added *as is* as baseline condition, and excluded 3 combinations: face x pointlight, face x bar, face x inpainting.).

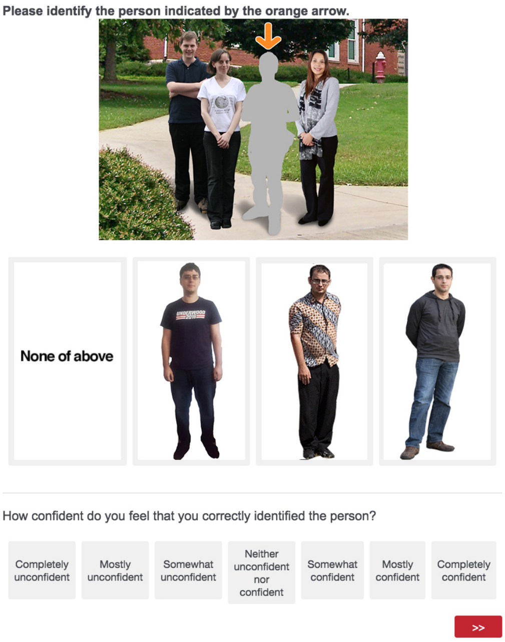
Example	Name & Definition	Related Work	Example	Name & Definition	Related Work
	**Blurring.** Reduces image detail by generating a weighted average of each pixel and its surrounding pixels.	[6, 10, 29, 41, 45]		**Pixelating.** Replaces original small pixels, which are single-colored square display elements that compose the bitmap, with larger pixels.	[24, 39, 40, 45, 80]
	**Silhouette.** Replaces content with a monochrome visual object that mirrors the extracted shape of the original content.	[17, 41, 60, 85]		**Avatar.** Replaces content with a graphical representation that preserves some elements of the underlying content. A human avatar can preserve facial expression and gesture, but hide biometrically unique elements (e.g., face) of identity.	[60, 65, 70]
	**Point-light.** Replaces content with dots that preserves some elements of the underlying content. A human point-light can preserve a person's activity, but hide many biometrically unique elements.	[17]		**Bar.** Replaces content with a monochrome visual object that is the shape of a small, thin rectangle.	[85]
	**Masking.** Replaces content with a monochrome solid box that covers the content to be protected and surrounding image content.	[40, 41, 85]		**Inpainting.** Completely removes content fills in the missing part of the image in a visually consistent manner.	[41, 60, 73, 85]

3.5 Measurements

We measured obfuscation effectiveness using identification success and confidence, and users' experience via existing, psychometrically validated Likert scales.

3.5.1 *Obfuscation effectiveness.*

- **Identification Success.** We measured identification success by asking "Please identify the person indicated by the orange arrow." Four answer choices included three ID photos and "None of above."



Please identify the person indicated by the orange arrow.

How confident do you feel that you correctly identified the person?

Fig. 1. Experiment interface with one stimuli and ID photo examples

- **Identification Confidence.** After each identification, we measured confidence using the question "How confident do you feel that you correctly identified the person?" Participants rated their response on a scale from 1 'Completely unconfident' to 7 'Completely confident,' where the higher score meant more confident [63].

3.5.2 Users' experience. Next, we measured the following four aspects of the privacy-enhancing obfuscation in the photo. All the responses used 7-point Likert scale from 1 'Strongly disagree' to 7 'Strongly agree.' For participants' ease of use, we adapted all scales to 7-point. Additionally, 7-point scales are more suitable for electronic distribution [26] and the data collected is more accurate than other point scales [36].

- **Photo Satisfaction.** We measured perceived photo satisfaction using the item "The photo is satisfying" derived from the image appeal scale [22].
- **Perceived Photo Information Sufficiency.** We selected a single item "The photo provides sufficient information" from the photo information quality scale to measure the perceived information sufficiency [68].
- **Photo Enjoyment.** We measured perceived photo enjoyment using the single-item photo enjoyment scale [64].
- **Perceived Social Presence.** We measured perceived social presence using the item "There was a sense of human contact when I saw the photo" from perceived social presence scale [44].
- **Obfuscation Likability.** We measured likability of each obfuscation using the item "I like the ____________ obfuscation" which was derived from the interface preference scale [56].
- **Obfuscation Preference.** We asked participants' preference for each obfuscation with the question "If you could use any of the obfuscations for photos you post on online social

networks, which one, if any, would you like to use?" We followed up this question by asking an open-ended question about the reason, and queried participants' willingness to use the obfuscation they selected. We also asked participants, "Have you ever declined to upload a photo to an online social network for privacy reasons?" If yes, they additionally answered which obfuscation they might use in such a scenario, and their reasons.

Note that we also captured the time participants spent on each question so that we could exclude participants who used automatic survey response software.

3.6 Procedure

Prior to the study, we conducted three pilot tests to check for bugs, gather data about the length of the study and ensure that the data collection worked well.

In the actual testing, first, participants accessed the experiment website (Qualtrics) via the publically distributed link through MTurk. After consenting, they answered six demographic questions and two social network familiarity questions. Next, they tested the browser and monitor size and followed resizing instructions to make sure they all viewed stimuli in a similar visual environment. Afterwards, they saw 14 obfuscation conditions examples with the descriptions as an overview.

Next, we trained participants about the tasks. During training, participants learned about the tasks they would perform, and completed two training trials. Participants then completed 14 trials where they saw photos with semi-randomly assigned obfuscation conditions and targets, and identified the target person. Participants saw all 14 conditions and 14 targets. There were no repeating conditions or targets. For example, in the first trial, if the photo includes condition 1-target 3, photos including condition 1 and target 3 will be excluded in future trials. Note that in most cases, the target was among the four choices offered, but there was around 21% chance that the target was NOT present. Afterwards, they rated their confidence, and rated the four statements about their feeling.

After finishing all trials, participants were shown 14 conditions individually, and rated their preference towards each condition. Then they answered a set of obfuscation preference questions. After all tasks, a random code was generated. Participants copied this code to MTurk to receive remuneration.

4 RESULTS

The experiment was completed by 347 participants. We excluded the data of 76 participants who either failed more than one attention check questions, or answered some questions instantly (reaction time = 0), indicating the potential use of automatic responding software [62]. The final sample size is 271, which provides sufficient power for the statistical tests we planned (i.e., 271 is more than the required 225 suggested by our a priori power analysis to achieve a power of 0.85).

4.1 Obfuscation Effectiveness

The primary measures of obfuscation effectiveness are identification success and identification confidence. Identification success is the percentage of trials in which a participant correctly identified a target. If we were to recast this as obfuscation success, or the percentage of trials in which a participant was unable to correctly identify a target, we would subtract the identification success percentage from 100%. For example, if a participant achieved a 60% identification rate, the corresponding obfuscation rate would be 40%. Identification confidence is a self-reported rating of how confident the participant was that their identification was correct.

Table 2. Identification success rate, odds ratio, 95% confidence interval, and p-value by region and obfuscation for all cases where the *as is* is the baseline. The obfuscations are ordered by identification success of body region from lowest (most effective) to highest (least effective).

		% of success	**Odds ratio**	**95% CI**	**p-value**
Face	Masking	41%	0.20	[0.14, 0.29]	<.001***
	Silhouette	45%	0.23	[0.16, 0.34]	<.001***
	Avatar	47%	0.26	[0.18, 0.37]	<.001***
	Blurring	64%	0.52	[0.36, 0.76]	.05*
	Pixelating	72%	0.73	[0.50,1.08]	.97
Body	Inpainting	19%	0.07	[0.05, 0.10]	<.001***
	Masking	20%	0.07	[0.05, 0.11]	<.001***
	Bar	27%	0.11	[0.07, 0.16]	<.001***
	Point-light	28%	0.12	[0.08, 0.17]	<.001***
	Avatar	33%	0.14	[0.10, 0.21]	<.001***
	Silhouette	40%	0.20	[0.13, 0.28]	<.001***
	Blurring	67%	0.59	[0.41, 0.87]	.33
	Pixelating	67%	0.58	[0.40, 0.86]	.27
As is (Baseline)		77%	NA	NA	NA

4.1.1 Identification Success. We analyzed the identification results using signal detection [72]: *hit* (the target is present, and the response is correct), *miss* (the target is present, but the response is incorrect, such as selecting the wrong person, or "None of above"), *correct rejection* (the target is absent, and the response is "None of above"), and *false alarm* (the target is absent, but participants do not select "None of above"). Using this approach, we can classify identification success using three categories: among all cases, among trials where the target is present, and among trials where the target is absent. In next paragraph, we focus on identification success among all cases, as shown in Table 2 .

As expected, the identification success of *as is* is the highest across categories (*all cases* (77%), *target present* (80%), and *target absent* (70%)). A Tukey post-hoc test based on a logistic mixed-effects model of *all cases* shows that the identification success of *as is* (77%) is higher than all obfuscations (all $p < .05$) except for *body blurring* (67%), *body pixelating* (67%), and *face pixelating* (72%). In addition, the identification success of *blurring* (face: 64%; body: 67%) and *pixelating* (face: 72%; body: 67%) are similar to each other (all $p > .05$), and much higher than other obfuscations (all $p < .001$; see Table 2). The success percentage difference between *blurring*/*pixelating* and other obfuscations ranges between 17 and 48%, which suggests that, in addition to being stastically less effective, they are also practically less effective. The lack of a difference between *blurring* and *pixelating*, two of the most common obfuscations [29, 45], and *as is* (5-13%) on the other hand, indicates that they are ineffective protections against human recognition, regardless of whether they are applied to the face or the entire body.

4.1.2 Body vs. Face. Overall, body-obfuscations were more difficult to identify (M = 45%) than face-obscuring obfuscations (M = 54%; $p < .001$), indicating body-obscuring obfuscations are generally more effective than face-obscuring obfuscations. Looking at individual obfuscation methods, though, there was not always a difference between face and body. Face-obscuring obfuscations were about as effective as body-obfuscations for many of the less effective obfuscations including

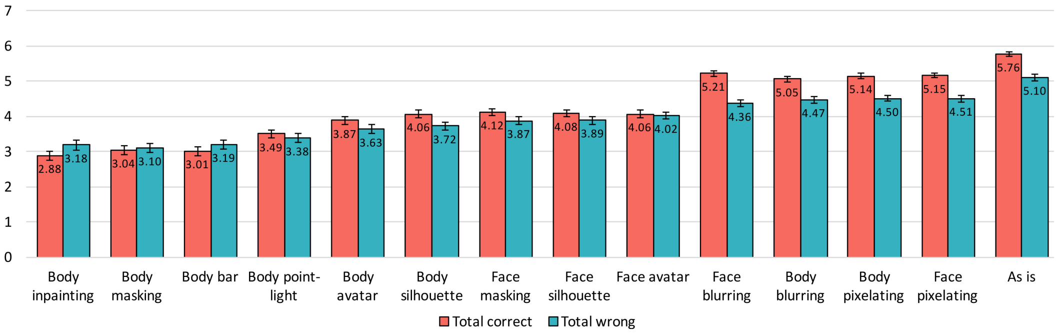


Fig. 2. Means and standard errors of identification confidence of Total Correct (Hit + Correct Rejection) and Total Wrong (Miss + False Alarm).

blurring (face: 64%; body: 67%), *pixelating* (face: 72%; body: 67%), and *silhouette* (face: 45%; body: 40%; all $p > .05$).

Obfuscations that protect more details of the target including *body avatar*, *body point-light*, *body masking*, *body bar*, and *body inpainting*, tend to be more effective. While *body inpainting* performs the best, there is no difference among these obfuscations, except between *body inpainting* (M = 19%) and *body avatar* (M = 33%, $p < .05$). It is also worth noting that for *target absent* cases, the correct rejection rate is higher either when the obfuscation transformation level is low (e.g., *as is*, *face blurring*) or when the the obfuscation shows no sign of a visible body (e.g., *body masking*, *body bar*, *body inpainting*). The reasons for these higher rates are different, though: in the former participants easily found out the target was not in three full-body ID photos, while in the latter cases there was no hint at all to identify the target, hence participants tended to choose “None of above” as a last resort.

4.1.3 Identification Confidence. Identification confidence increases as obfuscation effectiveness decreases, or, in other words, people are more confident with answers when they can correctly identify the target. In Figure 2 , for each obfuscation, the left bar represents identification confidence of *total correct* (*hit* and *correct rejection*) and the right bar represents *total wrong* (*miss* and *false alarm*).

We conducted a linear mixed effects model for *total correct* and *total wrong*, and compared obfuscation conditions using a Tukey post-hoc test. When the participant is correct, the identification confidence of *as is* is much higher than any other obfuscation methods, as expected (all $d \geq 0.36$, all $p < .001$). Notably though, confidence when viewing *blurring* and *pixelating* obfuscations—while lower than *as is*—is higher than other obfuscations, with medium to large effects (all $d \geq 0.58$, all $p < .001$). The means are above five (somewhat confident), providing further evidence that *blurring* and *pixelating* are ineffective. Moreover, identification confidence of *total correct* is higher than *total wrong* for these four methods (all $d \geq 0.41$, all $p < .05$), and larger than the differences for any of the other obfuscations, indicating that it is also easier for participants to detect when they incorrectly identified the target (see Table 3 for means and standard deviations).

Conversely, as we see in Figure 2 , mean identification of the five most effective obfuscation methods (those on the left side of Figure 2 : *body inpainting*, *body masking*, *body bar*, *body point-light*, and *body avatar*) are all below four (neither unconfident nor confident) for both *total correct* and *total wrong*, indicating that participants were not confident about their identification, regardless of whether they correctly or incorrectly identified the target.

Table 3. Identification confidence for Hit, Miss, Correct Rejection, False Alarm, Total Correct (Hit + Correct Rejection), and Total Wrong (Miss + False Alarm) on a scale from 1 - 7 where 7 is most confident. Standard deviations appear in parentheses beside the means. Within face and body categories, the order of the obfuscations is from most to least effective.

		Hit	Miss	Correct rejection	False alarm	Total correct	Total wrong
	As is	5.93 (1.08)	5.29 (1.38)	5.14 (1.52)	4.68 (1.34)	5.77 (1.23)	5.10 (1.39)
Face	Masking	4.07 (1.61)	3.89 (1.86)	4.28 (1.93)	3.74 (1.66)	4.12 (1.68)	3.87 (1.83)
	Silhouette	4.21 (1.68)	3.90 (1.84)	3.45 (1.57)	3.81 (1.62)	4.08 (1.68)	3.89 (1.79)
	Avatar	4.06 (1.73)	4.06 (1.80)	4.09 (1.95)	3.88 (1.36)	4.06 (1.76)	4.02 (1.71)
	Blurring	5.19 (1.22)	4.27 (1.55)	5.36 (0.95)	4.50 (1.56)	5.21 (1.19)	4.36 (1.55)
	Pixelating	5.18 (1.17)	4.64 (1.42)	5.03 (1.25)	4.31 (1.67)	5.15 (1.18)	4.51 (1.53)
Body	Inpainting	3.29 (1.90)	3.25 (2.24)	2.74 (2.18)	2.47 (1.78)	2.88 (2.10)	3.18 (2.21)
	Masking	3.68 (1.92)	3.08 (2.18)	2.69 (2.15)	3.25 (1.77)	3.04 (2.11)	3.10 (2.15)
	Bar	2.93 (1.64)	3.18 (2.18)	3.07 (2.29)	3.35 (2.09)	3.01 (2.06)	3.19 (2.16)
	Point-light	3.82 (1.81)	3.34 (2.05)	3.03 (2.24)	3.63 (1.86)	3.49 (2.02)	3.38 (2.03)
	Avatar	3.70 (1.79)	3.56 (1.97)	4.24 (2.20)	3.94 (1.63)	3.88 (1.94)	3.63 (1.91)
	Silhouette	4.34 (1.71)	3.73 (2.05)	3.31 (2.11)	3.71 (1.62)	4.06 (1.87)	3.72 (1.96)
	Blurring	5.09 (1.39)	4.76 (1.48)	4.84 (1.18)	4.03 (1.34)	5.05 (1.37)	4.47 (1.46)
	Pixelating	5.15 (1.39)	4.62 (1.50)	5.12 (1.20)	4.35 (1.29)	5.14 (1.36)	4.50 (1.41)

4.2 Users' Experience of Obfuscations

We analyzed users' experience of the obfuscations via five linear mixed-effect models, where the outcome variables were photo satisfaction, information sufficiency, enjoyment, social presence, and obfuscation likability, and the predictor was the obfuscation condition. We conducted Tukey post-hoc tests to compare all possible obfuscation pairs.

4.2.1 Photo Satisfaction. We now know that some obfuscation filters are more effective than others, but how do they influence users' satisfaction with the photos? From the results of our linear mixed-effects model, the overall χ^2 shows significant variation among 14 obfuscation conditions, $\chi^2(13) = 986.62$, $p < .0001$, indicating that obfuscations affected satisfaction differently. Indeed, Figure 3 shows that participants are generally less satisfied with the more effective obfuscations (see Table 2). From the Tukey post hoc test on this model, the results show that participants are most satisfied with *as is* ($M = 4.82$, $SD = 1.62$) compared to any other obfuscations (all $d \geq 0.37$, all $p < .001$. As the smallest difference, the difference between *as is* (4.82) and *face pixelating* (4.20) has an effect size of $d = 0.37$; while other effect sizes are all above 0.5, which represent medium or large effects). Participants are also satisfied with *face pixelating*, *face blurring*, *body pixlating*, and *body blurring*, but as mentioned before, these methods are not particularly effective.

Among the more effective obfuscations, participants are most satisfied with *face avatar*(1) ($M = 3.49$, $SD = 1.71$) and *body avatar*(2) ($M = 3.43$, $SD = 1.76$) with both scores higher than *body masking* ($M = 2.44$, $SD = 1.51$, $d_1 = 0.59$, $p_1 < .001$, $d_2 = 0.56$, $p_2 < .001$), *body bar* ($M = 2.59$, $SD = 1.55$, $d_1 = 0.54$, $p_1 < .001$, $d_2 = 0.48$, $p_2 < .001$), *body point-light* ($M = 2.77$, $SD = 1.54$, $d_1 = 0.44$, $p_1 < .001$, $d_2 = 0.41$, $p_2 < .001$), and *body silhouette* ($M = 2.86$, $SD = 1.49$, $d_1 = 0.39$, $p_1 < .001$, $d_2 = 0.36$, $p_2 < .001$). Moreover, the most effective obfuscation among all 14 conditions, *body inpainting* ($M = 3.10$, $SD = 1.73$), scores are higher than *body masking* ($d = 0.39$, $p < .001$) and *body bar* ($d = 0.32$, $p < .001$), and is also slightly (but not significantly) more satisfying than *body point-light*, *body silhouette*, and *face silhouette*.

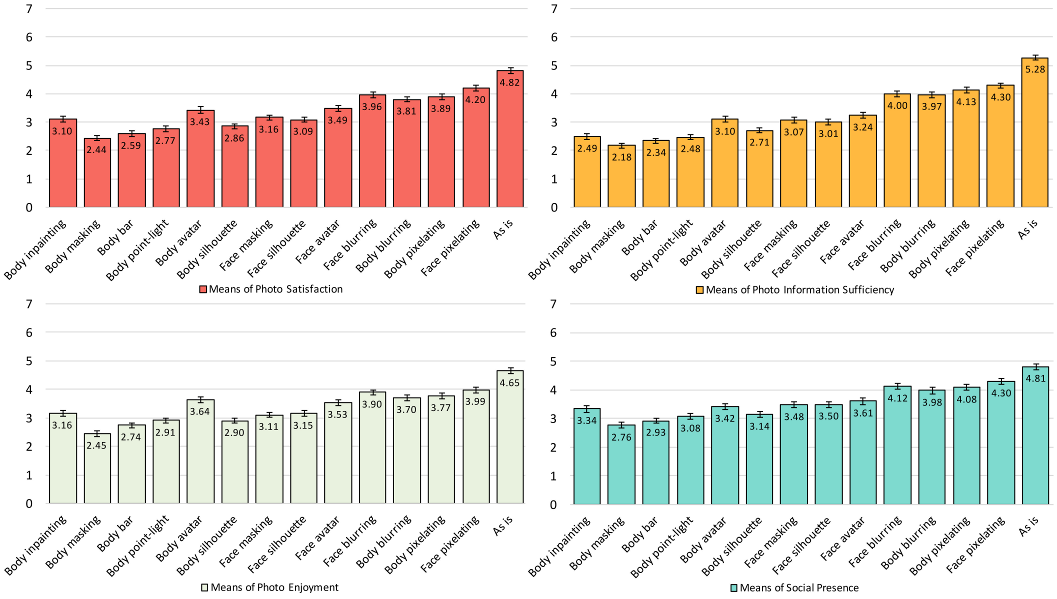


Fig. 3. Photo satisfaction, information sufficiency, enjoyment, and social presence (*M* and *SE*). Obfuscations ordered from most to least effective.

4.2.2 Photo Information Sufficiency. Do users believe that obscured photos still provide sufficient information? It seems that this also depends on the obfuscation method. Similar to photo satisfaction, from the linear mixed-effects model, the overall χ^2 on information sufficiency shows a variation among the 14 obfuscations, $\chi^2(13) = 1555.11$, $p < .0001$, with more effective obfuscations generally provide less information (Figure 3). As expected, the information sufficiency of *as is* ($M = 5.28$, $SD = 1.54$) is higher than all other obfuscations (all $d \geq 0.59$, all $p < .001$). Participants also give higher information sufficiency ratings to *face pixelating* ($M = 4.30$, $SD = 1.52$), *body pixelating* ($M = 4.13$, $SD = 1.59$), *body blurring* ($M = 3.97$, $SD = 1.62$), and *face blurring* ($M = 4.00$, $SD = 1.59$) compared to the remaining 9 obfuscation methods (all $d \geq 0.41$, all $p < .01$), which means that *blurring* and *pixelating* preserve more information in photos. Among the more effective obfuscation methods, *body avatar* ($M = 3.10$, $SD = 1.65$) provides more information than *body inpainting* ($M = 2.49$, $SD = 1.64$, $d = 0.33$, $p < .001$), *body masking* ($M = 2.18$, $SD = 1.43$, $d = 0.55$, $p < .001$), *body bar* ($M = 2.34$, $SD = 1.55$, $d = 0.45$, $p < .001$), *body point-light* ($M = 2.48$, $SD = 1.56$, $d = 0.38$, $p < .001$), and *body silhouette* ($M = 2.71$, $SD = 1.52$, $d = 0.24$, $p = .01$).

4.2.3 Photo Enjoyment. From the linear mixed-effects model of enjoyment, a similar pattern occurs where there is again a variation among the 14 conditions, $\chi^2(13) = 795.09$, $p < .0001$, with that more effective obfuscations are less enjoyable (Figure 3). The mean enjoyment of *as is* photos ($M = 4.65$, $SD = 1.64$) is higher than all others (all d ≥ 0.39, all $p < .001$). Participants felt that photos with the *body avatar* obfuscation ($M = 3.64$, $SD = 1.81$) were about equally enjoyable with *body pixelating* ($M = 3.77$, $SD = 1.61$, $d = 0.07$, $p = .99$), *body blurring* ($M = 3.70$, $SD = 1.61$, $d = 0.03$, $p = 1.00$), and *face blurring* ($M = 3.90$, $SD = 1.58$, $d = 0.15$, $p = .38$), though they create the most enjoyable photos (aside from *as is* and *face pixelating*). In addition, as our most effective obfuscation method, *body inpainting* ($M = 3.16$, $SD = 1.70$) is more enjoyable than *body masking* ($M = 2.45$, $SD = 1.46$, $d = 0.43$, $p < .001$) and *body bar* ($M = 2.74$, $SD = 1.54$, $d = 0.27$, $p < .01$).

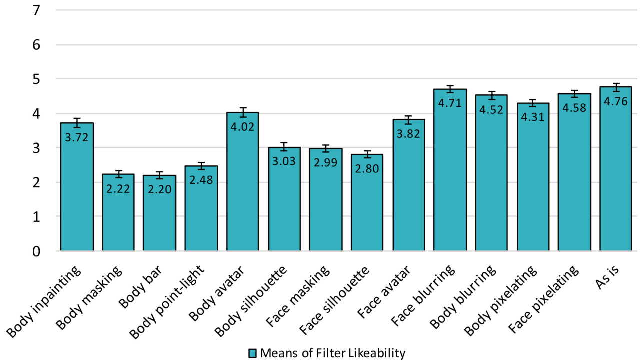


Fig. 4. Obfuscation likability (*M* and *SE*) from most to least effective.

4.2.4 Social Presence. Do the obscured photos still provide a sense of human contact? From the results of the linear mixed-effects model, the overall χ^2 of social presence scores demonstrated significant variation among the 14 conditions, $\chi^2(13) = 754.27$, $p < .0001$. The social presence score in the *as is* condition ($M = 4.81$, $SD = 1.69$) is higher than in all other obfuscation conditions (Figure 3) (all $d \geq 0.30$, all $p < .001$). Beyond *as is*, the scores of other obfuscations are less spread out between conditions than the other scores, with most social presence scores around 3 or 4. *Body masking* has the lowest social presence score ($M = 2.76$, $SD = 1.65$). Again, *body inpainting*(1) ($M = 3.34$, $SD = 1.85$) and *body avatar*(2) ($M = 3.42$, $SD = 1.75$) provide a better sense of human contact than *body masking* ($M = 2.76$, $SD = 1.65$, $d_1 = 0.34$, $p_1 < .001$, $d_2 = 0.40$, $p_2 < .01$) and *body bar* ($M = 2.93$, $SD = 1.64$, $d_1 = 0.24$, $p_1 < .001$, $d_2 = 0.29$, $p_2 < .001$). While not significant, their social presence ratings are slightly higher than *body point-light* ($M = 3.08$, $SD = 1.71$) and *body silhouette* ($M = 3.14$, $SD = 1.67$).

4.2.5 Obfuscation Likability. Moving from participants' attitudes towards the photos to their attitudes towards the obfuscations themselves, we ask how much they like (or dislike) the obfuscations. From the results of the linear mixed-effects model, there is a variation among obfuscation conditions, $\chi^2(13) = 963.46$, $p < .0001$, but There is no difference between *as is* ($M = 4.76$, $SD = 2.02$), *face pixelating* ($M = 4.58$, $SD = 1.74$), *body pixelating* ($M = 4.31$, $SD = 1.75$), *body blurring* ($M = 4.52$, $SD = 1.68$), and *face blurring* ($M = 4.71$, $SD = 1.70$) (all $d \leq 0.19$, all $p > .05$). Generally, the rightmost five conditions in Figure 4 are similarly likable. Among the remaining nine obfuscation methods, participants like *body avatar* ($M = 4.02$, $SD = 2.08$), *face avatar* ($M = 3.82$, $SD = 1.99$), and *body inpainting* ($M = 3.72$, $SD = 2.13$) more than the other six obfuscations (all $d \geq 0.26$, all $p < .05$).

4.2.6 Obfuscation Preference. At the end, we asked participants which obfuscation method they would most like to use to obfuscate their own online photos (Table 4). Participants reported they would most like to use *as is* (23%), *face blurring* (15%), *body avatar* (12%), *body inpainting* (11%), and *face avatar* (9%). In contrast, very few people chose *body bar* (1%), *body masking* (2%), *body point-light* (2%), *body silhouette* (2%), or *face masking* (2%), and there was only one participant who preferred *face silhouette* (resulting in a rounded percentage of zero). Leaving out ineffective *blurring* and *pixelating*, the preferences for *body avatar* and *inpainting* (around or larger than 10%) are about five times as high as for other obfuscations which are mostly below 2%. Asking participants how willing they would be to use their preferred obfuscation method, we found that they generally had a positive attitude, with all obfuscations scoring at or above 4 on a 7-point scale (Table 4). Aside from *as is* ($M = 6.15$, $SD = 1.21$), participants who preferred *body avatar* reported the highest

Table 4. Obfuscation preference, willingness to use, and preference given privacy concerns. Standard deviations appear in parentheses beside the means. Obfuscations are ordered from most to least effective.

		General preference	Willingness to use	Preference given privacy concern
	As is	23%	6.15 (1.21)	1%
Face	Masking	2%	5.40 (0.89)	2%
	Silhouette	0%	4.00 (0.00)	0%
	Avatar	9%	5.80 (0.96)	17%
	Blurring	15%	5.60 (1.40)	26%
	Pixelating	7%	5.74 (0.73)	9%
Body	Inpainting	11%	5.29 (1.53)	15%
	Masking	2%	4.50 (2.74)	0%
	Bar	1%	5.25 (1.50)	4%
	Point-light	2%	5.00 (2.35)	1%
	Avatar	12%	5.94 (1.03)	16%
	Silhouette	2%	4.67 (0.52)	1%
	Blurring	5%	5.23 (1.30)	4%
	Pixelating	7%	5.75 (0.97)	4%

willingness to use the obfuscation of their choice (M = 5.94, SD = 1.03). In the open-ended question, participants stated that *body avatar* "as least give some context to the photo if someone saw it online and looks kind of fun, " "most pleasing to the eyes, cute, " "protects someones privacy but it makes it lighthearted," "the avatar keeps the person's identity semi-private while not taking away from the composition of the photo with a line, block, or blur," and "privacy does not have to be so bland, the avatar is creative." For *inpainting*, they considered it "looks best to fully remove the person from the picture if it can be done in a way that isn't fully obvious," "it is like they are not there at all," "just removes the person so that the photo isn't ruined," and "provides the true privacy." All above results introduce that *avatar* and *inpainting* are practically more preferable and create a better user experience than other effective obfuscations.

4.2.7 Would Privacy Obfuscations Change Privacy Behaviors? As a follow up question, participants answered whether they had ever decided not to upload a photo to an OSN for privacy reasons. Fifty three percent of participants reported they had indeed done so. Over half (56%) of those who had declined to upload a photo for privacy reasons reported that they would upload the photo they previously declined to share, if having access to an obfuscation. We asked the 81 participants who had privacy reasons that prevented them from sharing a photo in the past but reported they would upload a photo using one of the obfuscations which which obfuscation they would choose. Twenty-six percent selected *face blurring*, 17% selected *face avatar*, 16% preferred *body avatar*, and 16% would like to use *body inpainting* (Table 4).

5 DISCUSSION

Our overall goal is to increase the privacy options people have when sharing photos by discovering obfuscations that are both effective against re-identification and preferred/likable by users. First, we discuss the effectiveness of the obfuscations. We find that body obfuscations are generally more effective than face obfuscations (see the "body vs. face" part of the Results section), and there is no practical difference in user experience between face and body (for example, the likability difference between *face avatar* and *body avatar* is just 0.2, which means participants have almost the same

Table 5. Summary of photo obfuscation methods (body-obfuscations only because they are more effective; see “Effectiveness: Face-obscuring vs. Body-obscuring.”) Effectiveness is defined by the difference in the identification success percentage of *as is* and each body obfuscation (see Table 2). The misidentification of *as is* is 23% (100% minus 77%). An obfuscation that achieves at least twice of *as is* misidentification (46%) is defined as "Somewhat effective", so the identification success should be no more than 54%. An obfuscation that achieves at least three times of *as is* misidentification (69%) is considered "Effective", so the identification success should be at most 31%. Obfuscations are ordered from most to least effective.

	Prior Use for Privacy Protection	**Preference**	**Effectiveness Against Human Recognition**	**Effectiveness Against Machine Recognition**
Inpainting	Less common. Used for photo [73] and video [41, 60, 85].	Preferred	Effective	Unknown, suspected highly effective
Masking	Less common. Used for photo [40] and video [41, 85].	Not preferred	Effective	Unknown, suspected highly effective
Bar	Rare. Used for video [85].	Not preferred	Effective	Unknown, suspected highly effective
Point-light	Rare. Used for video [17].	Not preferred	Effective	Unknown, suspected effective
Avatar	Rare. Used for photo [65] and video [60, 70].	Preferred	Somewhat effective	Unknown, suspected effective
Silhouette	Less common. Used for photo [60, 85] and video [41].	Not preferred	Somewhat effective	Unknown, suspected effective
Blurring	Common. Used for photo [6, 29, 35, 49] and video [10]	Less-preferred	Ineffective	Ineffective [46, 55]
Pixelating	Common. Used for photo [24, 45, 80] and video [11, 39].	Less-preferred	Ineffective	Ineffective [55]
As is	N/A	Preferred	Ineffective	Ineffective [61]

attitude towards these two obfuscations). Hence in the following discussions, we only discuss body obfuscations which are relatively more effective and without user experience decreasing. Next, we discuss the user experience of the obfuscations. Finally, we integrate these, along with prior work on machine re-identification (vs. human re-identification) to generate recommendations about the most effective and likable obfuscations for photo privacy (Table 5).

5.1 Effectiveness: Face vs. Body

We found that body-obfuscations were more effective than face-obscuring obfuscations with a 9% success difference (see section *Body vs. Face*). From the practical perspective, obscuring the body is also supposed to be more effective against human recognition than obscuring the face because it can conceal more details such as clothes, gestures, gender, race, and height that may reveal a person's identity [1, 67]. Similarly, machines may be able to infer a person's identity from a photo with only the face obscured based on body information or the same clothes appearing in different photos over time [59]. In the case of OSNs, this effect would be exacerbated because we would expect people to primarily view familiar faces; *blurring* and *pixelating* are even less effective for familiar vs. unfamiliar faces [24]. Because they are more effective overall both in our work and in previous work, in the following discussion we only consider body obfuscations.

5.2 Moving Beyond Blurring and Pixelating

Although *blurring* and *pixelating* are commonly used both in research and in practice [6, 35, 80], our results suggest that they are two of the least effective obfuscation methods against human recognition (identification rates as high as 67%, Table 2; with above average confidence, Figure 2 and Table 3).

Consistent with prior work on *blurring* and *pixelating* obfuscations against human recognition [8, 45], participants in our study were able to identify humans who were blurred and pixelated in photos. This may because these obfuscations fail to hide body shape, skin and hair color. Color cues are important in face recognition. The effect of color becomes more evident when shape cues are degraded [84]. As we mentioned in section "Controlling Content", these features may also allow the obscured photo to be re-identified by machines. For example, generative adversarial networks (GAN) [46], and artificial neural networks [55] worked well to identify blurred and pixelated faces [55].

On the other hand, *inpainting*, *masking*, *bar*, *point-light*, and *avatar* are much more effective in obfuscating the target in each photo (Table 2). Participants are also less confident about their ability to identify people who are de-identified using these obfuscations (Figure 2 and Table 3), regardless of whether their identification is correct or incorrect. In other words, these obfuscations are effective and viewers feel less confident in their ability to recognize targets when viewing them. This finding is consistent with prior work about the relationship between activity visibility and perception confidence that the less visible an activity is, the perceptions are more likely to derive from participants' own experiences, thus lower accuracy and confidence they have [4].

Perhaps surprisingly, participants were only somewhat unconfident (with mean ratings around three), rather than very unconfident about their ability to recognize targets in effective obfuscations. Partly, this may be due to the effect of our experimental interface. Participants were forced to make a choice even when they did not know which target was present. Once they made their choice, cognitive dissonance may have led them to report they were "somewhat" rather than "very" unconfident in that choice. Alternatively, or additionally, Americans are more likely to choose a Likert option that indicates positive emotion [47]. Participants may have chosen the most positive choice (somewhat unconfident) among the options on the unconfident side of the scale. These speculations do not take away from the key finding: participants were less confident in their recognition of effective obfuscations.

Inpainting, which removes all visual clues about the person in a photo, is the most effective obfuscation, yielding a mere 19% identification success, which is notably, less than chance (25%). When target is present, this rate decreases to 7% which is much lower than chance, indicating, as expected, participants were unable to identify a target in this condition. When the target is absent most participants chose "None of above" because the target is completely removed, resulting in more correct rejections (67%). In a sense, this is an ideal scenario: rather than trying to guess the target's identity, it is better for viewers to simply assume that there is no one there at all.

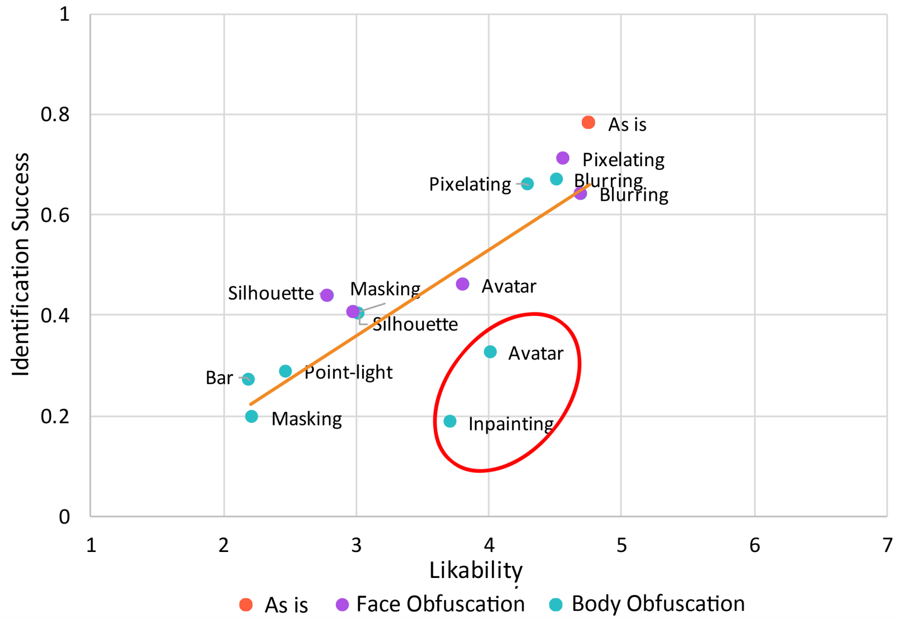


Fig. 5. Scatterplot of Likability (X axis) against Identification Success (Y axis). This plot shows the general trade-off between effectiveness and user experience. However, body avatar and body inpainting are outliers. They are both effective and provide a good user experience.

5.3 User Experience

The upward slopes in Figures 3–5 demonstrate that overall, there is a trade-off between obfuscation effectiveness and user experience: obfuscations with a higher effectiveness have a lower user experience in terms of satisfaction, information sufficiency, enjoyment, social presence, and likability. The scatter plot in Figure 5 , which plots likability against identification success, also demonstrates this trend.

Blurring and *pixelating* are subtle; they preserve many visual features of an image such as the colors and shapes [84]. Because of the subtlety, people may not notice the affected region at first glance. While this subtlety may contribute to relatively high levels of satisfaction, it also likely results in their relative ease of recognition. Conversely, *masking*, *bar*, and *point-light* are more effective, but they are less satisfying, give insufficient information, are less enjoyable, and lack a sense of social presence. This is also reflected by the preference percentages (only around 2%) and qualitative feedback of these three obfuscations. For example, participants thought dots or lines damaged the photo aesthetics. As we will discuss in the following section, *inpainting* and *avatar* are exceptions that are both effective and provide a relatively good user experience.

5.4 Better Options: Inpainting and Avatar

Although effective obfuscations are generally less satisfying (Figure 5), *inpainting* and *avatar* are outliers to this trend. They are very effective, and, as compared to other effective obfuscations, have high levels of satisfaction, information sufficiency, enjoyment, social presence and likability.

We could argue that the user experience ratings of *inpainting* should be similar to the *as is* condition, because *inpainting* does not add unrelated content (e.g. a large gray box) to the image.

Ostensibly, with the target completely removed and the area filled in by existing photo content, the only difference is the number of people in the group photo. However, after removing the target, an unnatural seeming space were left, damaging the composition [48]. Furthermore, participants probably knew, based on in-study experience, that there likely used to be a person in the gap they saw in the photo. The awkwardness of this gap may have reduced the user experience.

Future versions of *inpainting* could improve the user experience by using more sophisticated image re-construction techniques to recompose the picture after removing the target [21, 30]. Using these techniques, we can imagine a system that could first extract the people in the photo, identify and fill gaps in the background, and finally put the people back to achieve an optimal composition, but without the target. Indeed, we see promising commercial applications that have elements of this functionality already present such as Photoshop's "content aware patch" and Snapseed's "Expand [75] " feature. While currently these advanced editing options are not suited to the task (e.g., sometimes these generate unnatural double images), we see promise for techniques such as these to create *inpainting* obfuscation options that provide a better user experience.

Unlike *inpainting*, *avatar* does add content to an image, so we might not expect the user experience ratings of *avatar* to be similar to *as is*. However, the user experience ratings of the *avatar* obfuscation were higher than all other effective obfuscation methods, and therefore should be further explored. One noteworthy thing about *avatar* is that the photo enjoyment rating of *body avatar* is slightly higher than *face avatar*, indicating that people may prefer to see a complete cartoon character rather than just a cartoon face. However, except for Bitmoji [9], existing approaches to avatar creation mainly focus on generating avatars that look somewhat like the target, but with an exclusive focus on the face (e.g., facial component matching [65]). Future avatar-based approaches for photo obfuscation may benefit from the development of methods to create full-body avatars instead of face avatars as this may improve the user experience.

Our results show that *avatar* and *inpainting* also provide a greater sense of human contact than other effective obfuscations. For *avatar*, the cartoon human character preserves the target's facial expression and gesture. Viewers may feel this feature allows them to perceive human contact both among the people within the photo, and between themselves and the people in the photo [5]. For *inpainting*, since the target is totally removed, people may be less likely to be jarred by the visual indicator of the lack of presence of a person in the photo. People tend to select the medium that they perceive to have the highest human contact, hence enough human contact in a photo or on OSNs would increase their participation and encourage them continue using the medium [28].

Participants qualitative input was consistent with the quantitative results about users' experience. For example, *inpainting* and *avatar* are more likable and preferable than other highly effective obfuscations. In open response format, participants mentioned that they liked *inpainting* because "it is the most thorough privacy technique," "it seems you were never there in the first place and there is no way to identify you," "it is the best way to make the photo visually appealing," and "provides true privacy." For *avatar*, they stated it is "cute and fun," "catches the eyes," "still shows the person in a positive light," and "inserts personality, you can customize it." Participants' comments revealed that they preferred *face blurring* for many of the reasons they liked *inpainting* and *avatar*, but were unaware of the ineffectiveness of *blurring*. Participants reported that they thought *blurring* "adequately hides identity while still giving information about the original photo and person's attitude," "the body without a clear face doesn't tell much," and "preserves the integrity of the picture while providing some form of privacy." This implies that, perhaps because of its widespread use, people are unaware that *blurring* is ineffective against both human (Table 2 and Table 5) and machine identification [46, 55]. One clear implication is that if users are provided with obfuscation options, they should be clearly informed about the benefits and drawbacks of each (e.g., *blurring* is ineffective as a privacy-enhancement).

Finally, *inpainting*, *avatar* and *face blurring* were the most commonly selected obfuscations people would want to use to obscure a photo they had previously declined to upload to an OSN for privacy reasons. Participants reported they would be willing to upload that photo, if they had an obfuscation available as a solution to their privacy dilemma. **These results indicate that obfuscation methods, especially *inpainting* and *avatar*, have the potential to dramatically increase the privacy options available to people who want to share photos on OSNs.** In OSN scenario, users can *inpaint* themselves in a photo which their friend uploads, that generates a re-constructed photo that is closest to the original one. Hence, the photo uploader will not feel much sharing loss, and viewers will not even be aware. On the other hand, though both the uploader and viewers will be aware of the *avatar* obfuscation, it brings positive emotions, as our participants stated: "cute" and "fun." It is similar to other frequently used applications which add cartoon figure or emoji in a photo. *Avatar* makes photos more interesting and protects privacy. Both obfuscations reduce privacy conflicts in photo sharing on OSNs.

5.5 Obfuscation Timing: at capture, upload or share?

Besides the obfuscation methods, obfuscation timing is also important to consider when developing photo privacy control mechanisms. Obfuscations can be applied at various stages of photo processing: at the time of capture, on the device, at the time of upload, or at the time of sharing. Applying an obfuscation at each stage has different privacy benefits and addresses different concerns [43]. Applying at the time of sharing means that an OSN, for example, would gain access to a raw photo (including identifiable information) but "friends" may not see the raw photo because of the obfuscation, which addresses concerns about social threats [32, 43]. On the other hand, we could apply an obfuscation at the time of photo capture, such that only an obfuscated image is captured on a device (e.g., phone). In this example, an image would be obfuscated before upload, and an OSN would never gain access to the raw photo, which addresses organizational threats related to OSN providers and various third parties [43].

We already see somewhat related commercially available examples of the first situation, where "filters" are applied at the sharing stage (e.g., Facebook and Snapchat photo filters [31, 69]). However, these obfuscations are not designed to obfuscate, nor are they likely effective as a privacy-enhancement, though this warrants future investigation. From our qualitative data, we know that at least some participants have privacy concerns about the privacy of their photos as shared with platforms (e.g., an OSN like Facebook). One participant raised his/her concern about this by saying: "*Facebook identifies you first, then blurs you, but Facebook already tracks you.*" People fear that their information will be collected, stored, sold, and reuse by OSN providers or other third parties [43].

One possible solution, therefore, is to apply privacy obfuscations before uploading images to such platforms. However, identifying and obfuscating sensitive parts in an image is computationally resource-intense, for example, increasing CPU usage [42]. A remarkable degradation in efficiency in case of devices is observed with the increase in the number of people in the photos being processed. Thus, accomplishing privacy obfuscation on a device (vs. offloading to the cloud, for example) will require a re-thinking of desired device capabilities. Should new cameras be designed with computer vision capabilities on board, as suggested by [16]? How can automated redaction be done in a more efficient (from a memory, power, etc. perspective) on the device rather than on the cloud so that private information does not need to leave the device thus putting it at greater risk for leaking, hacking, etc.?

6 LIMITATIONS AND FUTURE WORK

First, other information, besides a visual representation of the face and body of a person can be revealing. The risk of contextual cues in identification is particularly acute in OSNs because of their social nature. For example, in an OSN un-obscured mutual friends, the background [71], any text or personal belongings, the comments under the photo [35], and the time and location [77] may lead to identification of an obscured person. The approaches we have identified here may be similarly effective and satisfying when applied to these contextual photo elements. However, this is certainly worth investigating in the future.

Second, participants were recruited via mTurk. Though Turkers are relatively more demographically diverse than the sample collected by other means [12], recruiting this way has drawbacks. For example, MTurk only allows studies to be conducted online and has a unique nature of labor [54]. Future work should replicate this study with non-mTurk participants.

Third, we expected to see more spread across user experience scores, and were especially surprised by the low baseline scores for *as is*. We expect some the relative homogeneity of scores may be due to the limited photo quality. Because user experience scores were low in the baseline condition there was less room for differences to emerge between baseline and other conditions. Thus, while we saw statistically different scores, these differences were small (less than one point on a seven-point scale).

Fourth, the user experience rating of *masking* is the worst compared to all other obfuscations. Besides the box covering content in the photo beyond just the target, the gray color used may also be an issue. We decided to use gray for the box to ensure a consistent experience and to prevent any gender indication, (e.g., a pink box could indicate the obscured target is a female [37]). However, gray may evoke negative emotions compared to warmer and brighter colors and result in less perceived human contact both within the photo and between the viewer and the photo [52].

Finally, a research question around computer vision emerge from this work: What automated interpolation techniques are most effective at creating effective, acceptable and seamless inpainting? For example, reconstructing 3D models of world landmarks using collections on photo sharing sites may allow recovery of obfuscated parts of photos [21]. Future studies need to further investigate how platforms and devices might implement the user experience enabling these obfuscations.

7 CONCLUSION

There are two elements to protecting privacy: recipient and content. While most prior work in photo privacy focused on controlling the recipient, in this work, we focused on controlling the content. We evaluated 14 obfuscation methods in terms of their effectiveness against human recognition and user experience. The results show that the two most commonly studied and used obfuscations, *blurring* and *pixelating*, are not effective at preventing humans (or, drawing from related work, machines) from recognizing the content of a photo. Thus, the most commonly used privacy obfuscations do not provide privacy protection. We then introduce novel obfuscations that *are* effective at preventing humans from recognizing content in an image. Of the highly effective obfuscations we introduce, we then analyze these from the perspective of user experience finding that *inpainting*, which totally removes the content from the photo, and *avatar*, which replaces the content with an avatar, outperform other obfuscations. We suggest that *body inpainting* and *body avatar* show promise as photo privacy-enhancing technologies because they are effective from a human recognition perspective and provide a good user experience.

ACKNOWLEDGMENTS

This research was supported by the National Science Foundation under grant no.1527421. We thank Cheng Guo for assistance with Qualtrics and colleagues from the HATlab for suggestions that improved this study. We would also like to thank Mahdi Nasrullah Al-Ameen, Byron Lowens, Yangyang He, Daricia Wilkinson, Pratitee Sinha, Mary-Jo May, Brian Justice, Ellie Ebrahimi, Geoffry Sheehan, Brady Bannister, Jason Alexander, Levin Czenkusch, Freddie Pope and Matthew Ellsworth

who served as models for our stimuli. Finally, we are grateful to the people who participated in this study.

REFERENCES

[1] Prachi Agrawal. 2010. *De-Identification for Privacy Protection in Surveillance Videos*. Ph.D. Dissertation. International Institute of Information Technology Hyderabad, India.

[2] Hazim Almuhimedi, Shomir Wilson, Bin Liu, Norman Sadeh, and Alessandro Acquisti. 2013. Tweets are forever: a large-scale quantitative analysis of deleted tweets. In *Proceedings of the 2013 conference on Computer supported cooperative work*. ACM, 897–908.

[3] Irwin Altman. 1975. The environment and social behavior. (1975).

[4] Eric P.S. Baumer, Xiaotong Xu, Christine Chu, Shion Guha, and Geri K. Gay. 2017. When Subjects Interpret the Data: Social Media Non-use As a Case for Adapting the Delphi Method to CSCW. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 1527–1543. https://doi.org/10.1145/2998181.2998182

[5] Gary Bente, Sabine Rüggenberg, Nicole C Krämer, and Felix Eschenburg. 2008. Avatar-Mediated Networking: Increasing Social Presence and Interpersonal Trust in Net-Based Collaborations. *Human communication research* 34, 2 (2008), 287–318.

[6] Andrew Besmer and Heather Lipford. 2009. Tagged photos: concerns, perceptions, and protections. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. ACM, 4585–4590.

[7] Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1563–1572.

[8] Markus Bindemann, Janice Attard, Amy Leach, and Robert A Johnston. 2013. The Effect of Image Pixelation on Unfamiliar-Face Matching. *Applied Cognitive Psychology* 27, 6 (2013), 707–717.

[9] Bitmoji. 2016. Your own personal Emoji. (2016). Retrieved April 23, 2017 from https://www.bitmoji.com/.

[10] YouTube Official Blog. 2012. Face blurring: when footage requires anonymity. Blog. (18 July 2012). Retrieved April 13, 2017 from https://youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html.

[11] Michael Boyle, Christopher Edwards, and Saul Greenberg. 2000. The effects of filtered video on awareness and privacy. In *Proceedings of the 2000 ACM conference on Computer supported cooperative work*. ACM, 1–10.

[12] Michael Buhrmester, Tracy Kwang, and Samuel D Gosling. 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on psychological science* 6, 1 (2011), 3–5.

[13] U.S. Census Bureau. 2010. American FactFinder - Race Results. (2010). https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=DEC_10_DP_DPDP1&src=pt

[14] United States Census Bureau. 2014. Geography Division. (2014). Retrieved April 21, 2017 from https://www2.census.gov/geo/pdfs/maps-data/maps/reference/us_regdiv.pdf.

[15] Kelly Caine and Rima Hanania. 2013. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association* 20, 1 (2013), 7–15.

[16] Kelly Erinn Caine. 2009. *Exploring everyday privacy behaviors and misclosures*. Ph.D. Dissertation. Georgia Institute of Technology.

[17] Kelly E Caine, Wendy A Rogers, and Arthur D Fisk. 2005. Privacy perceptions of an aware home with visual sensing devices. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 49. SAGE Publications, 1856–1858.

[18] L Elisa Celis, Sai Praneeth Reddy, Ishaan Preet Singh, and Shailesh Vaya. 2016. Assignment Techniques for Crowdsourcing Sensitive Tasks. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 836–847.

[19] Datong Chen, Yi Chang, Rong Yan, and Jie Yang. 2009. Protecting personal identification in video. In *Protecting Privacy in Video Surveillance*. Springer, 115–128.

[20] Hichang Cho and Anna Filippova. 2016. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 503–514.

[21] David Crandall and Noah Snavely. 2012. Modeling people and places with internet photo collections. *Commun. ACM* 55, 6 (2012), 52–60.

[22] Dianne Cyr, Milena Head, Hector Larios, and Bing Pan. 2009. Exploring human images in website design: a multi-method approach. *MIS quarterly* (2009), 539–566.

[23] Bernhard Debatin, Jennette P Lovejoy, Ann-Kathrin Horn, and Brittany N Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15, 1 (2009), 83–108.

[24] Jelle Demanet, Kristof Dhont, Lies Notebaert, Sven Pattyn, and André Vandierendonck. 2007. Pixelating Familiar People in the Media: Should Masking Be Taken at Face Value? *Psychologica belgica* 47, 4 (2007).

[25] Martha Farah, GW Humphreys, and HR Rodman. 1999. Object and face recognition. *Fundamental neuroscience, ed. MJ Zigmond, FE Bloom, SC Landis, JL Roberts & LR Squire. Academic Press.[aFVDV]* (1999).

[26] Kraig Finstad. 2010. Response interpolation and scale sensitivity: Evidence against 5-point scales. *Journal of Usability Studies* 5, 3 (2010), 104–110.

[27] Michael Fire, Roy Goldschmidt, and Yuval Elovici. 2014. Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials* 16, 4 (2014), 2019–2036.

[28] Andrew J Flanagin and Miriam J Metzger. 2001. Internet use in the contemporary media environment. *Human communication research* 27, 1 (2001), 153–181.

[29] Andrea Frome, German Cheung, Ahmad Abdulkader, Marco Zennaro, Bo Wu, Alessandro Bissacco, Hartwig Adam, Hartmut Neven, and Luc Vincent. 2009. Large-scale privacy protection in google street view. In *Computer Vision, 2009 IEEE 12th International Conference on.* IEEE, 2373–2380.

[30] Pulkit Goyal, Sapan Diwakar, et al. 2010. Fast and enhanced algorithm for exemplar based image inpainting. In *Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on.* IEEE, 325–330.

[31] Amelia Heathman. 2017. Fabook's Snapchat-style stories and effects are live. Here's how to use them. (28 March 2017). Retrieved April 23, 2017 from http://www.wired.co.uk/article/facebook-filters-like-snapchat.

[32] Anne Hewitt and Andrea Forte. 2006. Crossing boundaries: Identity management and student/faculty relationships on the Facebook. *Poster presented at CSCW, Banff, Alberta* (2006), 1–2.

[33] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing.* ACM, 571–582.

[34] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2011. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference.* ACM, 103–112.

[35] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.* ACM, 781–792.

[36] Rob Johns. 2010. Likert items and scales. *Survey Question Bank: Methods Fact Sheet* 1 (2010), 1–11.

[37] Holy Juan. 2010. Facebook redacting. (2010). Retrieved April 23, 2017 from http://www.holyjuan.com/2010/12/facebook-redacting.html.

[38] Mohammed Korayem, Robert Templeman, Dennis Chen, David Crandall, and Apu Kapadia. 2016. Enhancing lifelogging privacy by detecting screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* ACM, 4309–4314.

[39] Pavel Korshunov, Claudia Araimo, Francesca De Simone, Carmelo Velardo, J-L Dugelay, and Touradj Ebrahimi. 2012. Subjective study of privacy filters in video surveillance. In *Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on.* Ieee, 378–382.

[40] Pavel Korshunov, Andrea Melle, Jean-Luc Dugelay, and Touradj Ebrahimi. 2013. Framework for objective evaluation of privacy filters. In *SPIE Optical Engineering+ Applications.* International Society for Optics and Photonics, 88560T–88560T.

[41] Takashi Koshimizu, Tomoji Toriyama, and Noboru Babaguchi. 2006. Factors on the sense of privacy in video surveillance. In *Proceedings of the 3rd ACM workshop on Continuous archival and retrival of personal experences.* ACM, 35–44.

[42] Sokol Kosta, Andrius Aucinas, Pan Hui, Richard Mortier, and Xinwen Zhang. 2012. Thinkair: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In *Infocom, 2012 Proceedings IEEE.* IEEE, 945–953.

[43] Hanna Krasnova, Oliver Günther, Sarah Spiekermann, and Ksenia Koroleva. 2009. Privacy concerns and identity in online social networks. *Identity in the Information Society* 2, 1 (2009), 39–63.

[44] Nanda Kumar and Izak Benbasat. 2006. Research note: the influence of recommendations and consumer reviews on evaluations of websites. *Information Systems Research* 17, 4 (2006), 425–439.

[45] Karen Lander, Vicki Bruce, and Harry Hill. 2001. Evaluating the effectiveness of pixelation and blurring on masking the identity of familiar faces. *Applied Cognitive Psychology* 15, 1 (2001), 101–116.

[46] Christian Ledig, Lucas Theis, Ferenc Huszár, Jose Caballero, Andrew Cunningham, Alejandro Acosta, Andrew Aitken, Alykhan Tejani, Johannes Totz, Zehan Wang, et al. 2016. Photo-realistic single image super-resolution using a generative adversarial network. *arXiv preprint arXiv:1609.04802* (2016).

[47] Jerry W Lee, Patricia S Jones, Yoshimitsu Mineyama, and Xinwei Esther Zhang. 2002. Cultural differences in responses to a Likert scale. *Research in nursing & health* 25, 4 (2002), 295–306.

[48] Congcong Li, Alexander C Loui, and Tsuhan Chen. 2010. Towards aesthetics: A photo quality assessment and photo selection system. In *Proceedings of the 18th ACM international conference on Multimedia*. ACM, 827–830.

[49] Yifang Li, Nishant Vishwamitra, Hongxin Hu, Bart P. Knijnenburg, and Kelly Caine. 2017. Effectiveness and users' experience of face blurring as a privacy protection for sharing photos via online social networks. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61. SAGE.

[50] Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Blur vs. Block: Investigating the Effectiveness of Privacy-Enhancing Obfuscation for Images. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2017 IEEE Conference on*. IEEE, 1343–1351.

[51] Heather Richter Lipford, Pamela J Wisniewski, Cliff Lampe, Lorraine Kisselburgh, and Kelly Caine. 2012. Reconciling privacy with social media. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion*. ACM, 19–20.

[52] Banu Manav. 2007. Color-emotion associations and color preferences: A case study for residences. *Color Research & Application* 32, 2 (2007), 144–150.

[53] Alice E Marwick and Danah Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 7 (2014), 1051–1067.

[54] Winter Mason and Duncan J Watts. 2010. Financial incentives and the performance of crowds. *ACM SigKDD Explorations Newsletter* 11, 2 (2010), 100–108.

[55] Richard McPherson, Reza Shokri, and Vitaly Shmatikov. 2016. Defeating Image Obfuscation with Deep Learning. *arXiv preprint arXiv:1609.00408* (2016).

[56] Kyle B Murray and Gerald Häubl. 2010. Freedom of choice, ease of use, and the formation of interface preferences. (2010).

[57] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[58] Helen Nissenbaum. 2011. A contextual approach to privacy online. *Daedalus* 140, 4 (2011), 32–48.

[59] Seong Joon Oh, Rodrigo Benenson, Mario Fritz, and Bernt Schiele. 2016. Faceless person recognition: Privacy implications in social media. In *European Conference on Computer Vision*. Springer, 19–35.

[60] José Ramón Padilla-López, Alexandros Andre Chaaraoui, Feng Gu, and Francisco Flórez-Revuelta. 2015. Visual privacy by context: proposal and evaluation of a level-based visualisation scheme. *Sensors* 15, 6 (2015), 12959–12982.

[61] Omkar M Parkhi, Andrea Vedaldi, and Andrew Zisserman. 2015. Deep Face Recognition.. In *BMVC*, Vol. 1. 6.

[62] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. 2014. Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior research methods* 46, 4 (2014), 1023–1031.

[63] Mark R Phillips, Bradley D McAuliff, Margaret Bull Kovera, and Brian L Cutler. 1999. Double-blind photoarray administration as a safeguard against investigator bias. *Journal of Applied Psychology* 84, 6 (1999), 940.

[64] Joseph P Redden. 2008. Reducing satiation: The role of categorization level. *Journal of Consumer Research* 34, 5 (2008), 624–634.

[65] Chi-Hyoung Rhee and C LEE. 2013. Cartoon-like avatar generation using facial component matching. *Int. J. of Multimedia and Ubiquitous Engineering* 8, 4 (2013), 69–78.

[66] Joel Ross, Lilly Irani, M Silberman, Andrew Zaldivar, and Bill Tomlinson. 2010. Who are the crowdworkers?: shifting demographics in mechanical turk. In *CHI'10 extended abstracts on Human factors in computing systems*. ACM, 2863–2872.

[67] Mukesh Saini, Pradeep K Atrey, Sharad Mehrotra, and Mohan Kankanhalli. 2014. W3-privacy: understanding what, when, and where inference channels in multi-camera surveillance video. *Multimedia Tools and Applications* 68, 1 (2014), 135–158.

[68] Peter Seddon and Min-Yen Kiew. 1996. A Partial Test and Development of Delone and Mclean's Model of IS Success. *Australasian Journal of Information Systems* 4, 1 (1996). https://doi.org/10.3127/ajis.v4i1.379

[69] Snapeditor. 2017. Snapchat effeects: how to use lenses & filters for face effects. (24 January 2017). Retrieved April 23, 2017 from https://snapchat.photography/snapchat-effects/.

[70] Nadia Spock. 2016. Snapchat gives a voice to survivors of sexual abuse. Blog. (21 July 2016). Retrieved April 13, 2017 from http://news.wgbh.org/2016/07/21/snapchat-gives-voice-survivors-sexual-abuse.

[71] Anna Cinzia Squicciarini, Dan Lin, Smitha Sundareswaran, and Joshua Wede. 2015. Privacy policy inference of user-uploaded images on content sharing sites. *IEEE transactions on knowledge and data engineering* 27, 1 (2015), 193–206.

[72] John A Swets. 1964. Signal Detection and Recognition in Human Observers: Contemporary Readings. (1964).

[73] Yasuhiro Tanaka, Akihisa Kodate, Yu Ichifuji, and Noboru Sonehara. 2015. Relationship between Willingness to Share Photos and Preferred Level of Photo Blurring for Privacy Protection. In *Proceedings of the ASE BigData & SocialInformatics 2015*. ACM, 33.

[74] Kurt Thomas, Chris Grier, and David M Nicol. 2010. unfriendly: Multi-party privacy risks in social networks. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 236–252.

[75] Cody Toombs. 2017. Snapseed v2.17 adds tools to make wild facial adjustments, create double exposures, and more. Blog. (22 March 2017). http://www.androidpolice.com/2017/03/22/snapseed-v2-17-adds-tools-to-make-wild-facial-adjustments-create-double-exposures-and-more-apk-download/.

[76] Janet Vertesi, Jofish Kaye, Samantha N Jarosewski, Vera D Khovanskaya, and Jenna Song. 2016. Data Narratives: uncovering tensions in personal data management. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 478–490.

[77] Carmen Ruiz Vicente, Dario Freni, Claudio Bettini, and Christian S Jensen. 2011. Location-related privacy in geo-social networks. *IEEE Internet Computing* 15, 3 (2011), 20–27.

[78] Nishant Vishwamitra, Yifang Li, Kevin Wang, Hongxin Hu, Kelly Caine, and Gail-Joon Ahn. 2017. Towards PII-based Multiparty Access Control for Photo Sharing in Online Social Networks. In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*. ACM, 155–166.

[79] Jessica Vitak and Jinyoung Kim. 2014. You can't block people offline: Examining how Facebook's affordances shape the disclosure process. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, 461–474.

[80] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2015. Filter Selection and Evaluation. (2015).

[81] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[82] Pamela Wisniewski, AKM Islam, Bart P Knijnenburg, and Sameer Patil. 2015. Give social network users the privacy they want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, 1427–1441.

[83] Bin Xu, Pamara Chang, Christopher L Welker, Natalya N Bazarova, and Dan Cosley. 2016. Automatic archiving versus default deletion: What Snapchat tells us about ephemerality in design. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 1662–1675.

[84] Andrew W Yip and Pawan Sinha. 2002. Contribution of color to face recognition. *Perception* 31, 8 (2002), 995–1003.

[85] Xiaoyi Yu, Kenta Chinomi, Takashi Koshimizu, Naoko Nitta, Yoshimichi Ito, and Noboru Babaguchi. 2008. Privacy protecting visual processing for secure video surveillance. In *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*. IEEE, 1672–1675.

Received April 2017; revised July 2017; accepted November 2017