# More than Meets the Eye: Understanding the Effect of Individual Objects on Perceived Visual Privacy

Mete Harun Akcay
Åbo Academy University,
Nokia Bell Labs
meteharun.ackay@abo.fi

Siddarth Prakash Rao
Nokia Bell Labs
sid.rao@nokia-bell-labs.com

Alexandros Bakas
Nokia Bell Labs
alexandros.bakas@nokia-bell-labs.com

Buse Atli
Linköping University,
Nokia Bell Labs
busega@acm.org

***Abstract*—User-generated content, such as photos, comprises the majority of online media content and drives engagement due to the human ability to process visual information quickly. Consequently, many online platforms are designed for sharing visual content, with billions of photos posted daily. However, photos often reveal more than they intended through visible and contextual cues, leading to privacy risks. Previous studies typically treat privacy as a property of the entire image, overlooking individual objects that may carry varying privacy risks and influence how users perceive it. We address this gap with a mixed-methods study (n = 92) to understand how users evaluate the privacy of images containing multiple sensitive objects. Our results reveal mental models and nuanced patterns that uncover how granular details, such as photo-capturing context and co-presence of other objects, affect privacy perceptions. These novel insights could enable personalized, context-aware privacy protection designs on social media and future technologies.**

## I. Introduction

With the advent and ubiquity of affordable camera technologies, capturing and sharing visual content has become the new norm of everyday social interactions. A study in 2025 [1] reports that 14 billion images are shared daily on social media networks and instant messengers, a high percentage of which include photos of people with friends and family members. However, by sharing photos of their private lives and personal moments, they may inadvertently jeopardize their privacy. Exposing personally identifiable or sensitive information online can have serious consequences, such as identity theft [2], cyber-bullying [3], or cyber-stalking [4].

One of the well-studied privacy concerns related to sharing content online is behavioral profiling and targeted advertisements. These systems mainly rely on users' search queries, browsing patterns, and metadata to transform personal data and privacy into a commodity [5], [6]. However, a significant amount of information can be harvested purely from the visual content by humans and computer vision systems. Figure 1 demonstrates an example of how much information a single photo can reveal by combining different visual cues extracted from the image. News media investigations [1] have demonstrated how open-source intelligence tools and techniques can be utilized to extract rich information from shared visual content that was not originally intended [7], [8], [9]. Similarly, accessibility-focused research works in the field of human-computer interaction (HCI) have also explored privacy concerns associated with intentional or accidental disclosure of visual information [10], [11], [12], [13]. However, there is still some uncertainty about whether and how users can understand the complex visual and contextual cues in the photos they share online. Our work aims to explore this research theme to uncover the nuances of perceived visual privacy.

Our goal is to understand how individual objects (i.e., the visual elements within the image), which may have varying privacy risks in different contexts, influence users' privacy decisions. Previous studies focused mainly on the perceived privacy of the entire image to understand users' perceptions and behaviors while sharing photos online. More specifically, these works have focused on understanding whether a user evaluates the whole image as private or not [14], [15], [16], [17], or focuses on assessing the privacy risks of a single object [18]. However, these approaches overlook the effect of context and the co-presence of different privacy-sensitive objects within an image. A few works on users' privacy preferences regarding the sharing of visual content on social media have examined spatial context (location where the photo was taken) and social context (e.g., the number of individuals present in the image and the subject's relation to the image) [19]. Our work extends this line of research by exploring more fine-grained aspects of visual content.

**Contributions:** We offer novel insights into how end-users evaluate visual privacy and the factors that shape their privacy perceptions. Secondly, we provide empirical evidence on users' privacy heuristics, derived from a mixed-methods analysis of qualitative and quantitative data gathered through an online user survey (n = 92). Finally, we explore the use of synthetic images in user studies as a valuable alternative when real-world data is difficult to obtain.

**Overview of results:** We draw results by fixing the individual visual element, referred to as objects, in the foreground and

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23050
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

[1]The New York Times visual investigations and Bellingcat investigations


Fig. 1: An example demonstrating the amount of information revealed (intentionally or inadvertently) through a single visual content. The image is sampled from the MS-COCO dataset explorer and the text descriptions are a combined interpretation by a human observer (one of the authors of this work) and commercial GenAI methods (link to actual image is here).

studying its perceived privacy using varying combinations of objects in the background. In summary, we make the following observations:

- We found that users demonstrate a latent cognitive model for evaluating the intricate visual and contextual cues of the images. Users pay attention to granular details about the objects, such as what or who is in the photo and the situational context in which the photo is captured. This finding supports the well-established theories of contextual anchors of privacy decisions [20], and extends the knowledge by providing evidence about micro-details of context.
- We found that having certain categories of sensitive objects in the background dictates the privacy perception of those in the foreground. Especially when the background objects are unrelated to each other, the presence of other background objects has a negligible impact on the users' privacy perception of the foreground object due to the *dominance effect*. While previous studies have discussed the impact of similar salient features on privacy perception using anecdotal examples, we provide empirical evidence for the dominance effect.
- Certain combinations of semantically related sensitive objects in the background contribute to the perceived privacy of those in the foreground. While such individual background objects may still influence users' privacy judgments to some extent, their co-presence can trigger stronger concerns than what each would cause in isolation. Prior research has investigated the inference risks that arise when related elements from different datasets. However, a similar effect emerging from a single data item (such as individual images) is less explored to the best of our knowledge. In this direction, our findings offer novel insights into *co-presence effect* and its potential to trigger privacy concerns.

Our work contributes towards a comprehensive understanding of visual privacy perception that can potentially be utilized to develop personalized privacy preference options for sharing visual content online. In particular, the insights from this study can be leveraged for designing assistive technologies that share the entire content while removing, blurring, or masking privacy-sensitive objects, but still function effectively. Such technologies can be integrated into various AI applications, including privacy-sensitive visual aid devices, smart home assistants, wearable cameras, augmented reality platforms, surveillance systems, and live classroom environments.

## II. Related Work

### A. Contextual Foundations of Visual Privacy

Many privacy theories argue that human perception of privacy is both content- and context-dependent [21]. Rather than treating privacy as a static property of information, these theories highlight how people interpret its meaning, intent, and appropriateness in the moment. For example, contextual integrity theory argues that privacy is about whether information flows align with the social norms of a given context, such as who receives the information, what is being shared and how it is shared [20]. Similarly, boundary regulation [22] and privacy calculus [23], [24] treat privacy as a negotiation outcome of interpersonal boundaries with others and of perceived benefits of information disclosure. Empirical HCI research supports these theoretical perspectives, showing that users' information sharing decisions depend heavily on situational norms and social relationships. Prior work on visual privacy has explored, e.g., how user dispositions (e.g., demographics, personal traits), the aesthetics of the content (e.g., location, people), the intended audience, the presence of bystanders, and the surrounding environment in which a photo is taken can influence privacy perceptions [16], [17], [19], [25], [26]. Collectively, these findings indicate that visual

privacy judgments emerge from contextual signals and micro-details of the content. Our work builds on these foundations and empirical results by examining privacy perception under controlled manipulation of micro-details and contextual conditions. While prior work has focused mainly on whole image, we investigate how object-level cues and their interactions contribute to perceived privacy.

### B. Visual Privacy Risks and Protection

A wide range of privacy risks associated with visual content have been documented in the research literature. Such risks emerge from the distinct and recognizable elements contained in the image, often revealing more information than the sharer intends. Prior work has shown that photos can expose biometric or demographic details, geolocation, social relationships and status, or health and economic conditions [27], [28], [29]. Individuals who did not voluntarily participate in image creation (e.g., bystanders, passersby, or children) could also be exposed when the image is shared without their knowledge or consent [10], [11], [25], [30]. Privacy risks are further amplified by sensitive attributes inferred at scale from image content and metadata by modern data-harvesting systems [31]. These findings illustrate that privacy risks in images arise from inferences that can be drawn from how visual and contextual cues relate to each other within a scene.

To mitigate the risks mentioned above, prior work has explored privacy-enhancing technologies for visual content [32], [33], [34]. Technical solutions include automatic detection and obfuscation of sensitive details using blurring, redaction, and facial de-identification [18], [35], [36], [37]. On the other hand, user-centric solutions offer options to restrict the sharing of visual content to a specific set of people or to delegate privacy decisions to trusted assistants [13], [19], [30], [38]. However, these solutions treat all sensitive elements as uniformly risky, overlooking how the co-presence of multiple elements impacts users' privacy perception. The mismatch between existing protection mechanisms and human perception emphasizes the need for a deeper understanding of object-level interactions, which is the focus of our work.

### C. Visual Privacy Methodological Approaches

Research on visual privacy has traditionally relied on natural images collected from social media, photo-sharing platforms, or curated datasets. Prior studies have used such images in user studies, where participants are asked to report, e.g., their comfort level in sharing them with others, their intended audience, the control mechanisms they use, and the reasoning behind their decisions, which stem from participants' privacy preferences. Furthermore, many studies have leveraged photos provided by participants to investigate which types of content are considered sensitive. Researchers have also studied how the visibility of certain objects affects privacy judgments by obfuscating sensitive regions of the image before measuring participants' privacy perceptions [18], [39], [40]. Despite ecological validity and high-level insights, the main limitation of using natural images is the lack of control over modulating specific visual aspects. As a result, it is difficult to observe the role of individual foreground or background objects, their co-presence and interactions, or changes in the surrounding environment that shape perceived privacy. To overcome such limitations, synthetic images produced by modern generative models that offer the controlled manipulation of visual features can be a helpful approach. Recent HCI research has explored whether humans can differentiate between synthetic and real faces [41], [42], [43], [44]. Neurophysiological studies also demonstrate that synthetic images can approximate human perceptual judgments in controlled settings and motivate the use of synthetic stimuli in experimental research [45]. Building on this direction, our study employs carefully designed prompts to control the components of images during the image generation process. We utilize these synthetically generated images as stimuli in a user study aimed at investigating how object-level features and contextual factors shape privacy perception.

## III. Methodology

### A. Preliminaries

In line with prior work [10], [25], [46], we define the key concepts and their relationships as follows.

- **Object** denotes a bounded, semantically meaningful entity that belongs to a specific category and can be distinguished from other objects and the background. Visual objects (e.g., face, person, tree) are entities that can be recognized based on their visual appearance such as shape, texture, color, while textual objects (e.g., name, date) consist of symbolic representations (characters, words, phrases).
- **Privacy-sensitive object (PSO)** refers to an object that contains personally identifiable or sensitive information that owners may feel uncomfortable sharing on public platforms. A visual content generally consists of objects with different levels of sensitivity, along with the background. Objects may be identified as PSOs based on specific data protection regulations or visual indicators such as the surrounding context. As illustrated in Figure 1, the person in the center of the image and the nearby bystanders are marked as PSO (since they constitute personally identifiable information under GDPR), whereas the sky and the floor belong to the background. Other objects, such as trees or trash bins, can also be elevated to PSO when the goal is to infer the geographical location where the image was captured.
- **Foreground PSO** is the primary subject of interest and is typically located in the center of the visual content. In Figure 1, the person in the center is the foreground PSO and the bystanders are the background PSO.
- **Perceived privacy level (PPL)** is the degree to which users believe their personal information, activities, or beliefs are protected from unwanted observation, access, or misuse.
- **Comfortability level** is the degree of ease and safety experienced by an individual in a given setting. PPL and comfortability level are conceptually aligned, but they are inversely related: as the perceived privacy level increases, the comfortability level decreases.

Based on this terminology, we construct hypotheses as follows:
**H1** : The perceived privacy level of a foreground PSO increases when it is accompanied by a background PSO.
**H2** : The surrounding visual scene affects the perceived privacy level of the same PSOs present in the image.
**H3** : The co-presence of multiple background PSOs further elevates the perceived privacy level of a foreground PSO compared to when only a single background PSO is present.

### B. Study Design

*1) Environment Selection:* We considered two environments for the user study: a café and an office. They represent distinct social and professional contexts, and are communal spaces where photos may be taken. Privacy expectations are usually lower in cafés due to the sense of privacy through anonymity. In offices, clear roles and the handling of sensitive or private information can make people uncomfortable with taking and sharing photos on social networks.

*2) Foreground and Background PSOs:* To determine both foreground and background PSOs, we examined the subset of the VISPR dataset designed for image redaction (VISPR-Redacted [46]) and the VizWiz-Priv dataset [47]. VISPR-Redacted contains user uploaded, publicly available Flickr images and is curated for automatic detection of PSOs and redacting them by masking. VISPR-Redacted contains 24 labels, all marked as PSOs. VizWiz-Priv is a large-scale collection of real-world images captured by blind photographers and accompanied by questions and crowd-sourced answers. VizWiz-Priv includes 23 categories that annotators label as PSO. Our analysis revealed that both datasets include several identical labels, providing insights into PSOs that are commonly shared with others and online. We chose the three most common object categories from VizWiz-Priv as our foreground PSOs: **Face, Miscellaneous Paper and Computer/phone screen**. Each foreground PSO carry inherent sensitive information while also offering potential information for users:

1) **Face**: Visual identification of a person. Sharing a face can support social connection (sending it to friends), identity verification (online applications), or professional representation (LinkedIn profile, news).
2) **Miscellaneous Paper**: Documents such as tickets, forms, printouts, or receipts. These may contain private information (e.g., names, addresses, birthdates, signatures), but are often shared for practical purposes such as proof of purchase, reimbursement, or customer support.
3) **Computer/phone screen**: Digital content displayed on electronic devices. Screens may reveal sensitive information (e.g., usernames, phone numbers, emails), but screenshots are frequently shared for collaboration or troubleshooting purposes.

For each foreground PSO, we identified five background PSOs through an internal expert discussion on both datasets, considering diversity in modality (visual vs. textual), potential sensitivity, and their frequency of being together with foreground PSOs. Our set of foreground/background PSO combinations is presented in Table I.

TABLE I: List of Foreground and Background PSOs.

| Foreground PSO | Background PSOs |
|---|---|
| Face | Face (another, a.), Poster, Medicine, Tattoo, Landmark |
| Miscellaneous Paper | Face (photo, p.), Full name, Address, Birth date, Signature |
| Computer/phone Screen | Face (reflection, r.), Date, E-mail, Username, Phone number |

*3) Image Generation:* We deliberately avoided real images to prevent participants' judgments from being influenced by uncontrolled factors such as inconsistent lighting, backgrounds, or photographic context. Instead, we relied on synthesized images to keep visual conditions consistent across variations, allowing participants to focus on the intended differences between foreground and background PSOs.

We used OpenAI's SORA text-to-image model [2] to generate all images. For images containing only a foreground PSO, we designed comprehensive prompts to produce realistic and contextually meaningful scenes. To maintain visual consistency, we applied SORA's Remix functionality: instead of regenerating an entire image, we selected specific regions and instructed the model to add the required background PSO within that context. This approach preserved lighting, perspective, and composition under all conditions. The generated images did not deviate significantly from each other, so the focus remains on PSOs. We used a male subject for the office environment and a female subject for the café. The gender assignments are random and are designed solely to provide variation across the environments. It does not convey or reinforce any potential gendered association biases. Figure 2 shows examples from both environments. The top row starts with the base café image containing only the face foreground PSO, followed by versions where medicine and then landmark are added as background PSOs. The bottom row starts with the base office image, followed by versions where the tattoo and then an additional face (a.) are added as background PSOs. The prompts we used for image generation are provided in Appendix A.

For each foreground PSO, we generated images for three cases: (a) the foreground PSO alone (1 condition), (b) the foreground PSO individually paired with each of its five background PSOs (5 conditions), and (c) the foreground PSO combined with every possible pair of background PSOs ($\binom{5}{2} = 10$ conditions). This yields $1 + 5 + 10 = 16$ image conditions per foreground PSO. With three foreground PSOs, this corresponds to $3 \times 16 = 48$ images per environment, which means that in total $48 \times 2 = 96$ images were generated for the two versions of the survey.

*4) Branch Logic Design:* Requiring participants to evaluate 48 images could lead to participant fatigue, reduced engagement, and unreliable responses due to rushed decision making. To mitigate this, we implemented branching logic that routed participants into different survey flows, depending on how

[2]https://sora.chatgpt.com/


(a) Café: Face only (base image) (b) Face + Medicine (c) Face + Medicine + Landmark

(d) Office: Face only (base image) (e) Face + Tattoo (f) Face + Tattoo + Face (a.)

Fig. 2: Illustrative examples of image generation in café (top) and office (bottom) environments. Each sequence progresses from a face only foreground PSO to combinations with additional background PSOs.

they ranked their comfortability levels when images included background PSOs. Instead of rating all possible combinations, the participants began by ranking the five background PSOs according to how strongly they affected the comfortability level of the foreground PSO. Subsequently, only those combinations involving the background PSO with the lowest effect on the foreground PSO's perceived privacy level (PPL) were shown. As a result, participants rated $1 + 5 + 4 = 10$ images per foreground PSO and 30 images in total. Each participant views identical $3 \times (1 + 5) = 18$ images from the same environment, while the last 12 differ due to branching. This approach also avoided redundant evaluation: If the PPL of a foreground PSO is highest when paired with a certain background PSO, then requesting participants to reassess it alongside other background PSOs becomes redundant, since the foreground PSO is already perceived as the most sensitive across all pairings. Appendix B shows how the branch logic is implemented when the environment is café, the foreground PSO is face, and the landmark is chosen by the background PSO with the lowest effect.

### C. Study Practicalities

*1) Survey Organization:* The first page of the survey contains the informed consent form, explaining the general objective of the study, how the data will be collected and processed, and compliance with GDPR. Proceeding the survey requires the confirmation of all mandatory consent statements, and an optional checkbox allows entry into a lottery for a movie ticket. Once consent is obtained, participants respond to demographic questions and questions about their social media habits and privacy awareness. The privacy awareness questions included four brief items to understand individual privacy preferences in general. Following the approach of Hoyle et al. [19], we opted for a short scale with minimal burden on respondents rather than a full psychometric scale such as the IUPUC [48]. Following this, participants complete three sections, each focusing on a different foreground PSO. In total, the survey contains 50 mandatory questions, except for the optional open-text fields. We should note that we do not evaluate whether individuals with stronger privacy preferences are more likely to perceive PSOs as private (i.e., less comfortable sharing them online). Our focus is on the *effect of context* rather than individual privacy awareness. Previous work [19] has shown that higher privacy awareness is often associated with perceiving visual content, and attributes shape information sharing behaviors [49]. Nevertheless, we acknowledge that the reported comfortability levels may vary depending on the privacy awareness of the participants. Individuals with stronger privacy concerns might rate PSOs as less comfortable to share, while those with lower awareness may perceive the same objects as less sensitive.

In our user study, each section begins with an image that

displays a single foreground PSO, and participants are asked about their comfortability level of sharing this object. The initial question is necessary to obtain a baseline perceived privacy level (PPL). The participants then view a row of images showing the same foreground PSO that is paired with a single background PSO different for each image, and are asked for the comfortability level for the same foreground PSO. They also rank the effect of background PSO on the degree of change and are asked about the rationale behind their ranking choice (optional open-text answer). The branch logic design is utilized according to their ranking. In the final stage, participants view a row of images including the same foreground PSOs, the background PSO ranked with the lowest decrease in their comfortability level (lowest PPL effect) paired with the remaining background PSOs. The final stage also includes an optional question asking to describe whether and in what way the lowest-ranked background PSOs influenced the comfortability level of the foreground PSO when combined with other background PSOs.

All ratings used a 5-point Likert scale, where 1 indicated "not comfortable at all" and 5 "very comfortable". We asked for comfortability level instead of PPL since it is easier for participants to interpret while still naturally capturing the perceived privacy. Table IX in Appendix C shows the inverse mapping between the comfortability level and PPL. The complete survey questionnaire is provided in the Appendix B.

*2) Survey Deployment:* Based on a careful review of the data storage policies, customizability, and control logic offered by different survey platforms, we selected Streamlit[3] to implement the survey from scratch. We deployed the survey online and provided participants with a shared link to access it. Streamlit stores responses locally during completion and sends them to a designated email address upon submission. We downloaded these responses to a local machine for analysis.

*3) Participant Recruitment and Demographics:* Participants were recruited using a chain-referral (snowball) sampling approach. We initially distributed the survey link through our personal contacts and social media channels, reaching 73 individuals, and encouraged them to share it further within their own networks. In total, 109 participants completed the survey, with 61 assigned to the café version and 48 to the office version. After excluding responses that showed inconsistencies between ratings and rankings, 92 valid responses remained (51 café and 41 office). Participants were compensated with movie tickets through voluntary participation in a raffle.

Table X shows the demographic distribution of the participants. The participants were balanced in sex (51% female, 47% male) and predominantly White/Caucasian (63%) or Asian (22%). Most of the participants' age was in the range $25-34$ (35%) or $45-54$ (32%), with smaller groups in the ranges $18-24$ (20%), $35-44$ (10%) and $55+$ (4%). Regarding education, the majority had a bachelor's degree (35%) or a master's degree (32%), while a quarter (26%) had a doctorate. More than half of the participants were employed full-time (57%), and students made up 30%. Social media usage varied: 37% reported sometimes, 36% rarely, and only 2% daily usage.

[3]https://streamlit.io/

### D. Analysis overview

*1) Quantitative Analysis:* To evaluate **H1**, we used the non-parametric Wilcoxon signed-rank test, since our design compares paired measurements of the same foreground PSO with and without background PSO (repeated measure with post intervention). The null hypothesis **H1** is "There is **no** difference between the perceived privacy level of a foreground PSO when it appears alone versus when accompanied by a background PSO". To test **H2**, we compared the comfortability scores between different environments using the non-parametric Mann-Whitney U test, since each participant rates the same foreground PSO only in one of the environments (café vs. office as independent variable). The null hypothesis for **H2** is "The distributions of perceived privacy levels are the same for café and office". For **H3**, we did not perform statistical testing, as the subset of participants who answered each combination question varied by individual rankings, making group-level inference unreliable (less number of repeated measures). Instead, we report the mean change in comfortability level and the proportion of participants who changed their comfortability level when two background PSOs were present. In addition to these tests, we used the Mann-Whitney U test (with single categories) to understand whether demographics influence perceived privacy levels. To test factors with more than two categories, including age group, profession, and educational level, we used the Kruskal–Wallis H test.

*2) Qualitative Analysis:* We conducted a qualitative analysis of the open-text responses from the survey questionnaire using inductive, in-vivo coding followed by thematic clustering to group related codes into higher-order themes [50], [51]. First, the author with an HCI background performed an independent review of the responses to get acquainted with the data using memoing and to generate the initial list of codes. Then, the author iteratively reviewed the initial codes along with the memos to deduce themes that could represent users' cognition or behaviour while dealing with visual privacy. This process was repeated until saturation was reached, with no further codes and themes or sub-themes emerging. Finally, the author drafted a codebook along with the definitions, inclusion, and exclusion criteria. The codebook was then reviewed to refine the wording of codes, their definitions, and thematic categories. The final codebook was reviewed once again to ensure that it resonated with the research questions and represented the survey data. Two authors then used the codebook to code all individual responses independently. Since the participants provided their responses as a summary of their cognitive walkthrough during our study, it is possible to tag the responses with multiple codes. Due to this overlap, the coders were allowed to use up to three codes per response. To assess reliability at the theme level, we collapsed the codes into their respective themes. We quantified agreement among coders using Krippendorff's alpha as the inter-rating reliability (IRR) measure due to its suitability [52]. We found the IRR to

TABLE II: Responses to privacy awareness questions (%) and mean value of the Likert scale. (**SD** = Strongly Disagree (1), **SWD** = Somewhat Disagree (2), **N** = Neutral (3), **SWA** = Somewhat Agree (4), **SA** = Strongly Agree (5)).

| Question | SD | SWD | N | SWA | SA | Mean |
|---|---|---|---|---|---|---|
| Q1: I am concerned about my privacy online | 1% | 1% | 8% | 30% | 60% | 4.47 |
| Q2: I am concerned about my privacy in everyday life | 2% | 7% | 14% | 32% | 46% | 4.12 |
| Q3: It bothers me to give personal information to so many online companies | 1% | 1% | 4% | 30% | 64% | 4.52 |
| Q4: When I share a photo in social media, I check whether the picture contains personal information about me | 8% | 10% | 8% | 24% | 50% | 4.00 |

be 0.891, which indicates that coders consistently identified the same overarching themes and a strong agreement at the theme level, supporting the reliability of our thematic analysis.

### *E. Study Ethics*

This study was conducted in accordance with regional privacy compliance and well-established best practice guidelines for user studies [53], [54], [55]. Before the actual survey began, the participants were presented with information about the use of study results and the participation reward terms. The participation was voluntary, and we sought explicit consent from each participant who attempted the survey. The consent and privacy policy included in our study was drafted and provided by the data privacy regulation unit of our institution. A high-level privacy impact assessment was also conducted to review the study methodology and data to be collected to ensure ethical treatment of sensitive data. We ensured that personally identifiable information was solely used for contacting the participants and excluded from the analysis. We used an open-source, GDPR-compliant tool to build and host our study. All data is stored on EU-based servers under our control and handled in accordance with strict data protection and deletion practices. The images used in our study are purely illustrative and do not depict real human subjects.

## IV. Results

Before analyzing the results, the responses that showed clear inconsistencies between the rankings and ratings were excluded from the dataset. Inconsistency refers to instances where a participant's assessment of the comfortability level concerning a foreground PSO, when there is a single background PSO, conflicts with the subsequent ranking question. This method also allowed us to filter out inattentive participants, thereby improving the quality of the remaining data.

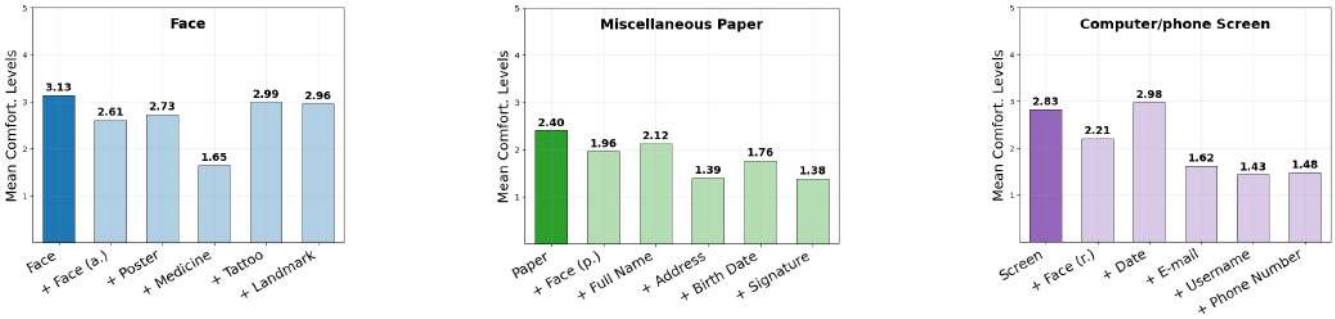
### *A. Effect of Users' Privacy Attitudes*

Table II presents the participants' responses to questions concerning privacy awareness. Concern about online privacy (Q1, 90% agreed) and discomfort with the disclosure of personal information to online companies (Q3, 94% agreed) received the highest ratings. Concern about privacy in daily life (Q2, 78% agreed) was also significant but slightly lower overall. From the responses, we inferred that the majority of the participants expressed their concerns about their privacy online, in everyday life, and with the companies. The responses to (Q4) show that the participants' ratings of how often they check personal information before sharing a photo on social media were lower than their ratings of concern for privacy online. This indicates that while most participants express concern about online privacy, this concern does not consistently translate into proactive behaviors, including looking for personal information before sharing it on social media, highlighting a gap between privacy attitudes and practices.

### *B. Effect of Background PSOs (H1)*

To examine **H1**, we quantitatively compared comfortability levels and averaged them using both environments. Figure 3 illustrates how the presence of background PSO influences the comfortability level (the perceived privacy level, PPL) of each foreground PSO. In each figure, the first bar indicates the baseline comfortability level when the image contains only the foreground PSO, while the subsequent bars represent its combination with different background PSOs. For **Face**, the strongest reduction occurs with *medicine* (mean = 1.65; –1.48 from the baseline of 3.13), followed by *face (a.)* (2.61; –0.52). In contrast, *tattoo* (2.99) and *landmark* (2.96) produce minor decreases. For **Miscellaneous Paper**, *full name* shows the smallest drop (2.12; $-0.28$), whereas *address* (1.39) and *signature* (1.38) yield the largest decreases. For **Computer/phone Screen**, identifiers such as *email* (1.62), *username* (1.43), and *phone number* (1.48) lead to strong reductions, *face (r.)* causes a moderate decrease (2.21). Interestingly *date* stands out as the only case associated with an increase. A possible reason for this might be the averaging of rankings from both settings, which influences the participants' judgements. Overall, the addition of background PSOs mostly elevates the PPL of the foreground PSO, with certain categories (e.g., medicine for Face, signature for Miscellaneous Paper, username for Computer/phone Screen) exerting the most pronounced effects.

Figure 3 shows only mean values and does not capture the underlying distributions. To systematically examine whether observed differences were consistent, we compared the comfortability levels of each foreground PSO alone with their corresponding foreground/background PSO pair using the Wilcoxon signed-rank test. Table III shows that the presence of background PSOs often reduced the comfortability level, indicating an increase in perceived privacy level (PPL). For **Face**, the addition of *face (a.)* significantly increased PPL in the office but not in the café, suggesting that the effect of background PSO matters more in professional contexts. *Medicine* strongly increased PPL in both environments, while *tattoo* and *landmark* had no significant effect. For **Miscellaneous Paper**, *address, birth date*, and *signature* consistently




(a) Face (b) Miscellaneous Paper (c) Computer/phone Screen

Fig. 3: Average comfortability level ratings for foreground PSOs and the effect of a single background PSO.

TABLE III: Wilcoxon signed-rank test results: Change in comfortability level ($\Delta$ mean) when adding a background PSO. Significant $p$-values ($< 0.05$) are highlighted in **bold and blue**.

| Foreground PSO | Background PSO | Café ($\Delta$, $p$) | Office ($\Delta$, $p$) | Significance |
|---|---|---|---|---|
| Face | Face (a.) | -0.37 (0.0576) | -0.71 (**0.0003**) | Only Office |
| | Poster | -0.55 (**0.0345**) | -0.22 (0.2193) | Only Café |
| | Medicine | -1.78 (**0.0000**) | -1.10 (**0.0000**) | Both |
| | Tattoo | -0.22 (0.4359) | -0.05 (0.6917) | None |
| | Landmark | -0.16 (0.4115) | -0.20 (0.1895) | None |
| Miscellaneous Paper | Face (p.) | -0.33 (0.0815) | -0.59 (**0.0049**) | Only Office |
| | Full Name | -0.25 (0.1256) | -0.32 (0.0920) | None |
| | Address | -1.22 (**0.0000**) | -0.76 (**0.0006**) | Both |
| | Birth Date | -0.57 (**0.0039**) | -0.73 (**0.0012**) | Both |
| | Signature | -1.16 (**0.0000**) | -0.85 (**0.0001**) | Both |
| Computer/phone Screen | Face (r.) | -0.47 (**0.0165**) | -0.80 (**0.0001**) | Both |
| | Date | +0.25 (0.0849) | +0.02 (0.7181) | None |
| | E-mail | -1.37 (**0.0000**) | -1.00 (**0.0005**) | Both |
| | Username | -1.57 (**0.0000**) | -1.17 (**0.0000**) | Both |
| | Phone Number | -1.59 (**0.0000**) | -1.05 (**0.0001**) | Both |

raised PPL across both environments. *Face (p)* increased PPL only in office, while *full name* had no significant effect. For **Computer/phone Screen**, nearly all background PSOs increased PPL, except *date*, which has no effect.

Our analysis shows that **not all background PSOs equally affect perceived privacy**. Highly sensitive cues (e.g., medicine, addresses, signatures, digital identifiers on screens) consistently amplify the PPL of foreground PSOs, while more ambiguous cues (e.g., tattoos, landmarks, dates) are often ignored. This pattern reflects the behavior of everyday social networks, where users avoid sharing sensitive explicit information such as medicine or ID cards, but tend to underestimate the risks posed by ambigious cues that can be exploited in inference attacks such as social engineering or identity linking.

### C. Effect of Environment (H2)

To evaluate H2, we first compared the average comfortability levels between environments. The comfortability level was consistently lower in office settings than in café, with the strongest drop observed for **Face** as a foreground PSO (Face: $-0.67$; Miscellaneous Paper: $-0.37$; Computer/phone Screen: $-0.31$). To systematically assess these differences, we applied the Mann–Whitney U test. As shown in Table IV, participants reported significantly lower comfortability (i.e., higher perceived privacy level, PPL) in office settings across multiple foreground/background PSO pairs. The effect was especially pronounced for pairs that involve the face as a single foreground PSO ($p = 0.0062$), face/face(a.) ($p < 0.001$), face/tattoo ($p = 0.0261$), and face/landmark ($p = 0.0032$); where office settings consistently amplified PPL. In contrast, paper-based PSOs (e.g., birthdate, face(p.)) yielded lower overall comfortability levels but smaller differences between environments. The violin plots presented in Figure 8 (Appendix C) strengthen the analysis of H2 by visually illustrating the underlying distributional patterns. Across all eight statistically significant pairings, participants consistently reported lower comfortability level in the office setting compared to the café, reaffirming the context sensitivity of perceived privacy. Figure 8 also highlights changes in distribution spread, indicating a greater consensus on discomfort in office environments.

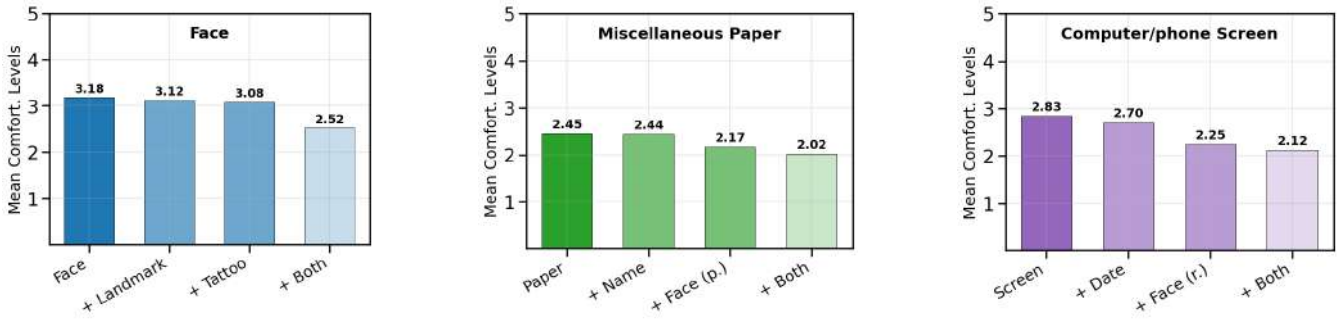
These results suggest that not all PPLs of PSOs are equally shaped by the environmental context. Highly identifiable cues, such as faces, are perceived particularly private in professional settings, where co-presence may further amplify privacy concerns. In contrast, more document-like PSOs show consistently low comfortability regardless of the environment. The violin plots in Figure 8 add nuance to this interpretation by revealing how comfortability levels are lower in average in office set-

TABLE IV: Mann-Whitney U test results comparing comfortability levels between café and office environments. Positive ΔMean values indicate a higher average comfortability in the café, while negative values indicate a higher comfortability in the office. Significant $p$-values are highlighted in **bold and blue**.

| **Face** | | | **Miscellaneous Paper** | | | **Computer/phone Screen** | | |
|---|---|---|---|---|---|---|---|---|
| Background PSO | ΔMean | $p$-value | Background PSO | ΔMean | $p$-value | Background PSO | ΔMean | $p$-value |
| None | +0.81 | **0.0062** | None | +0.42 | 0.1193 | None | +0.43 | 0.0722 |
| Face (a.) | +1.14 | **0.0000** | Face (p.) | +0.67 | **0.0152** | Face (r.) | +0.77 | **0.0098** |
| Poster | +0.48 | 0.0518 | Full Name | +0.48 | 0.1549 | Date | +0.66 | **0.0057** |
| Medicine | +0.12 | 0.4519 | Address | -0.04 | 0.9488 | Email | +0.06 | 0.7789 |
| Tattoo | +0.64 | **0.0261** | Birth Date | +0.58 | **0.0043** | Username | +0.04 | 0.7930 |
| Landmark | +0.85 | **0.0032** | Signature | +0.11 | 0.2426 | Phone | -0.11 | 0.4312 |

TABLE V: Background PSOs rated as having the least effect on comfortability level for each foreground PSO. Values indicate counts with percentages for café ($n = 51$) and office ($n = 41$). For each environment and foreground PSO, the background PSO most frequently selected is highlighted in **bold and blue**.

| **Face** | Café / Office | **Miscellaneous Paper** | Café / Office | **Computer/p. Screen** | Café / Office |
|---|---|---|---|---|---|
| Face (a.) | 13 (26%) / 8 (20%) | Face (p.) | 15 (29%) / 6 (15%) | Face (r.) | 13 (26%) / 4 (10%) |
| Poster | 9 (18%) / 10 (24%) | Full Name | 12 (24%) / **19 (46%)** | Date | **36 (71%)** / **32 (78%)** |
| Medicine | – (–%) / 2 (5%) | Address | 4 (8%) / 2 (5%) | E-mail | – (–%) / 1 (2%) |
| Tattoo | 11 (22%) / **10 (24%)** | Birth Date | **16 (31%)** / 6 (15%) | Username | 2 (4%) / 2 (5%) |
| Landmark | **18 (35%)** / 11 (27%) | Signature | 4 (8%) / 8 (20%) | Phone Number | – (–%) / 2 (5%) |




(a) Face (b) Miscellaneous Paper (c) Computer/phone Screen

Fig. 4: Average comfortability level ratings for each foreground PSO, showing the baseline, the effect of the two background PSO most often rated as having the lowest effect when alone (see Table V), and the effect of co-presence with both background PSOs present in the image (**both**).

tings, and more tightly distributed, indicating stronger agreement among participants. In conclusion, the context amplifies perceived privacy levels, and sensitivity is affected not only by single objects but also by their combinations and settings. This strengthens the claim that privacy-aware systems must move beyond binary recognition to incorporate compositional object definitions and contextual awareness.

### *D. Effect of Co-Presence (H3)*

We evaluated H3 by testing whether the co-presence of background PSOs further increases the perceived privacy level (PPL) of a foreground PSO compared to the presence of a single background PSO. To avoid survey fatigue by rating all possible combinations, we adopted a branching procedure: each participant first identified the background PSO that had the lowest effect on a given foreground PSO, and this "least effective" background PSO was paired with each remaining background PSO for the same foreground PSO. Table V reports how often each background PSO was assessed as the least effective, determining the combinations evaluated. The resulting selection imbalance made formal statistical testing approaches inappropriate. Therefore, we report two complementary quantitative measures: (1) the mean change in the comfortability level when a second background PSO is added to the image and (2) the proportion of participants whose comfortability level decreased after this addition.

Figure 4 illustrates the magnitude of mean changes when two least effective background PSOs (extracted from Table V) are present in the image, labeled "both". Table VI reports the proportion of participants who decreased their comfortability level when they observed two background PSOs. Both results converged to the same pattern: a small subset of PSO pairs consistently decreased the comfortability level (amplified perceived privacy level) beyond their single-object effects. For

TABLE VI: Co-presence effects of background/background PSO pairs on perceived privacy levels for the foreground PSO (Face, Miscellaneous Paper, Computer/phone Screen). $n$ denotes the number of participants who rated the comfortability levels for a given pair. The % Decrease column shows the proportion of these participants who rated a lower comfortability level than images where each background PSO is shown separately, highlighting cases where co-presence amplifies privacy concerns.

| **Face** | | | **Miscellaneous Paper** | | | **Computer/phone Screen** | | |
|---|---|---|---|---|---|---|---|---|
| Pair | n | % Decrease | Pair | n | % Decrease | Pair | n | % Decrease |
| poster/tattoo | 40 | 37.5 | full name/face (p.) | 52 | 17.3 | e-mail/username | 5 | 60.0 |
| landmark/tattoo | 50 | 28.0 | birthdate/face (p.) | 43 | 16.3 | phone number/username | 6 | 33.3 |
| face (a.)/poster | 40 | 22.5 | address/full name | 37 | 13.5 | face/username | 21 | 23.8 |
| landmark/poster | 48 | 20.8 | birthdate/full name | 53 | 13.2 | date/e.mail | 69 | 18.8 |
| face (a.)/landmark | 50 | 20.0 | birthdate/signature | 34 | 11.8 | face/phone number | 19 | 15.8 |
| landmark/medicine | 31 | 19.4 | full name/signature | 43 | 11.6 | date/face (r.) | 85 | 14.1 |
| medicine/poster | 21 | 19.0 | address/birthdate | 28 | 10.7 | e-mail/face (r.) | 18 | 11.1 |
| medicine/tattoo | 23 | 17.4 | photo/signature | 33 | 9.1 | date/phone number | 70 | 8.6 |
| face (a.)/tattoo | 42 | 16.7 | address/face (p.) | 27 | 7.4 | date/username | 72 | 2.8 |
| face (a.)/medicine | 23 | 13.0 | address/signature | 18 | 5.6 | e-mail/phone number | 3 | 0.0 |

TABLE VII: Dominance effects of background PSOs on foreground PSOs (Face, Miscellaneous Paper, Computer/phone Screen) during co-presence with other background PSOs. Columns: **Background PSO** = background privacy sensitive object co-present with other background PSOs; **N** = number of co-presence ratings; **D** = number of dominance cases; **%D** = proportion of dominance cases (D/N).

| **Face** | | | | **Miscellaneous Paper** | | | | **Computer/phone Screen** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Background PSO | N | D | %D | Background PSO | N | D | %D | Background PSO | N | D | %D |
| Medicine | 98 | 64 | 65.3 | Address | 110 | 36 | 32.7 | Username | 104 | 61 | 58.7 |
| Poster | 149 | 40 | 26.8 | Signature | 128 | 41 | 32.0 | Phone number | 98 | 52 | 53.1 |
| Face (a.) | 155 | 38 | 24.5 | Face (p.) | 155 | 25 | 16.1 | E-mail | 95 | 45 | 47.4 |
| Landmark | 179 | 39 | 21.8 | Birth Date | 158 | 24 | 15.2 | Face (r.) | 143 | 35 | 24.5 |
| Tattoo | 155 | 27 | 17.4 | Full Name | 185 | 20 | 10.8 | Date | 296 | 17 | 5.7 |

example, the co-presence of landmark/tattoo produced a considerable average drop in comfortability level (0.66) and the co-presence reduced the willingness to share the foreground PSO for many participants. Pairs such as *poster/tattoo* and *landmark/tattoo* repeatedly ranked among the most impactful, with other notable combinations including *e-mail/username* and *phone number/username* on the foreground PSO **Computer/phone Screen**. Most of the other co-presences exhibited only minor effects.

To further investigate co-presence, we examined whether particular background PSOs exhibit a dominance effect. A dominance effect arises when multiple background PSOs are presented simultaneously, but the participant's reported comfort level aligned almost exclusively with the more influential one. Table VII presents a summary of these findings. For the **Face** foreground PSO, *medicine* dominated almost two-thirds of the cases (65.3%), indicating that the participants largely ignored the other background PSO where *medicine* was present. Similarly, for **Miscellaneous Paper**, *address* (32.7%) and *signature* (32.0%) often dominated the influence of other background PSOs. For **Computer/phone Screen**, identifiers such as *username* (58.7%), *phone number* (53.1%) and *e-mail* (47.4%) showed strong dominance, while *date* (5.7%) rarely dominated other background PSOs. Importantly, lower $N$ values in Table VII indicate that more participants initially considered these PSOs to be relatively more effective on their own, making their strong dominance effects even more notable. For example, *medicine* was often chosen as the most effective background PSO when in isolation and overwhelmingly dominated the participant's judgment when paired with others.

Our findings show that some PSOs act as **primary drivers of perceived privacy risk**, overshadowing other co-present cues. This suggests that privacy-aware systems should prioritize flagging dominant cues since these alone often drive users' judgments rather than treating every cue equally, which is less critical for achieving better usability.

**Demographic Effects:** We also examined whether demographic factors influenced privacy perceptions. Significant effects are summarized in Table XI in Appendix C. In general, gender effects were the most present, with female participants reporting higher comfortability levels, while other demographic factors showed more isolated differences. Our results suggest that privacy-aware systems may benefit from considering demographic variability, particularly when tailoring defaults for awareness mechanisms.

### *E. Qualitative Insights*

Qualitative thematic analysis (refer to Section III-D2) of responses to open-ended survey questions yielded ten codes spanning across three discrete themes. The refined codebook is shown in Table VIII. Our results indicate that participants have a latent cognitive model when self-evaluating the privacy of visual content that comprises multiple sensitive elements.

TABLE VIII: Thematic analysis results.

| Theme | Code | Definition |
|---|---|---|
| Perceived Privacy Norms | Social (media) norms | Participants feel safer sharing when attention is distributed or others are present. |
| | Need for consent | Participants seek permission before posting others to respect privacy and consent. |
| | Tolerance for incremental exposure | Disclosure risk is perceived as low when similar information is already public, reducing reluctance to incrementally share more. |
| Inference & Linkability | Contamination risks | Concerns about being associated with unrelated or unwanted ideological affiliations that could create false reputation. |
| | Spatio-temporal pinpointing | Concerns about the combination of location and time information from visual content. |
| | Temporal unlinkability | Concerns about time-based linkage or exposure. |
| | Aggregation risks | Risk multiplies when multiple identifiers combine, enabling identity theft or profiling even if each item alone seems safe. |
| Irreversible Harms | Uniqueness | Concerns about unique features affecting personal privacy. |
| | Stigmas | Certain sensitive information is perceived as categorically too risky, as their exposure leads to stigma, discrimination, or fraud. |
| | Threat actors | Concerns about potential adversaries and their capabilities. |

In particular, the identified themes depict a layered model with heuristics, deeper reasoning, and consequence weighing as follows: First, the participants have mental shortcuts and norms (such as "*Everyone does it this way; So, it is fine!*") as comfort heuristics. If such heuristics raise a red flag, they dig deeper into inference (e.g., "*What if someone figures out more?*") and potential consequences (e.g., "*Would that be dangerous?*").

**Perceived Privacy Norms:** (See quotes Q1 & Q2) This theme explores the comfort heuristics inferred by participants based on their interpretation of social expectations, consent norms, and perceived acceptability while sharing photos online.

> ***Q1:*** *..... if there's someone else in the photo I might feel more comfortable sharing rather than being just me. .....*

This theme's codes included instances where the participants mentioned the co-presence of other individuals and situations requiring mutual consent for the photo to be shared online. The codes also covered scenarios where the public availability of sensitive information reduced privacy concerns for revealing additional data. We excluded quotes related to non-human objects.

> ***Q2:*** *..... I usually post other humans when it is some social event, like a party or celebration, so by default everyone is aware pictures are taken and they usually say if they don't like them so they don't want them posted .....*

**Inference and Linkability:** (See quotes Q3 & Q4) This theme captures a deeper reasoning by a user about how information in an image can reveal hidden attributes or be linked across datasets to identify, profile, or de-anonymize themselves or others present in the shared image.

> ***Q3:*** *..... Poster can contain certain propaganda that I do not affiliate myself with, so I wouldn't want it showing up. .....*

The underlying codes of this theme capture scenarios of risks related to being associated with unrelated topics or the combination of multiple Personally Identifiable Information (PII) in the photo that reveal more than intended. Furthermore, they also included concerns about the disclosure of real-time locations directly through the cues in the shared photo or indirectly through the metadata. Some codes also reflect ad-hoc strategies employed by participants to mitigate the aforementioned risks.

> ***Q4:*** *..... A combination of my (full) name plus all the other would be considered an information breach for me and I would not feel comfortable of people that I am not close with (as is the case in social media) knowing all this stuff about me plus it would create a high risk .....*

**Irreversible Harms:** (See quote Q5) This theme captures specific visual objects whose disclosure can cause long-lasting harms that cannot be easily remediated. The codes reflect instances where the participant expresses concerns about privacy risks associated with disclosure of, for example, distinctive physical attributes (e.g., tattoos or birthmarks) or health conditions. The codes also covered responses that mention well-known cyber-threat actors and the permanent consequences they could cause. General privacy concerns and non-sensitive information leaks were excluded from this theme.

> ***Q5:*** *..... Address is also very personal, especially to females, due to possibilities of stalkers, kidnappers, or robbers. Birthdate can be used for some type of fraud as well, given that in many countries the personal code contains birthday date.....*

In summary, the results of the qualitative analysis emphasize various aspects of user mental models for visual privacy self-evaluation. The *Perceived Privacy Norms* theme reflects ad-hoc strategies for managing comfort. *Inference and Linkability* captures the risk assessment. The *Irreversibility Harms* theme reflects on the potential dangers if the risk is actualized.

## V. Discussion

One of our key observations is that users' privacy perceptions do not always translate into privacy behavior or user actions. For example, the results from the privacy awareness questions (Table II) show that the participants expressed general concern about online privacy, but not all examined the photos for personal information before sharing. Qualitative data from the survey also displays several instances of privacy awareness among participants, which appears to have been formed through public news media debates around privacy concerns and mandatory training at the workplace and edu-

cational institutions. Despite the awareness, users often fail to assess the privacy risks or control their behavior while sharing visual content on online platforms [56], [57], [58]. The lack of proactive practices highlights that current systems fail to bridge the gap between users' mental models and actions.

The complexity of privacy–utility tradeoffs further contributes to this gap. Usually, foreground PSOs carry inherent sensitivity. However, people may choose to share them because of the tangible benefits they provide, such as identity verification, professional collaboration, or social connection. Our results show that the perceived privacy risks associated with these PSOs are not fixed but dynamically reshaped by the presence of background PSOs. For example, a selfie becomes more sensitive when medicine is visible, a document becomes more risky to share when a signature is present, and a screenshot becomes problematic when the username or phone number is exposed. Such contextual amplification indicates that privacy–utility tradeoffs, especially in the case of visual contents, are a rather complicated process beyond a simple binary choice. The complexity in privacy decision-making arises from users' attempts to weigh multiple contextual factors and engage in multidimensional self-negotiation for the tradeoffs.

These observations emphasize the need for novel technical interventions and research opportunities to explore the notion of context-aware privacy. In this realm, the hypothesis evaluation and results from our study provide insight into the design principles and required characteristics of a context-aware privacy system. From a system design point of view, such a system should avoid uniform treatment of visual elements and adapt privacy sensitivity based on contextual cues. Also, the design should consider two broad categories of contextual cues: (i) subtle, latent cues (e.g., religious symbols or political affiliations) that are hard to detect, and (ii) categorically sensitive elements (e.g., medicine) that have a dominance effect by overriding other cues and disproportionately influencing user perceptions, as users often base their privacy judgments on such cues instead of the full context. Moreover, we observed that the co-presence of certain visual elements can lead to even higher perceived privacy risks. Thus, we argue that privacy-aware system design benefits from integrating object-level detection with contextual inference that accounts for the dominance and co-presence of visual elements. Our recent work follows up on this idea by demonstrating its feasibility through an ML-assisted access control system for visual data [59].

From an HCI design perspective, privacy-aware systems should provide automated assistance and fine-grained control to users. The assistance can be provided in the form of nudges, via visual highlighting and prompts, that guide users towards low-burden, privacy-oriented actions. Alternatively, assistance can also be provided through the automatic detection of highly sensitive objects or contextual cues in the background that could amplify the perception of privacy. Automatic assistance should also suggest appropriate privacy controls, allowing users to selectively obfuscate specific sensitive objects of the image while retaining the utility of the image and preserving privacy in its redacted form. Within this context, we argue that a human-centered design approach can assist users in translating their privacy perceptions into concrete actions, reducing cognitive load and improving decision-making.

Existing online social media and instant communication platforms, which deal with user-generated visual content, largely lack user assistance and nuanced controls for privacy. The privacy settings for the user accounts offered by some of these platforms fail to address the risks highlighted in our work. The results and discussions of our work can provide actionable insights to integrate visual privacy protection components. These insights can also guide usable system design themes of research works and development of future technologies that deliver personalized privacy protection.

### A. Limitations and Future Work

This subsection discusses the limitations of our work in terms of methodological trade-offs and factors affecting generalizability, which may constrain the external validity of our results, as well as outline future research directions.

Most of the participants in our study identify themselves as White/Caucasian, highly educated, younger and mid-career adults. This skewed demographic sample may limit the generalizability of our results regarding cultural and personal background diversity, as such factors shape users' privacy awareness and perceptions. Likewise, although we used a representative set of privacy-sensitive objects, this finite set may not capture the full diversity or combinations of objects encountered in the wild, and our findings may apply to real-world scenarios only to a certain extent. Future work should include more diverse participants and broaden the scope of objects to capture the complexity of everyday contexts better.

Methodologically, we relied mainly on synthetically generated images to eliminate possible external effects on perceived privacy. While generative AI is useful in HCI research and we instructed participants to imagine themselves as the subject or photographer, artificial images may not evoke the same cognitive responses as real ones. On the other hand, we studied privacy perception with at most two objects, whereas real-world visual content contains higher-order combinations; examining these could yield more detailed observations about co-presence and dominance effects. Furthermore, conditional branching reduced survey fatigue but resulted in too few responses in some branches, limiting statistical comparisons. Future work may complement synthetic stimuli with ethically curated real-world images and increase the sample size, ensuring sufficient coverage across all branches.

## VI. Conclusion

This paper advances the study of visual privacy by moving beyond a whole-image approach to a fine-grained, object-level perspective. Using a mixed-methods study with 92 participants, we uncovered how specific objects, their co-presence, and contextual cues shape people's privacy perceptions. Our results highlight the hidden dynamics that guide privacy judgments and demonstrate that small contextual details can

substantially influence perceived privacy concerns. We reemphasize the importance of human-centric design approaches that can help simplify the cognitive and technical complexity of visual privacy. Towards this end, we believe that our work lays the groundwork for developing adaptive, context-aware systems by providing empirical and practical insights.

## REFERENCES


[1] M. Broz, "How many photos are taken every day?" 2025, accessed: 2025-10-10. [Online]. Available: https://photutorial.com/photos-statistics/

[2] D. Burnes, M. DeLiema, and L. Langton, "Risk and Protective Factors of Identity Theft Victimization in the United States," *Preventive Medicine Reports*, vol. 17, p. 101058, 2020.

[3] T. K. H. Chan, C. M. K. Cheung, and R. Y. M. Wong, "Cyberbullying on Social Networking Sites: The Crime Opportunity and Affordance Perspectives," *Journal of Management Information Systems*, vol. 36, no. 2, pp. 574–609, 2019. [Online]. Available: https://doi.org/10.1080/07421222.2019.1599500

[4] P. Kaur, A. Dhir, A. Tandon, E. A. Alzeiby, and A. A. Abohassan, "A Systematic Literature Review on Cyberstalking. An Analysis of Past Achievements and Future Promises," *Technological Forecasting and Social Change*, vol. 163, p. 120426, 2021.

[5] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, "Online behavioral advertising: A literature review and research agenda," *Journal of advertising*, vol. 46, no. 3, pp. 363–376, 2017.

[6] S. Puglisi, D. Rebollo-Monedero, and J. Forné, "On web user tracking of browsing patterns for personalised advertising," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 32, no. 5, pp. 502–521, 2017.

[7] A. Mossou, "Solving World War II Photo Mysteries With Open Source Techniques," 2023, accessed: 2025-09-09. [Online]. Available: https://www.bellingcat.com/news/2023/08/04/solving-world-war-ii-photo-mysteries-with-open-source-techniques/

[8] Y. v. d. Weide, "Chronolocation: Determining When a Photo was Taken Using Facebook, Google Street View and Assorted Tiny Details ," 2023, accessed: 2025-09-09. [Online]. Available: https://www.bellingcat.com/resources/2023/05/08/chronolocation-determining-when-a-photo-was-taken-using-facebook-google-street-view-and-assorted-tiny-details/

[9] I. Urbina, "The Deadly Secret of China's Invisible Armada," 2020, accessed: 2025-09-09. [Online]. Available: https://www.nbcnews.com/specials/china-illegal-fishing-fleet/

[10] T. Akter, B. Dosono, T. Ahmed, A. Kapadia, and B. Semaan, "I am Uncomfortable Sharing what I can't see: Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 1929–1948. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/akter

[11] T. Akter, T. Ahmed, A. Kapadia, and S. M. Swaminathan, "Privacy Considerations of the Visually Impaired with Camera Based Assistive Technologies: Misrepresentation, Impropriety, and Fairness," in *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3373625.3417003

[12] A. Stangl, K. Shiroma, B. Xie, K. R. Fleischmann, and D. Gurari, "Visual Content Considered Private by People Who are Blind," in *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3373625.3417014

[13] L. Zhang, A. Stangl, T. Sharma, Y.-Y. Tseng, I. Xu, D. Gurari, Y. Wang, and L. Findlater, "Designing Accessible Obfuscation Support for Blind Individuals' Visual Privacy Management," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, ser. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3613904.3642713

[14] K. Patwari, C.-N. Chuah, L. Lyu, and V. Sharma, "PerceptAnon: Exploring the Human Perception of Image Anonymization Beyond Pseudonymization for GDPR," in *Proceedings of the 41st International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, R. Salakhutdinov, Z. Kolter, K. Heller, A. Weller, N. Oliver, J. Scarlett, and F. Berkenkamp, Eds., vol. 235. PMLR, 21–27 Jul 2024, pp. 39 955–39 971.

[15] A. Tonge and C. Caragea, "Image Privacy Prediction Using Deep Neural Networks," *ACM Trans. Web*, vol. 14, no. 2, Apr. 2020. [Online]. Available: https://doi.org/10.1145/3386082

[16] H. Habib, N. Shah, and R. Vaish, "Impact of contextual factors on snapchat public sharing," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–13.

[17] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "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, pp. 357–366.

[18] T. Orekondy, B. Schiele, and M. Fritz, "Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images," in *IEEE International Conference on Computer Vision (ICCV)*, 2017.

[19] R. Hoyle, L. Stark, Q. Ismail, D. Crandall, A. Kapadia, and D. Anthony, "Privacy Norms and Preferences for Photos Posted Online," *ACM Trans. Comput.-Hum. Interact.*, vol. 27, no. 4, Aug. 2020. [Online]. Available: https://doi.org/10.1145/3380960

[20] H. Nissenbaum, "Privacy as Contextual Integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[21] P. J. Wisniewski and X. Page, "Privacy theories and frameworks," in *Modern socio-technical perspectives on privacy*. Springer International Publishing Cham, 2022, pp. 15–41.

[22] S. Petronio, *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2002.

[23] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information systems research*, vol. 17, no. 1, pp. 61–80, 2006.

[24] A. Acquisti and J. Grossklags, "What can behavioral economics teach us about privacy?" in *Digital privacy*. Auerbach Publications, 2007, pp. 363–378.

[25] Y. Niu, N. Meng-Schneider, W. Qiu, and N. Kokciyan, "I am not the primary focus - Understanding the Perspectives of Bystanders in Photos Shared Online," ser. CHI '25. New York, NY, USA: Association for Computing Machinery, 2025. [Online]. Available: https://doi.org/10.1145/3706598.3713826

[26] S. Kairam, J. Kaye, J. A. Guerra-Gomez, and D. A. Shamma, "Snap decisions? How users, content, and aesthetics interact to shape photo sharing behaviors," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 113–124.

[27] Y. Li, N. Vishwamitra, H. Hu, and K. Caine, "Towards a taxonomy of content sensitivity and sharing preferences for photos," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–14.

[28] C. Liu, T. Zhu, J. Zhang, and W. Zhou, "Privacy Intelligence: A Survey on Image Privacy in Online Social Networks," *ACM Comput. Surv.*, vol. 55, no. 8, Dec. 2022. [Online]. Available: https://doi.org/10.1145/3547299

[29] D. Goyeneche, S. Singaraju, and L. Arango, "Linked by Age: A Study on Social Media Privacy Concerns Among Younger and Older Adults," *Industrial Management & Data Systems*, vol. 124, no. 2, pp. 640–665, 12 2023. [Online]. Available: https://doi.org/10.1108/IMDS-07-2023-0462

[30] A. Stangl, K. Shiroma, N. Davis, B. Xie, K. R. Fleischmann, L. Findlater, and D. Gurari, "Privacy concerns for visual assistance technologies," *ACM Trans. Access. Comput.*, vol. 15, no. 2, May 2022. [Online]. Available: https://doi.org/10.1145/3517384

[31] Y. Amil *et al.*, "The Impact of AI-Driven Personalization Tools on Privacy Concerns and Consumer Trust in E-commerce," Tech. Rep., 2024.

[32] R. Zhao, Y. Zhang, T. Wang, W. Wen, Y. Xiang, and X. Cao, "Visual Content Privacy Protection: A Survey," *ACM Comput. Surv.*, vol. 57, no. 5, Jan. 2025. [Online]. Available: https://doi.org/10.1145/3708501

[33] W. Wen, Z. Yuan, Y. Zhang, T. Wang, X. Xiao, R. Zhao, and Y. Fang, "Image Privacy Protection: A Survey," *arXiv preprint arXiv:2412.15228*, 2024.

[34] C.-W. Chiang, H. Y. Tian, and M. Yin, "Understanding User Needs and Attitudes for Privacy Protection Tools in Online Visual Content Sharing," *Proceedings of the ACM on Human-Computer Interaction*, vol. 9, no. 7, pp. 1–31, 2025.

[35] S. Ravi, P. Climent-Pérez, and F. Florez-Revuelta, "A Review on Visual Privacy Preservation Techniques for Active and Assisted living," *Multimedia Tools and Applications*, vol. 83, no. 5, pp. 14 715–14 755, 2024. [Online]. Available: https://doi.org/10.1007/s11042-023-15775-2

[36] M. Khamis, H. Farzand, M. Mumm, and K. Marky, "DeepFakes for privacy: Investigating the effectiveness of state-of-the-art privacy-enhancing face obfuscation methods," in *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, 2022, pp. 1–5.
[37] N. Vishwamitra, B. Knijnenburg, H. Hu, Y. P. Kelly Caine *et al.*, "Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2017, pp. 39–47.
[38] S. Zerr, S. Siersdorfer, and J. Hare, "PicAlert! A System for Privacy-Aware Image Classification and Retrieval," in *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*, ser. CIKM '12. New York, NY, USA: Association for Computing Machinery, 2012, p. 2710–2712. [Online]. Available: https://doi.org/10.1145/2396761.2398735
[39] Y. Li, N. Vishwamitra, B. P. Knijnenburg, H. Hu, and K. Caine, "Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos," *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, no. CSCW, pp. 1–24, 2017.
[40] M. Khamis, R. Panskus, H. Farzand, M. Mumm, S. Macdonald, and K. Marky, "Perspectives on DeepFakes for Privacy: Comparing Perceptions of Photo Owners and Obfuscated Individuals towards DeepFake Versus Traditional Privacy-Enhancing Obfuscation," in *Proceedings of the International Conference on Mobile and Ubiquitous Multimedia*, 2024, pp. 300–312.
[41] Z. Lu, D. Huang, L. Bai, J. Qu, C. Wu, X. Liu, and W. Ouyang, "Seeing is not always believing: Benchmarking human and model perception of ai-generated images," *Advances in neural information processing systems*, vol. 36, pp. 25 435–25 447, 2023.
[42] F. Lago, C. Pasquini, R. Böhme, H. Dumont, V. Goffaux, and G. Boato, "More real than real: A study on human visual perception of synthetic faces [applications corner]," *IEEE Signal Processing Magazine*, vol. 39, no. 1, pp. 109–116, 2021.
[43] S. Nightingale, S. Agarwal, E. Härkönen, J. Lehtinen, and H. Farid, "Synthetic faces: how perceptually convincing are they?" *Journal of vision*, vol. 21, no. 9, pp. 2015–2015, 2021.
[44] B. Shen, B. RichardWebster, A. O'Toole, K. Bowyer, and W. J. Scheirer, "A study of the human perception of synthetic faces," in *2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021)*. IEEE, 2021, pp. 1–8.
[45] M. Bilucaglia, C. Casiraghi, A. Bruno, S. Chiarelli, A. Fici, V. Russo, and M. Zito, "Emotional reactions to AI-generated images: a pilot study using neurophysiological measures," in *International Conference on Machine Learning, Optimization, and Data Science*. Springer, 2024, pp. 147–161.
[46] T. Orekondy, M. Fritz, and B. Schiele, "Connecting Pixels to Privacy and Utility: Automatic Redaction of Private Information in Images," in *Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018.
[47] D. Gurari, Q. Li, C. Lin, Y. Zhao, A. Guo, A. Stangl, and J. P. Bigham, "VizWiz-Priv: A Dataset for Recognizing the Presence and Purpose of Private Visual Information in Images Taken by Blind People," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 939–948.
[48] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, pp. 336–355, 2004.
[49] F. Bélanger and R. E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, vol. 35, no. 4, pp. 1017–1041, 2011. [Online]. Available: http://www.jstor.org/stable/41409971
[50] V. Braun, V. Clarke, N. Hayfield, L. Davey, and E. Jenkinson, "Doing Reflexive Thematic Analysis," in *Supporting Research in Counselling and Psychotherapy: Qualitative, Quantitative, and Mixed Methods Research*. Springer, 2023, pp. 19–38.
[51] A. Blandford, D. Furniss, and S. Makri, *Qualitative HCI Research: Going Behind the Scenes*. Morgan & Claypool Publishers, 2016.
[52] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, Nov. 2019. [Online]. Available: https://doi.org/10.1145/3359174
[53] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek, "A Summary of Survey Methodology Best Practices for Security and Privacy Researchers," University of Maryland, Tech. Rep., 2017.
[54] L. M. Rea and R. A. Parker, *Designing and Conducting Survey Research: A Comprehensive Guide*. John Wiley & Sons, 2014.
[55] S. Egelman, J. King, R. C. Miller, N. Ragouzis, and E. Shehan, "Security User Studies: Methodologies and Best Practices," in *CHI '07 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 2833–2836. [Online]. Available: https://doi.org/10.1145/1240866.1241089
[56] M. Cheung and J. She, "Evaluating the privacy risk of user-shared images," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 12, no. 4s, pp. 1–21, 2016.
[57] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, 2006.
[58] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & security*, vol. 77, pp. 226–261, 2018.
[59] M. H. Akcay, B. G. Atli, S. P. Rao, and A. Bakas, "From See to Shield: ML-Assisted Fine-Grained Access Control for Visual Data," *arXiv preprint arXiv:2510.19418*, 2025.

## APPENDIX

### A. Prompts Used for Image Generation

The text prompts used to generate the example images shown in Figure 2. For each environment, the first image was generated from a base prompt, while subsequent variations were produced using SORA's remix functionality.

- Figure 2a (Base image for café, face foreground only): *"A realistic indoor café scene in the late morning, softly illuminated by natural daylight streaming through large street-facing windows. A woman in her late 20s is seated alone at a small round table near the window, angled slightly toward the light. She has shoulder-length dark auburn hair, loosely tied back, and wears a cream-colored short-sleeve knit top and dark jeans. Her forearms rest naturally on the table, making them clearly visible in the frame. Her skin is light olive-toned, and she has a calm, neutral expression as she gazes out the window with a subtle half-smile, unaware of the camera. On the table are a few personal items: a half-full ceramic mug, a closed leather-bound notebook, and a smartphone lying screen-down. The table itself is a worn, wooden surface with a bit of character—subtle scratches and warm tones. She sits on a simple wooden chair with a low back, and there's a canvas tote bag hanging off the side. In the softly blurred background, the café reveals other details: a brick accent wall, a large chalkboard menu partially visible above the counter, and some framed posters and event flyers loosely pinned to a corkboard near the entrance. There are a few other patrons seated further back—some chatting, some working on laptops—but none are clearly distinguishable. The camera angle is natural and intimate, positioned at eye level and slightly off-center, capturing the woman from the front-left in a three-quarter view. Her arms are fully visible on the tabletop. The lighting is warm, realistic, and casts soft, diffused shadows across the scene. The photograph feels candid and everyday—an ordinary moment caught in passing, creating a grounded and relatable atmosphere."*
- Figure 2b (Face + medicine): *On the table there is medicine.*
- Figure 2c (Face + medicine + landmark): *On the wall in the back, the café name is written: "Elm Street Café."*
- Figure 2d (Base image for office, face foreground only): *"A photorealistic indoor office scene set in a mid-size,*

*modern corporate workspace during a weekday morning. The environment is structured and clean, with carpeted floors, partitioned desks, and frosted glass panels along the corridor wall. Overhead lighting casts a neutral white tone across the space, supplemented by soft daylight from windows with mesh roller blinds half-drawn. In the foreground, a man in his early 30s is seated alone at an L-shaped desk inside a semi-open cubicle. He has short dark brown hair, light stubble, and wears a dark gray button-up shirt with a lanyard ID badge around his neck. His posture is engaged but relaxed, and he's focused on his dual-monitor workstation — one screen shows a spreadsheet, the other a messaging app. His desk has typical office clutter: a keyboard, notepad with scribbled notes, ceramic coffee mug, a phone dock, and a small branded desk calendar. A jacket is draped over the back of his ergonomic chair, and there's a cable tray visible beneath the desk. The background includes blurred silhouettes of other cubicles, vertical storage cabinets, and a meeting room with glass doors partially open. The tone is realistic and corporate — capturing a candid moment of one employee at work, with the environment grounded in everyday office detail."*

- Figure 2e (Face + tattoo): *Add a tiger tattoo to the forearm, "legend" should be written below tiger.*
- Figure 2f (Face + tattoo + face (a.)): *Add a person.*

### *B. Full Survey (Café Version)*

Note: Office version of the survey has the same questions. The only difference is that the displayed AI-generated images show a working office environment.

**Page 0: Instructions**

Participants were presented with a brief overview of the survey's context and informed that all images were synthetic and generated using AI tools, with no real individuals or personal data involved. Information on data processing was disclosed, including the names of the responsible parties, the types of personal data collected (e.g., demographic data and survey responses) and the applicable legal basis under GDPR. Participants were informed of their rights regarding access, correction and deletion of their data, and withdrawal of consent, along with instructions for submitting privacy-related requests or complaints. To start the survey, participants were required to give their informed consent and enter their email address for validation purposes. Optionally, they could choose to enter the lottery to win a movie ticket.

**Page 1: Demographic Information**

Please answer a few demographic questions.

**Q1. What is your age?**
18–24
25–34
35–44
45–54
55 and older

**Q2. How often do you share photos online?**
Never
Rarely
Sometimes
Often
Daily

**Q3. What type of devices do you regularly use? (Select all that apply)**
Mobile phone
Laptop/Desktop computer
Smart watch
Fitness tracker
Wearable devices (e.g., heart rate monitor, VR)
Other

**Q4. What is your ethnic background? (Select one)**
White / Caucasian
Black or African
Asian
Native American / Indigenous
Mixed / Multi
I don't wish to disclose
Other

**Q5. What is your gender?**
Male
Female
Other
Prefer not to say

**Q6. What is your highest level of education?**
Less than high school
High school graduate
Some college
2-year degree
Bachelor's degree
Master's degree
Doctorate

**Q7. What is your professional background?**
Employed full-time
Employed part-time
Unemployed (seeking)
Unemployed (not seeking)
Retired
Student

**Q8-11. Privacy Preference Statements**

Please indicate your agreement with the following statements:
(a) I am concerned about my privacy online
(b) I am concerned about my privacy in everyday life
(c) It bothers me to give personal info to many online companies
(d) I check photos for personal info before sharing online

*Likert Scale: 1 = Disagree, 2 = Somewhat Disagree, 3 = Neutral, 4 = Somewhat Agree, 5 = Agree*

**Page 2: Visual Privacy – Face**

Fig. 5: Visual accompanying Q12. *Likert Scale: 1 = Not comfortable at all, 2 = Slightly uncomfortable, 3 = Neutral, 4 = Slightly comfortable, 5 = Very comfortable*

Suppose you are sitting at a table in a cafeteria. For each of the below groups of images, picture yourself as the subject in the photograph. Either you are the one taking the photo from your perspective, or someone takes a picture of you.

**Q12. How comfortable would you feel sharing this photo of yourself on your social media account?**

**Q13-17. Suppose while taking the picture, there were some other objects captured along with the background. How comfortable would you feel sharing the picture of yourself if the following objects were in the image?**

**Q18. Based on your answers above, please rank the objects in order of sensitivity.**
Human Tattoo Poster Medicine Landmark

*1 = Most sensitive, 5 = Least Sensitive*

**Q19. Why did you rank the objects in this order?** (Open text)

**Q20-23. (Assume that the participant ranked the landmark as the background PSO with the least effect on the comfortability level) You realized that the photo including the landmark also included the following objects. How comfortable would you feel sharing the picture of yourself that also contains landmark if the following objects were in the image as well?**

**Q24. Can you explain what the effect of landmark was on how comfortable you felt sharing the picture of yourself with the other objects?** (Open text)

**Page 3: Visual Privacy – Miscellaneous Paper**
The structure of this page mirrors that of the previous section (face as a foreground PSO). Participants are asked to evaluate


(a) [1–5] Likert scale

(b) [1–5] Likert scale

(c) [1–5] Likert scale

(d) [1–5] Likert scale

(e) [1–5] Likert scale

Fig. 6: Visuals accompanying Q13-17. *Likert Scale: 1 = Not comfortable at all, 2 = Slightly uncomfortable, 3 = Neutral, 4 = Slightly comfortable, 5 = Very comfortable*

their comfortability levels with images involving **Miscellaneous Paper** as the foreground PSO. After rating their comfort with the foreground PSO alone, the participants are asked the same questions where the background PSOs are *face (photo), full name, birthdate, signature*, and *address*. As before, they complete individual Likert scale ratings, rank the background items according to their effect on the comfortability level, and rate the effect of the combination of background PSOs. This section includes questions **Q25–Q37**.

**Page 4: Visual Privacy – Computer/phone Screen**
The structure of this page mirrors that of the previous section (face as a foreground PSO). Participants are asked


Human

(a) [1–5] Likert scale


Tattoo

(b) [1–5] Likert scale


Poster

(c) [1–5] Likert scale


Medicine

(d) [1–5] Likert scale

Fig. 7: Visuals accompanying Q20-23. *Likert Scale: 1 = Not comfortable at all, 2 = Slightly uncomfortable, 3 = Neutral, 4 = Slightly comfortable, 5 = Very comfortable*

to evaluate their comfortability levels with images involving **Computer/Phone screen** as the foreground PSO. After rating their comfort with the foreground PSO alone, the participants are asked the same questions where the background PSOs are *face (reflection), email, username, date*, and *phone number*. As before, they complete individual Likert scale ratings, rank the background items according to their effect on the comfortability level, and rate the effect of the combination of background PSOs. This section includes questions **Q38–Q50**.

**Page 5: Review and Submit**

Participants were shown a summary of their responses and asked to confirm and submit.

### *C. Additional Tables and Figures*

TABLE IX: Mapping between comfortability levels and perceived privacy levels.

| Comfortability Level | Perceived Privacy Level |
|---|---|
| 1 (Not comfortable at all) | 5 (Most sensitive) |
| 2 (Slightly uncomfortable) | 4 |
| 3 (Neutral) | 3 |
| 4 (Slightly comfortable) | 2 |
| 5 (Very comfortable) | 1 (Least sensitive) |

TABLE X: Demographic distribution of survey participants (n=92).

| Category | Response | Count (%) |
|---|---|---|
| Ethnicity | White/Caucasian | 58 (63%) |
| | Asian | 20 (22%) |
| | Black/African | 6 (7%) |
| | Mixed/Multi | 3 (3%) |
| | I don't wish to disclose | 5 (5%) |
| Age | 18–24 | 18 (20%) |
| | 25–34 | 32 (35%) |
| | 35–44 | 9 (10%) |
| | 45–54 | 29 (32%) |
| | 55+ | 4 (4%) |
| Gender | Female | 47 (51%) |
| | Male | 43 (47%) |
| | Other | 2 (2%) |
| Education | High school graduate | 4 (4%) |
| | Some college | 3 (3%) |
| | Bachelor's degree | 32 (35%) |
| | Master's degree | 29 (32%) |
| | Doctorate | 24 (26%) |
| Profession | Employed full-time | 52 (57%) |
| | Employed part-time | 8 (9%) |
| | Student | 28 (30%) |
| | Retired | 2 (2%) |
| | Unemployed | 2 (2%) |

TABLE XI: Significant demographic effects on comfortability levels. Mann–Whitney U tests were applied for gender, showing that female participants reported higher comfortability levels in all significant cases. Kruskal–Wallis H tests were used for the remaining demographic variables, indicating at least one group distribution differed significantly from the others.

| Foreground PSO | Background PSO | Category | $p$-value |
|---|---|---|---|
| **Café** | | | |
| Computer/phone Screen | E-mail | Gender (F > M) | 0.0489 |
| Computer/phone Screen | Phone Number | Gender (F > M) | 0.0289 |
| Face | None | Social Usage | 0.0332 |
| Miscellaneous Paper | Face (p.) | Social Usage | 0.0126 |
| Computer/phone Screen | None | Social Usage | 0.0391 |
| Computer/phone Screen | Face (r.) | Social Usage | 0.0401 |
| Face | Landmark | Profession | 0.0377 |
| Computer/phone Screen | None | Profession | 0.0280 |
| Computer/phone Screen | Face (r.) | Profession | 0.0430 |
| Face | Landmark | Age | 0.0206 |
| Miscellaneous Paper | Full Name | Age | 0.0355 |
| Computer/phone Screen | E-mail | Age | 0.0177 |
| Computer/phone Screen | Face (r.) | Age | 0.0206 |
| **Office** | | | |
| Face | Face (a.) | Ethnicity | 0.0399 |
| Miscellaneous Paper | Full Name | Ethnicity | 0.0056 |
| Miscellaneous Paper | Signature | Ethnicity | 0.0391 |
| Computer/phone Screen | E-mail | Ethnicity | 0.0012 |
| Miscellaneous Paper | Face (p.) | Education | 0.0427 |
| Face | Tattoo | Age | 0.0393 |
| Computer/phone Screen | Date | Age | 0.0408 |

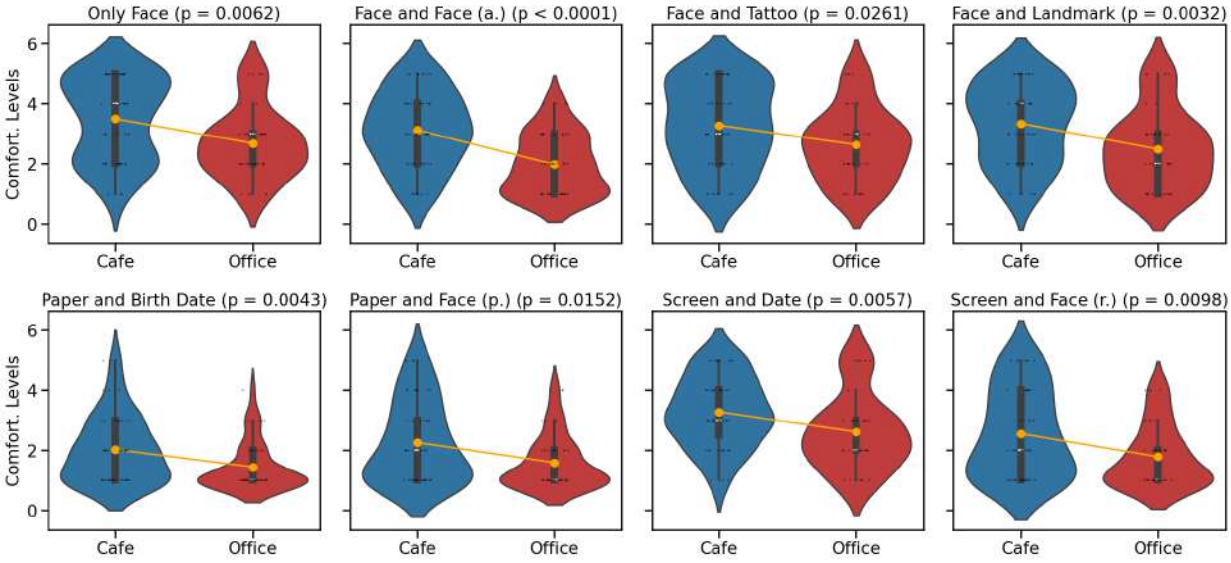



Fig. 8: Violin Plots of significant Mann-Whitney U test results for café and office environments (H2). Each subplot shows comfortability levels (1–5) for a foreground/background PSO pair; width reflects data density, and orange lines mark group mean differences.