"You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography

Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su, *Indiana University Bloomington*

https://www.usenix.org/conference/soups2018/presentation/rashidi

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

August 12–14, 2018 • Baltimore, MD, USA

ISBN 978-1-939133-10-6

Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

"You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography

Yasmeen Rashidi Tousif Ahmed Felicia Patel Emily Fath
Apu Kapadia Christena Nippert-Eng Norman Makoto Su
School of Informatics, Computing, and Engineering
Indiana University
Bloomington, IN, USA
{yrashidi, touahmed, fjpatel, ecfath, kapadia, cnippert, normsu}@indiana.edu

ABSTRACT

Pervasive photography and the sharing of photos on social media pose a significant challenge to undergraduates' ability to manage their privacy. Drawing from an interview-based study, we find undergraduates feel a heightened state of being surveilled by their peers and rely on innovative workarounds – negotiating the terms and ways in which they will and will not be recorded by technology-wielding others – to address these challenges. We present our findings through an experience model of the life span of a photo, including an analysis of college students' workarounds to deal with the technological challenges they encounter as they manage potential threats to privacy at each of our proposed four stages. We further propose a set of design directions that address our users' current workarounds at each stage. We argue for a holistic perspective on privacy management that considers workarounds across all these stages. In particular, designs for privacy need to more equitably distribute the technical power of determining what happens with and to a photo among all the stakeholders of the photo, including subjects and bystanders, rather than the photographer alone.

1. INTRODUCTION

In the United States, individuals view privacy as a largely personal managerial task including the selective concealment and disclosure of information about the self to manage relationships with others [54]. According to Altman, people engage in a dynamic 'boundary regulation' process to control access to one's self, which may change depending on the time and circumstance [3]. Through what Goffman calls 'impression management' [28], we try to control the ways others think of us by also managing our 'self presentation'. Individuals are members of multiple groups, and such impression management tends to vary based on the audience and the place [28, 45], e.g., managing one's work versus home personas [53]. Managing privacy thus encompasses a variety of activities both online and offline, utilizing personal socio-technical systems to try to control the accessibility and use of information about us by others [54, 52].

The rise of digital photography and the sharing of high-resolution imagery on social media is not only blurring the line separating the face-to-face and online worlds, it is also forcing us to grapple with a face-to-face world that is, in effect, losing its ephemerality. The implications for impression management are staggering, including an increasing threat to what Nissenbaum calls the 'contextual integrity' of personal information. Existing norms guiding the appropriate collection and dissemination of information are at an ever-greater risk of being broken [55]. The possibilities of what boyd calls 'context collapse' and its associated violations of privacy [55, 8, 9] loom as the captured actions associated with one's social, temporal, and physical context (e.g., photos from a party) are able to be viewed and judged from another – and very different – social context (e.g., an internet search by a potential employer) [73].

Young adults, still in their formative and exploratory years, are often subjected to and impacted by digital photography where smartphone cameras are now integrated with 'one-click' sharing onto social media. Growing up in a world where cameras augmented with seamless social sharing functions are pervasive, perhaps no population has had their privacy more impacted by digital photography than today's young adults. Face-to-face interactions – once a safe, impermanent place for exploratory thought and expression – may now be recorded, altered, reframed, and turned into a persistent online record capable of going viral in seconds, often without the subject's knowledge. Young adults today may thus feel they are being constantly surveilled by their peers. Such pervasive photography raises important questions: What does it mean to be a young adult living in such an environment? What does this mean for an individual's privacy, and for the challenges of trying to control the impression others have of one, now and in the future?

To understand the relationship between privacy, pervasive photography, and social media, we conducted interviews with 23 undergraduates. We focus on three research questions: (1) *What are the everyday privacy concerns of undergraduates with regard to photography and social media?*; (2) *How are undergraduates responding to these concerns?*; and (3) *What privacy enhanced designs might help support*

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

their more immediate and longer term goals given their concerns and current responses to them?

Based on our interviews, we constructed an 'experience model' [37] that represents our participants' experiences with photography on social media, focusing on the 'workarounds' young adults enact to better respond to and manage challenges posed by the current technology. This experience model presents four key stages in the life of a potentially social-media bound photo – when the photo is in its 'potential', 'imminent', 'existent', and 'shared' states. This model expresses the intersubjective nature of what happens to a photo in each of these stages as its fate is negotiated by the relevant actors: photographers, subjects, and bystanders. We build on past research that discusses the privacy concerns of our participants at each of these corresponding stages (e.g., [7, 1, 29]) while adding to existing research by presenting a holistic perspective on digital photography and privacy across time, space, and people. This model highlights, for instance, how the threat of even the potential of being photographed leads to various forms of self-discipline among our participants; how the perception of imminent photography involves split-second reactions from our participants and their friends; how the continued existence and uses of photos may be negotiated at the point of capture; and how the equivalent of 'neighborhood watches' work to mitigate the consequences of shared photos.

This holistic approach to workarounds makes two contributions. First, we provide a model of the constant state of watchfulness that undergraduate students are engaged in to manage their privacy in the face of surveillance from ubiquitous photography and social media. Second, we outline a map from our experience model to designs (a design opportunity map) that highlights how extant and future designs can address users' privacy concerns, both on individual stages and across stages. Taken as a whole, for instance, our model suggests that the power to determine what happens with a (potential) photo at any given stage should be spread more widely across all the stakeholders – not just those who control the taking, altering, and posting of photos.

2. RELATED WORK

In this section, we first describe concerns of surveillance in everyday life and social networking sites followed by a description of privacy management and workaround practices.

2.1 Surveillance Concerns in Everyday Life and in SNS

Due to the pervasiveness of technology and social media, digital records of our daily activities are now a common aspect of everyday life. We are, for example, physically surrounded by closed-circuit television cameras (CCTV) that operate 24/7. We also regularly use digital technologies (e.g., smartphones and digital cameras) to create and preserve fragments of digital information about ourselves, our friends and family members, and even strangers, permanently retrievable by anyone, anywhere, anytime, as long as they have access to the internet (e.g., Facebook, YouTube, and Flickr). Since the technology's inception, privacy advocates have investigated the intersection of privacy and technology. In direct response to the rise of print photography on the society pages of the daily newspaper, Warren and Brandeis wrote their celebrated 1890 article on privacy as the "right to be let alone" to enforce definite boundaries between public and private life [83].

Photography has become a "modern tool of choice for constructing one's identity and conveying it to others" [84, p. 4]. Photos (i.e. film or digital), unlike other media types, are seen as highly context-dependent [24, 77, 35, 34, 66]. Reading and interpreting a photo's context depends mainly on the viewer and could differ significantly from the photographer's intention/context in the moment of taking the photo [77, 78]. Due to our interest in the pervasiveness of personal photography, we will focus our discussion for surveillance concerns around photo recording technology, such as digital and wearable cameras and smartphones.

Various researchers have focused on privacy concerns about pervasive photo recording technology in both online (e.g., Facebook, Snapchat) and offline environments (e.g., public arenas, shared spaces, and private spaces) in different, *specified* stages of a photo's lifespan. Concerns about recording activities and behaviors were usually tied to the location where the activity is being recorded [17, 21, 74, 66]. For example, Choe *et al.* investigated activities that people do not want recorded in their home or shared with other stakeholders with whom they share the home [17]. They found that the most reported activities fell into the categories of self-appearance, intimacy, cooking and eating, media use, and oral expressions. They also found that bedrooms and living rooms were thought to be more private than other locations in the home. Denning *et al.* studied bystanders who may be captured by augmented reality glasses [21] and found various factors affected bystanders' comfort levels and behaviors. For instance, participants were not comfortable when glasses were used during certain activities (e.g., withdrawing money from the ATM), places (e.g., bedroom and bathroom), or if the recorded image conflicted with their desired self-presentation. Such *et al.* [74] found that co-owners (i.e., photographer and subjects) of online shared photos had privacy conflicts around photos of drinking or at parties. Photographers (uploaders) often did not ask for approval before sharing.

Research has also investigated the control, access, awareness, and consent of photo records [66, 6, 35, 34, 48, 51, 11]. For example, Besmer and Lipford [6] investigated users' concerns regarding photo tagging on SNS. Subjects worried about the negative consequences of a photo being seen by a specific social group or presenting them in an unfavorable light. Rashidi *et al.* investigated privacy concerns in mobile instant messaging application and found that some users had concerns about their profile photos being seen by others [61]. People anticipated no covert recording in their home and referred to others (e.g., friends, roommates, and family members) who might surreptitiously try to record them as "interlopers" [48]. Hoyle *et al.* studied the privacy of lifelogging cameras [35, 34] and found that camera wearers were concerned about impression management when managing the sharing of their lifelogs. They also found that sometimes camera wearers chose not to share photos because of objects in the image, activities in the image, and someone in photo (i.e., self or another bystander(s)). Nguyen *et al.* investigated the use of wearable cameras in everyday life [51] and reported on how bystanders wanted to be informed and provide their consent before recording, but felt at the same time

that they have no power and cannot even rely on their social relationships to enforce their preferences, such as asking for deletion or requesting not to share. In another study, although bystanders reported expecting and tolerating recording in public settings, they felt "helplessness" because of the absence of any tools, power, or knowledge necessary to effect a change [48]. Caine *et al.* described how older adults desired control over the collection and transmission of activity data from home monitoring systems [11].

2.2 Privacy Management and Workarounds

In today's networked world, privacy can be conceptualized as a 'dialectic' and dynamic 'boundary regulation' process according to Altman [3], as individuals alter their behavior to disclose or not disclose information to manage their identity and allegiances with others over time [57]. Managing one's personal information, privacy, and identity, specifically within social media, is no longer an individualistic process and is increasingly being seen as a collective process [82, 60, 46, 50, 36, 69, 55] – especially in collaborative settings (such as hospitals) [50] where information is co-owned by the original co-owners (e.g., photographer and subjects in the photo) and/or other extended co-owners (e.g., people who are granted access to the shared content by the original co-owners) [50, 74].

Among various strategies to manage privacy in today's socio-technical systems [44, 71, 85, 18, 10, 72, 6, 47, 19, 79, 16], we focus our study on students' use of 'workarounds', which are behaviors adopted in order to 'get the job done', manage gaps, and enact strategies [49] to maintain their privacy in today's era of pervasive photography. A workaround includes the "work patterns an individual or a group of individuals create to accomplish a crucial work goal within a system of dysfunctional work processes that prohibits the accomplishment of that goal or makes it difficult" [49, p. 52]. For Koppel *et al.* workarounds are "actions that do not follow explicit or implicit rules, assumptions, workflow regulations, or intentions of system designers. They are non-standard procedures typically used because of deficiencies in system or workflow design" [40, p. 409].

Workarounds are mentioned in several different research areas, especially those related to health information technology and organizations. Here, to 'workaround' is to "use computing in ways for which it was not designed or avoid its use and rely on an alternative means of accomplishing work" [27, p. 12]. We are not aware of studies that focus on workarounds related to privacy management in everyday life, certainly in the context of sharing photos on social networking sites. Yet, studying workarounds can provide insight into future improvements to computing systems [2]. Student attempts to manage their individual and collective privacy, and photographs can be categorized into two groups of workarounds: online and offline strategies. Online workarounds are the use of technology in unexpected ways to complete a task. For example, although users could create different 'Friend Lists' to control the visibility of individual posts, the associated costs of doing so (e.g., time consuming and tedious) has instead led many users to create multiple targeted profiles on the same site (e.g., Facebook) [85, 44, 81]. Offline workarounds are used when individuals cannot find a technical tool to support their needs [10, 6, 43, 85, 50, 80]. Besmer and Lipford [6] note that Facebook users modified their behavior both online and offline to cope with the use and popularity of Facebook photo sharing. Users self-censored their physical activities to prevent unwanted photos from being captured and to avoid physical confrontation with photographers for deletion of unwanted images.

Lampinen *et al.* propose another way to categorize workaround strategies [43] which are overlapping strategies to manage privacy and publicness on SNS (i.e., mental, behavioral, preventive, corrective, individual, and collaborative). Although the strategies do not necessarily have to all be workarounds – some of them include the straightforward, intended uses of technology – we can still build upon the workaround strategies in Lampinen *et al.*'s framework. 'Mental workarounds', for instance, include developing interpersonal arrangements to manage disclosure, trusting others to be considerate to one's boundary regulation, and becoming more responsible when posting material on social networking sites [44]. 'Behavioral workarounds' can be further divided into preventive workarounds to avoid unwanted outcomes and corrective workarounds to eliminate or reduce the threat after such an outcome has already occurred. Self-censorship and device (e.g., smartphone) avoidance are 'preventive workarounds'. Interpreting a potentially problematic issue to be non-serious and asking peers to remove content are 'corrective workarounds'. Because of the lack of SNS controls to support collaboration to manage privacy boundary [72, 43, 85, 79, 16, 50, 36, 69], we can consider most of the collaborative workaround strategies as 'offline workarounds' (e.g., asking another person to delete content, asking for approval before disclosing content, and negotiating what is appropriate to share on social networking sites). Murphy *et al.* found that emergency department staff, which are highly collaborative, use workarounds when privacy policies or security mechanisms interfered with their actual work practices. They raised the awareness of the need to improve design to facilitate collaboration endeavors and manage privacy in such environments.

We focus on how students work around technology because of the lack of satisfactory tools to manage privacy, especially for fine-grained tasks, with the goal of better understanding their needs and, therefore, providing design recommendations to suit these needs. Our research confirms many of the aforementioned privacy concerns and workaround strategies, but builds upon these findings by taking a holistic, bird's eye view of the ways a potentially social media-bound photo comes into being and garners the attention of various actors through the photo's 'lifecycle'.

3. METHODOLOGY

We conducted semi-structured interviews with 23 undergraduate students on a large, US college campus from March 2016 to August 2016. Undergraduates are a rich information source [59]: (1) they are likely to use social media and new technology; (2) having just transitioned from high school and simultaneously transitioning to professional life, students are aware of their social and professional images, and are grappling with the management of their individual and collective privacy; and (3) the environment of students (i.e., living together in dorms, social events) create rich contexts within which they navigate such concerns. Students were recruited through flyers placed in common areas, online university classifieds, and emails sent to campus orga-

nizations. In total, 14 students lived in dorms, 4 lived by themselves, 3 with family, and 2 with friends. 15 participants have used Facebook, 17 have used Snapchat, 16 have used Instagram, 13 have used Twitter, and 4 have used Yik Yak. Each participant was compensated $15 USD at the end of the study. This study was deemed exempt by the Indiana University IRB (#1510531315). Screened participants completed an informed consent form at the beginning of each interview. All interviews were audio recorded, transcribed, and de-identified. We employed critical incident techniques [15]; once participants told us stories/incidents, we probed for specific details, allowing participants to control the narrative and help us understand what occurred, from their perspectives. Interviews lasted 43–74 minutes ($M = 59.5, SD = 7.7$), including 12 women and 11 men, aged 18–24, and spanning diverse fields of study.

After the first 18 interviews, we met multiple times to analyze the first third of the transcripts in an iterative approach using open and axial coding [70]. We then discussed the identified themes and developed a draft codebook. Dedoose [20], a web application tool, was used to code and organize data. Using the draft codebook and working in pairs, we coded the remaining transcripts to identify new themes, which were then discussed with the entire team and, if appropriate, added to the codebook. Emergent themes led us to iterate on the interview protocol used in the first 18 interviews to investigate topics discussed by earlier participants. The updated protocol was then used with the last five participants. We then analyzed the newly collected data using the same process and reached theoretical saturation – no new themes were identified in this stage.

Our initial protocol investigated privacy concerns and behaviors associated with the ubiquitous presence of smartphones and social media technology in general. The overwhelming focus on shared photographs in these interviews led us to emphasize privacy concerns and photography for the final five students. In addition to demographic questions, our protocol focused on privacy- and technology-related events that happened face-to-face or online, and which then impacted interactions in the opposite realm as well as evolving attitudes and behaviors around digital photography.

4. FINDINGS: PHOTOS AS THREATS TO PRIVACY

The concern over the long-term effects of digital photography on one's privacy is timely – across SNSs, there is a dizzying array of default settings on how photos persist. Participants expressed how such default archiving with photos have a big impact on one's reputation "because [this photo is] there forever, and it's written [which] can be used as evidence against you" (P21). The persistence of photos on platforms such as Instagram creates a bigger, far more permanent, and less controllable audience than for others like Snapchat:

My friend on her 21st birthday [had] this picture that was entirely too ratchet [slang for crazy] ... Her friends sent her a Snapchat of it ... and [she] didn't realize it was on another site [Instagram] ... [Later] she did see it on [Instagram] and was like, "Come on guys, that's not okay." (P6)

Although P6's friend did not mind sharing the photo on Snapchat, which 'disappears' after being viewed twice, she was shocked to see her photo being posted on Instagram, where persistence was the default. This persistence had direct ramifications for her reputation.

The daily routines of undergraduates involve the creation and sharing of photos by themselves or others (e.g., friends or strangers). Consciously or unconsciously, our participants archived a timeline of their daily life events and activities via the sharing of these photos on different SNS. Photos are open to interpretation yet, due to their seemingly objective nature, provide an *evidentiary chain* to potentially invade one's personal and groups' (e.g., one's sorority) privacy.

4.1 Personal Privacy

Participants were aware of the power photos had over their viewers and felt that captured and shared photos could have serious consequences on their privacy and self-presentation. For example, participants expected others would *judge* them based on these images in a potentially negative and persistent manner. P14 notes below that photos can become a permanent stain on her friend's "record", providing misleading evidence that her friend is a "drunk" girl:

[My friend] came home and was drunk. Somebody was taking a video of her. She was really upset about this, because she didn't wanna be recorded and was really really embarrassed about it ... She asked the person to delete it ... [but] she found out the video wasn't completely deleted. That somebody sent it to somebody else ... She didn't want a video leaked on Twitter ... She didn't want her parents or any older friends, like adults, to see it ... She doesn't want that to go on her record. I don't think it's the general reputation she wants to have is this silly sloppy drunk girl. (P14)

When students felt their actions were not inappropriate, they still worried how others would *misinterpret* photos, taking them out of context and harming their image. P21 mentioned one such negative impression from a photo that might be seen out of its actual context:

[People] just sit there and judge you ... They don't want to understand why you are doing anything you do. The fact is that the picture [of you doing a shot is] there. You look happy in the moment. Whatever you're [doing] nothing else about you matters besides that picture to them because they can't see anything if it's not evident. (P21)

This was a sentiment reiterated by many participants: viewers of a posted photo will not exert the extra effort to truly understand its context. For instance, students cynically expected people to misinterpret photos taken in bars and parties. In these environments, the opportunity arises for misinterpretation of one's drinking behavior (e.g., excessive versus moderate drinking). Objects in a photo (e.g., alcohol bottles and cups) were vulnerable to misinterpretation. Participants were especially worried how photos would be interpreted by their professional peers; they knew that misinterpreted photos could effect future job prospects and curated their social media accounts appropriately.

Surprisingly, participants shared a concern for strangers or acquaintances stealthily capturing and altering original, shared photos with captions or framing them as part of a specific scene to create *memes*. Participants described a shaming trend in which people take photos of strangers,

craft them into memes, and "send them around with a rude caption" (P7), maybe because someone was "dressed not differently, but [in] something really radical" (P18) or because the "kind of things they were doing [was] out of the ordinary" (P18): "One day my jeans ripped really bad and I'm like, 'What am I gonna do?' ... That's like where memes come from. You don't want to be the next meme!" (P6) Participants complained that photos have become a means to deride or ridicule activities that the photographer deems as against current social norms. P4 witnessed such an incident; only in hindsight did she realize what was happening:

[I saw a] person taking a picture of a guy at the library, and ... they were laughing around 'cause he was a heavier-set guy. I didn't think anything of it at that time but after ... there was a trend going around social media of people taking pictures of each other and giving rude comments about it ... I was upset 'cause that person [is] just walking doing their normal stuff. They had no idea what was going on. I feel that's an invasion of privacy on their part. (P4)

The spread of such memes, especially in a college circle, can impact undergraduates' privacy and undermine their reputations [67]. Over half of our participants (N=13) were concerned that recipients would share photos with a wider, 'unintended' audience:

My roommate just went to Mardi Gras so she was dressed up really crazy and probably had too much to drink ... and would Snap individual people, but her friends would take a screenshot of it and upload it to Facebook and would be like, "Oh my gosh my friend's so funny." She was kinda like, "Why are they posting these? I know they're funny, but I send them privately to you for a reason" ... She contacted them and asked them to take it down, but I remember her dad called her and was like, "What is this picture?" He just didn't like what she was doing in the picture and people were commenting, "You're so drunk." (P10)

P10's roommate expected her shared photos over Snapchat to 'disappear' soon after being viewed by the specified receivers, but the unexpected sharing on other social media violated her privacy. This dissemination of privately shared photos by a friend to an unintended audience put P10's roommate in an embarrassing situation and opened a door for others, including her father, to judge her ways of celebrating. P15 explained the difference between a few reshares versus going viral: "[I]f one of my friends post a photo of me doing something stupid and it gets 10 retweets, that's ... not enough to truly hurt my reputation. But if it goes viral then people are knowing me as that guy that did whatever."

4.2 Group Privacy

Students were not just concerned about their personal privacy. Some participants (N=6) sought to maintain their privacy in order to maintain their groups' privacy (e.g., sorority or fraternity, IT department in university, and family) as they see themselves as "an extension" of the group (P6). Lampinen *et al.* [44] calls this 'mutual consideration' – one trusts others to be considerate of their privacy boundary-regulation efforts and puts in the effort to be deemed trustworthy in return. Four participants who were all members of a sorority described how they were required to provide their chapter with all their social media accounts for monitoring, and how particular members of their chapter were responsible for overall monitoring of social media for photos that would harm their organization's image:

We have people that, like, watch all our accounts so if you're ever drinking in your letters [in clothes with the sorority's name on them], that's a big no-no because our nationals can see it, and our chapter will be in trouble. So if you ever post a Snapchat at a bar or a party and you have your letters on ... you'll be asked to remove it ... [T]hat's a position in our house, to look at social media. (P11)

Sororities also created house rules to prevent context collapse as described earlier. For instance, P11 noted that her sorority does not allow red Solo cups in any pictures because "people will automatically think 'alcohol'. "

Aside from more formalized rules at sororities, P19 described being aware that any activities in his photos could be interpreted as being condoned by his organization:

There are times I totally forgot what I'm wearing [my work uniform], and I'm drinking and smoking weed. I'd rather that when people start taking pictures that I changed or something ... I'd rather not [make] people directly tie drugs to the place that I work at. (P19)

P19 knew that wearing his work clothes might impact the organization's image – he would not want his actions interpreted as the organization condoning or encouraging drinking or smoking marijuana.

Even family reputation can be impacted if family members shared a risky photo, as P2 recalled in this incident with her sister: "[My sister] sent an inappropriate [photo] to someone, and we were afraid that it was gonna get posted. Our family doesn't really have that reputation" (P2).

5. FINDINGS: WORKAROUNDS TO MANAGE PRIVACY

Previously, we articulated why undergraduate students worry about their individual and group privacy with digital photography and SNS. This sets the scene for our main focus: when they found technology lacking, participants had to create various *workarounds* (WAs), both individually and collaboratively, in various stages of a photo's lifecycle to ensure safe sharing that would not harm one's privacy.

Our results are framed through an experience model (see Fig. 1) that describes the workarounds through the photo lifecycle in college students' lives, which sheds light on the unique design opportunities for each negotiation point in the model. In this section, we first explain the concept of experience models. Then, drawing from our analysis, we describe four stages of a photo, starting with its potentiality to exist and to the phone when it is shared on social media.

5.1 Experience Models

Due to the integral role of photos in everyday life, researchers from different disciplines have examined the *lifecycle* of photos [39, 65, 14, 12, 13]. These models examine photos from the perspective of understanding the activities (e.g., reviewing and organizing) people perform with their digital photos after capturing but prior to their end use (e.g., sharing) [39] and how the assignment of phases in the mobile photo lifecycle to different platforms affects social discourse around

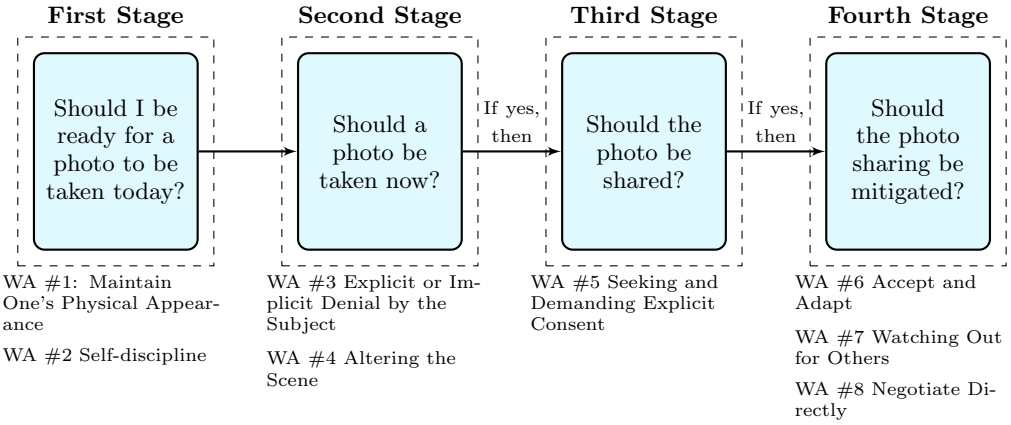

Figure 1: Experience Model: Privacy Workarounds for Surveillance from Everyday Photography

shared photos [65]. Chalfen [14, 12, 13] introduced a 'sociovidistic' framework for the communication activities of films, snapshots, and their artifacts in terms of events (e.g., filming and editing) and components (e.g., participants and topics). Although these models have given us an important temporal understanding of photography and its social use, they have not focused on how we might see the life of photos as intersecting with our privacy in everyday life.

In this paper, we introduce an *experience model* to examine this intersection. Experience models – visual models that facilitate design insights based on ethnographic research – have seen widespread use by ethnographers, especially in the industry [38, 5, 37]. They address the "gap between ethnographic description and the design of technology" [37, p. 2], and are particularly suited to our goal of deriving design insights through qualitative interviews.

An experience model is also "explanatory and developed in a way that has implications for strategic action" [37, p. 2]. Researchers can build upon and refine our model, and can also build other maps on top of our model as they wish. We will present one opportunity map to identify intersections with existing and future designs [37]. Thus, the experience model is both representative and generative.

5.2 First Stage: The Potential to Be Captured in a Photo

All participants remarked upon the pervasiveness of photography. Particularly in public spaces, there is now a constant awareness of the ever-present potential for photos to be (sometimes covertly) taken of anyone, by anyone, in everyday life. This sentiment parallels the feeling of constant surveillance in a modern 'panopticon' [26]. Most participants reported being alert to their environments and actions.

Workarounds at this stage address the following question, "**Should I be ready for a photo to be taken today?**" Our results reinforce Besmer et al.'s findings that people are most concerned with how audiences from their *own* social circles would perceive photos in which they were tagged [6]. However, our participants were also concerned with those to whom they had weaker ties – especially strangers and acquaintances who might perform 'secret captures' (i.e., surreptitiously-taken photos). Participants accepted that they would occasionally appear in strangers' photos as someone in the background; however, many (N=14) specifically feared secret captures (i.e., surreptitiously-taken photos) featuring themselves because of its content (e.g., something embarrassing), what would be done with it (e.g., a caption added to make a meme), and where it might end up (e.g., on popular social media). In other words, the life of the photo would be entirely out of their control:

It's . . . the fact that you don't know where [the photos are] . . . gonna end up. You would hope people won't post them anywhere else. Just that uncomfortable feeling, which is weird to think about because we're . . . photographed every day, without our knowledge, without being aware of it. (P9)

Thus, from the beginning, participants were worried about the potential impact of photos on their privacy.

Our participants sought to enact their views of what constitutes appropriate digital photography to evaluate the potentiality of someone taking a photo of them without their knowledge. Most participants (N=17) were keenly aware that their location (e.g., bar, party, living room, and bedroom) could put them at greater or lesser risk of inappropriate photography to be taken for them. Public places were especially worrisome because of strangers and the difficultly to scan for potential photographers effectively and completely:

[N]ow people don't care about other people's feelings, so they'll just whip their phones out and take pictures of them and make fun of them. I think that's crazy, but that's kind of affected the way I look at other people, or I don't want to eat in public or do other things in public because I'm like, "Oh my gosh . . . That could happen [to me]." I think that has affected my behavior in that aspect. (P4)

For instance, bars were prime locations for cameras to capture people whose guard were down and whose appearance might cause later regret. P14 described always being worried about being watched in bars: "I'm thinking about hanging out with my friends, dancing, having a good time, getting another drink. It's very subliminal, that thought . . . that people are watching you or taking photos" (P14). P18 reiterated that sentiment, saying, "I know that, for the future, I will not want to get really intoxicated in public because I do not want my picture taken" (P18). Small, private spaces,

like parties, were also of concern: "[S]o many people are just holding their phone and prepared to Snapchat some embarrassing moments" (P23). Thus, concerns of photography and space centered around the potential for photos to be especially vulnerable to judgment and misinterpretation.

Participants also told us that vulnerable photography was equally likely in spaces where people expect a higher level of privacy (e.g., living rooms and bedrooms). The very comfort and familiarity one expects in these private, domestic spaces makes the potential of compromising photos even greater. Roommates might document casual conversations, when one is "being kind of goofy" (P19), or general messiness:

When my roommate likes using her phone and [it] is facing toward me sometimes, I would think that she might be taking a picture. Like I don't really care, but there's like a teeny tiny sense of nervousness to it ... I'm not facing a mirror every day; I don't really see myself. Maybe, you know, I'm dressed funny or something and she sees it but I don't. (P5)

The resulting prospect of context collapse in any location and the lack of technical solutions to help with that led students to adopt various WAs to minimize the risk of inappropriate photos, regardless of where they were taken.

5.2.1 WA #1 Maintain One's Physical Appearance

Maintaining good physical appearances (e.g., good taste in clothes, neat hair styles, natural facial expressions, and proper eating habits) was a key (N=14) WA to protecting the propriety of any photos captured of participants. One's appearance was a concern most often mentioned by our women participants (9 out of 12). Men (3 out of 11) also expressed this concern: "[I]f I'm drinking, that's really the only time I'm concerned with [a shared photo], or if I don't think I look good, or if I'm in my pajamas" (P10).

Participants expected friends and family to record and share their activities in events with large attendance, like parties, and they planned accordingly: "I know if I'm going to a social gathering, like a lot of people are gonna take pictures so I make sure to do my makeup and do my hair and I'll wear a new top or whatever" (P6).

5.2.2 WA #2 Self-discipline

To better control their privacy and identity, people engage in self-discipline, modifying their behaviors in both their online [44, 85, 18] and offline worlds [10, 6]. Participants accepted the fact that they would be unable to directly prevent photos taken of them. The majority of our participants (N=15) reported being highly conscious of their surroundings and engaged in *self-censoring* behavior, omitting or curbing their activities to prevent context-dependent photos (i.e., activities open to interpretations). Even in social events where they were surrounded by their friends, some individuals reported carefully regulating their actions to avoid compromising situations that could be captured by others: "I'm very careful about what I say and do around people because I don't want them to share that information with future employers or something like that" (P2). P10 finds herself "just trying to avoid doing things I wouldn't want other people to see unless I was in my apartment or by myself or with my roommates." This decision is often based on having previously witnessed negative consequences for other people who did not censor their behavior:

There's been a time I saw someone really intoxicated, you know, making a scene and yelling, and they probably could have been videoed or something ... That just changed me because I don't really want to be like that ... I will not want to get really intoxicated in public because I do not want my picture taken. (P18)

Participants also reduced the amount of selfies or photos taken of one's friends while drinking or dancing. By self-censoring and continuously monitoring their behaviors, these individual WAs allowed participants to regain some control over their privacy, preventing their unknowingly captured actions from being judged and harming their privacy.

We now turn to the second stage in the photo lifespan, when there is direct evidence that a digital photo is imminent.

5.3 Second Stage: Imminent Photography and Altering the Scene

This stage covers the brief period from when someone is about to take a photo until the photo is actually taken. Our findings show this is a key point that asks both the subject and bystander, "**Should a photo be taken now?**" Of special interest are workarounds that involve implicit and explicit denial of consent to the photo taker as well as the alteration, or arrangement, of the physical scene to be photographed to protect privacy.

5.3.1 WA #3 Explicit/Implicit Denial by the Subject

When subjects felt that a photo shot is imminent, they had to react directly. Some participants (N=6) mentioned explicitly prohibiting photos from being taken, often because they would be depicted unflatteringly. Current appearance was one such reason for not wanting to be photographed: "I was at my friend's apartment the other day, and my hair was a mess, and I didn't want to be in their Snaps so I was kinda like, 'Hey, can you not?'" (P10).

Participants did not always try to explicitly prevent a photo from being taken. Instead, when participants did not want to be in a photo, they (N=4) employed a WA to physically step out of the frame: "I would just tell them if I didn't want to be in [the pictures] or avoid the area where they are taking pictures ... I would either get out of the frame or ... if I wanna be in it, I'll be hyped up and be like, 'Yeah!'" (P10). P9 and P2 also tried to avoid being in strangers' photos because they did not know where these photos would end up:

There's this party I went to where the guy kept taking pictures of his phone. He had like a professional light and everything, and I think there were a few concerns of where the pictures would end up. I mean, you'd think probably just some Facebook, but ... I don't really like my picture being taken if I'm not aware of how it looks. I kind of try not to be in pictures. (P9)

5.3.2 WA #4 Altering the Scene

Drinking (N=18) and dancing (N=7) were the most frequently mentioned activities of concern, and both subjects and photo takers spoke of ways of altering their behaviors when a photo was imminent. With drinking, undergraduates' main concerns were less about underage drinking; instead, they were worried such photos would be posted on social media and affect their relationships:

I wouldn't want people sharing photos of me or posting that I was at a party and drinking alcohol, because, first of all that's illegal for me, and I wouldn't want to be tagged in [it, or] my mom to see it. That would obviously cause a lot of tension between us [me and mom] and would just ruin my reputation 'cause ... I work hard at school. (P2)

Most of the time, a collaborative workaround was needed to ensure a 'clean' shot that would not compromise anyone's privacy in the future. Interestingly, participants (in the role of photo taker) described altering the scene before taking a photo to make a safe photo for a social media post. P4, in the role of photographer, said she always tries to keep alcohol bottles, glasses, or cans out of her pictures:

If I'm out with friends and I do take pictures, I make sure even if they're drinking then I'm not taking pictures with that ... I'm very self-conscious because I don't want [my parents] to think I'm doing those things. If I'm hanging out at a friend's apartment and they do have alcohol, I make sure not to include that in the picture. (P4)

Participants, as the subjects of photos, reported changing or stopping certain actions as soon as they noticed a photo was about to be taken. P1, for instance, explained how she stopped dancing as soon as her friend started to record them: "[W]e were dancing around and acting stupid, and my friend started recording us ... so I stopped dancing ... People would poke fun at me ... I'm just a terrible dancer." (P1)

The questions of whether a photo had the consent of subjects and whether the shot was 'clean' leads to the next stage where the photo exists but has not been posted online.

5.4 Third Stage: The Taken Photo

In this brief stage (before a photo is potentially shared on social media), a photo has now been taken by someone of a subject with (possible) bystanders. With the photo now being a more viable object for putting one's privacy at risk, workarounds turn to the actions that might be taken before possibly posting the photo on social media. Our data reveals one key point: **"Should the photo be shared?"** – actors must decide whether to disseminate the photo. For our college students, sharing usually meant posting the photo on social media. The lack of collaborative tools to facilitate privacy and sharing negotiations force participants to adopt workarounds to enable the safer sharing of photos. Although in most cases participants allowed photos to be shared, they also engaged in workarounds to ensure safer sharing by manually and mutually (with the photo taker) evaluating activities depicted in the photo before sharing the photo.

5.4.1 WA #5 Seeking & Demanding Explicit Consent

When asked how individuals should share photos about others, more than half of our participants (N=16) mentioned the necessity of proactively seeking *consent* from people who are involved in a photo *before sharing* – and sometimes before even taking the photo. Although some social media provide tools to facilitate such consent *after* sharing (e.g., tagging requests), most of them do not offer any tools to approve a sharing request before sharing a photo, which forces participants to adopt WAs. Asking for approval demonstrates responsibility and respect towards others, and the way participants would like others to treat them. Students often do not want to put their friends in harm's way: "If I'm taking Snapchat of someone I will always show them ... I don't want to post anything ... or send it to somebody they're not okay with" (P17).

Mutually negotiated approval allows everyone to be confident that photos will not invade one's privacy. This strategy is not seen as onerous since participants felt many peers were accommodating and reciprocal with this preventive strategy. P3 describes one instance of how this strategy works:

[W]e were finally moved in! Finally roomies! And we took a picture and she was like, "Oh my god my hair looks bad!" So we took a picture like 5 times to get a picture perfect so we could post it on social media. (P3)

Similarly, P10 explains her regular routine: "Before I post pictures I say, 'Hey look at my photos from the night before,' and we'll pass each others phones around, see if there's any good pictures or bad ones and say, 'Hey don't put this up' or 'Let's delete this'" (P10). Here, her friends help her reach an informed decision on what photos would be appropriate and not prone to negatively affecting their reputations.

Collectively approving a photo before posting is not always an option, nor is it the last step of preventing privacy violations. There remains a final stage of a photo open to negotiations: after the photo is shared online.

5.5 Fourth Stage: Photo as Shared Object

In this stage, a photo has already been shared online through social media. Students here asked, **"Should the sharing of the photo be mitigated?"** – how can one reduce the risk (i.e., possible impact on privacy) of a photo that has already been posted online? Interviews showed that students actively negotiate to decide the appropriate WAs to mitigate the risk of an undesirable photo posted on social media.

5.5.1 WA #6 Accept and Adapt

A few participants (N=6) simply accepted the risks associated with their photo being shared online when considering the downsides of confronting social contacts, since that might affect their relationships. Instead, participants *accepted* and *adapted* to the reality of posted photos that did not meet their approval. They mentally brushed off the effect these photos might have on their privacy, or convinced themselves they were overreacting:

I'll send videos of myself being kind of goofy or putting on really silly voices for my girlfriend. I'll ... tend to assume what I'm saying to her is in confidence, and sometimes she'll post one of those silly videos I made just for her onto Instagram, so I'm a bit embarrassed and feel vulnerable ... I try to work on being less self-conscious, so I let it slide pretty much, and she's less self-conscious than I am. (P19)

Avoiding conflict was preferred because participants felt that the negative impact usually is limited, and they would confront others only if there were serious threats to their privacy through misrepresentation that can cause context collapse. P1 explained that most of the time, it is not "worth putting a fuss about. If it was something ... that misrepresented me as a person, I'd probably say something."

5.5.2 WA #7 Watching Out for Others

Students rely heavily on their friends to remain vigilant about any undesirable shared photos that could put their

privacy at risk. They trust their friends to watch each others' backs on social media and warn them of any risks:

It was snowing and [my friend] was wearing open-back moccasins. One of her friends saw on a guy friend's Snapstory ... like, "Who is this girl wearing moccasins?" and she was like, "I know who that girl is." She took a screenshot and sent it to her. She was so weirded out. Cause it was a random guy who made fun of her. (P10)

As we mentioned before, social media accounts of students who live in Greek-letter organizations may be monitored to ensure clean sharing that does not harm the chapter's image. To achieve that, students reported collaborating together to get this mission done and not solely depending on the person formerly assigned to this mission. In some cases (N=4), vigilance translates into direct confrontation with transgressors on behalf of friends, especially with salacious pictures:

I knew a guy who got mad at this girl, and he had a picture of her butt. And on her butt he had written his name in marker. She thought she sent it just to him, but he got mad and posted it on social media ... I actually called the guy 'cause I knew him and I was like, "Look just take that down because that's pretty embarrassing," and it was a really shy girl ... Well, he took it down immediately. (P15)

5.5.3 WA #8 Negotiate Directly

When a shared photo might compromise someone's privacy, participants worked around by engaging in *direct negotiation* to mitigate risk and reclaim context. Most of our participants (N=12) had asked at least one person they knew to delete a posted photo. Since SNS do not provide built-in functionality to facilitate such negotiations, students used workarounds to take matters into their own hands. Negotiation often took place offline, mainly face-to-face. Participants recognized that once someone took ownership of a photo, they had no control over it and could not remove their digital footprint by themselves. They must instead negotiate with the account owner: "On Facebook it's easier ... You can just untag yourself. The concern is that it's still on someone's page, there's not much you can do besides convince them to delete it" (P9).

As mentioned earlier, students are selective in making their requests. They are tactful to both save face and preserve the friendship; they avoid ordering their friends to remove the disputed photo: "I'm just like, 'I look weird take that off' because that's the best way to approach people about stuff like that. Not like coming in really mad and stuff like that" (P22). Students may indirectly and jokingly warn their friends about their concerns: "My friends and I always joke, if we just send each other a stupid face, and we screen shot it we always call each other out like, 'Oh my gosh, I trusted you. It's Snapchat, that's not what you're supposed to do'" (P14). Underlying this humor is serious intent to negotiate a different ending to the photo's shared existence.

6. A DESIGN OPPORTUNITY MAP FOR PHOTO SURVEILLANCE

Our experience model suggests that, in response to the ubiquity of digital photography and SNS, undergraduates now enact a constant, low-level state of watchfulness. It is directed outwardly, toward those in physical and virtual proximity, and, inwardly – toward the self – as these students try to provide as little opportunity as possible for others to subject them to negative, long-term social sanction. This watchfulness is a logical consequence or "harm" of surveillance [63, 68, 56], but not of surveillance by the government or intelligence agencies or even corporations. Rather, it is the consequence of an informal social network of average citizens, including one's own friends and family, all of whom are armed with smart phones and social media accounts. In lieu of technological solutions, students perform workarounds incorporating a dynamic collection of people, practices, rules, devices, apps, and services to manage their privacy. This has an impact on their daily lives, adding to their individual burden of privacy [54]. These students worry that information about themselves and their intimate groups, often captured by themselves or others on social media, might be misunderstood or misused by others when appearing out of its context [55, 9, 73], resulting in negative consequences [4] for them or even losing their reputation [67]. Young adults' watchfulness adds nuance to previous work (cf. Section 2) on individual and collaborative strategies to manage privacy through both online and offline channels.

Moreover, our experience model describes watchfulness as not simply a response to the physical ubiquity of cameras but to the temporal persistence that surveillance via digital photography entails. Just as they did in high school [9], our students manage their boundaries and "presentations of self" [28]. Now, however, the stakes for maintaining students' privacy are indelible and include the loss of scholarships, jobs, and leadership opportunities in addition to the kinds of relationships they might want to have with others. In such a world, where anyone may be instantly, permanently spotlighted, everyone starts to look like the paparazzi.

The necessity of workarounds highlight that pervasive photography and the lack of technology to facilitate their needs forces students to form and respond to models of informational norms of collection and dissemination, both in face-to-face and online interactions. Students predict the vulnerability of photos by examining factors that might likely become misinterpreted (e.g., places). They describe an increasing awareness of invasion of privacy from secret capture by both friends and strangers. They engage in self-censoring behaviors in face-to-face interactions, enact intentional boundary work across different social media platforms, negotiate with each other over shared expectations and practices, and adopt positions of personal and social vigilance to prevent and respond to cases privacy invasion.

We will describe an *opportunity map* – a mapping from our experience model to design directions for researchers and practitioners to pursue [37] – that provides two design approaches to our experience map. First, it provides a way to identify and organize design requirements by temporal stages in the lifespan of a digital photo. With this map, we can readily survey what aspects of privacy management in a stage current designs address and do not address; in particular, it points to the need for designs to address the underlying causes of WAs. These design opportunities are grounded in our findings but are nonetheless speculative and sometimes future-oriented; they are not fully fleshed out solutions to the concerns of photographic surveillance. Second, our map provides designers ways to envision boundary management as not an isolated series of actions but as in-

terconnected. This perspective, for example, suggests new design avenues for dealing with surveillance from shared digital photos that address multiple stages.

6.1 Designs for Individual Stages

Since the emergence of social platforms and mobile cameras, researchers have proposed various mitigation strategies that are applicable to different stages of our experience model; we have arranged these solutions onto our model in Table 1. Social media platforms such as Facebook, Snapchat, and Instagram already support some privacy protection techniques where a subject can, for instance, 'untag' themselves from, or report, an offensive photo (Stage 4). Yet, such photos can still persist and continue to be shared. Much of the existing work has focused on Stages 1 and 3, where the user can specify regions, places, objects, and attires to be identified; these solutions protect their privacy by blurring or tagging photos that have these attributes. Some prototypes allow the user to alter a photo by marking or specifying sensitive areas [62, 76, 41] or setting up a privacy policy [64]. Other prototypes propose wearing additional accessories such as special stickers [75], clothes, and bracelets [42] to blur the subject's face in a captured image. Still other prototypes support Stage 2 by restricting photos in controlled environments.

Most of the existing prototypes support multiple stage interventions with some customizations. However, our experience model identifies a gap in designs that consider workarounds through different photo stages for privacy management. These prototypes are too specific; there is a need for more general-level designs giving more control to the subjects and bystanders, not just the photographers. Designs also need to consider how participants often prefer collaborative and collective strategies to mitigate privacy risks.

Many of the design directions we introduce below involve the integration of different devices and software into the ecosystem of digital photography and SNS. We do not have easy answers on how this will be accomplished but surmise that we will need technical solutions coupled with new policies. Scholars will need to consider how standards and processes can be developed between disparate stakeholders (e.g., software and hardware camera companies). Alternatively, we will need designs that are capable of defending against adversarial systems; such advances may only be practical when the appropriate sensors or algorithms have been researched (e.g., sensors that can detect camera activity). In the next subsections, for each stage, we discuss design opportunities, speculative designs that address these opportunities, and the research challenges of implementing such designs.

6.1.1 First Stage: Designing for Potential Captures

Opportunity: Actors live daily with the ongoing potentiality of a photo harming their privacy being taken with or without their awareness.

Designs that work despite the absence of communication between visible and invisible actors taking photos. There is a distinct lack of communication between the photographer and subject; one does not realize that a photo will be taken in any given moment. New designs would allow photographer and subject-specific systems (i.e., smartphones or tablets) to interoperate with each other to notify subjects about covert attempts to take their photo.

Designs that maintain preferred practices to prevent the creation of photos vulnerable to context collapse. Participants act idiosyncratically based on their own WAs to protect their privacy (e.g., self-disciplining their physical behavior and appearance at all times) from unknown and unobservable capture. Based on self-selected behaviors, designs may remind users to maintain certain workarounds. Such designs are analogous to apps like the 'Drunk Mode' app used by our participants to prevent themselves from taking photos that might affect their self-presentation negatively.

6.1.2 Second Stage: Designing for In-the-Moment Maneuvers and Scene Alteration

Opportunity: Photographers felt it was unnecessary to obtain consent from parties that might be involved when a shot was imminent. It was up to subjects and bystanders to react immediately to evidence of such a capture.

Designs that support in-the-moment maneuvers. College students reverted to face-to-face, in-the-moment WAs because technological solutions to convey their privacy and personal preferences regarding imminent capture were not available. In-the-moment capture requires a time-sensitive solution that communicates preferences to the photographer, whereas the previous stage requires an omnipresent, overseer-type system. Researchers will be challenged to find solutions sensitive to the social nuances of negotiating capture when the photographer and subject are in proximity.

Designs that support socially unobtrusive rejection of capture. These designs would alert subjects that photography was imminent in their area, allowing them to move out of the camera's physical frame. Designs may help subjects and bystanders visualize an active photographer or the path of a camera's focus. Lastly, designs may alert photographers themselves of social, even formal rules of capture tied to a location and/or event (such as a sorority party). This solution, for instance, may require a form of crowdsourcing to label a current location as the site of an occasion with rules.

Designs that evaluate how 'safe' a photo is. Participants reported manually scanning the scene before captures to ensure subjects were safe from potential contextual collapse (e.g., no drinking, no embarrassing dancing, and no Solo cups). Designs should support participants' active, in-person evaluations and allow negotiation over with whom to share the photo – this suggests designs need to support segmentation (i.e., an awareness of multiple photo sharing platforms and their use-cases for particular audiences).

6.1.3 Third Stage: Designing for Photo Negotiation

Opportunity: In this stage, the photo exists, and participants enacted WAs to determine whether it should be shared.

Designs that support in-situ photo negotiation. When negotiating the sharing of a photo, participants asked (or were asked) for consent face-to-face, away from the online world in which the photos would be shared. Participants found it more expeditious to seek consent in-person immediately after the photo was taken and before sharing it. Previous research has highlighted the need to facilitate in-person collaboration over photo sharing in social media sites [72, 43, 85, 79, 16, 36, 50]. However, SNS still lack a negotiation tool to notify involved parties before sharing the photo. Parties

Current Design/ Prototypes	Stage 1	Stage 2	Stage 3	Stage 4
BlindSpot [58]		×		
World-driven access control [64]	×	×		
PrivateEye [62]; PrivacyApp, PrivacyFabric, Privacy Bracelet [42]	×		×	
PlaceAvoider [76]; TagMeNot [75]; ScreeenAvoider [41]	×		×	
Obscuring scene elements [31]; Cartooning [32]; Snapme [33]			×	
Collaborative Privacy Management [69, 36]			×	×
Restrict Others [6]; Facebook; Snapchat; Instagram				×

Table 1: Designs and the stages of the Experience Model they support

need a mechanism that works at the site of capture, in-situ, directly after the group photo to facilitate obtaining consent. Additionally, a remote version would allow sharing to be decided after-the-fact. Researchers will need to investigate solutions that incorporate information such as the identity of people in a photo, one's social network, and the physical locations of relevant parties.

6.1.4 Fourth Stage: Designing to Shield from Consequences

Opportunity: In this final stage, people's privacy has already been compromised. Students had to find WAs with photographers. Those who chose to avoid conflict with the photographer had to accept the risk of unwanted disclosure. A few participants resorted to technical means to protect their privacy, untagging themselves from posted photos.

Designs that mitigate consequences. Participants spoke powerfully of the effects on their reputation from photos that were vulnerable to context collapse. How can we both mitigate damage on reputation and help one recover their reputation from these already-taken photos? Future research should address this under-investigated area.

Designs that support socially acceptable workarounds of photo removal. Direct negotiation is a means by which many participants got photos to be deleted. Scholars will need to address the challenge of supporting negotiation that is tactful or even passive. Designs might allow users to convey that they want a photo to be removed through the use of humor about the content or subject of the photo – this avoids direct conflict between subject and photographer while still communicating that the photo is inappropriate for sharing.

Designs that ease concern about consequences of context collapse. Some participants, after some consternation, simply accepted that context collapse had happened. Uniquely, systems might help users come to a realization that a risky photo may not adversely effect their reputation. Such systems may pose scenarios with similar photos and demonstrate that the consequences were not as dire as they seem now, and that the users should take the photo as a learning moment. Researchers will need to create appropriate exemplars that can form the basis of these scenarios.

Designs that support vigilance (i.e., 'neighborhood watch'). Bystanders sometimes alerted subjects that someone had posted a photo of them on social media without their knowledge. A system that supports such neighborhood watch-type communities would leverage the power and motivation of particular organizations (e.g., Greek communities or college career services) or social groups (e.g., close friends). Such crowd-sourced watching might root out reputation-damaging photos before they propagate widely but would need to avoid inadvertently creating a system for cyberbullying.

6.2 Photo Trajectories: It Takes a Village...

Our experience model visualizes the trajectory of workarounds for managing privacy throughout a digital photo's lifespan. Thus, aside from gleaning what systems must do at each specific stage over a photo's life, a wider, more significant contribution of our model is in highlighting issues germane to the photo's trajectory. Our experience model highlights several concerns that are difficult to see in any individual stage but are eminently visible when we step back and look at the entire process. Our central message here is that for college students – akin to the African proverb, "it takes a village to raise a child" – it takes an entire social group to help manage each others' privacy, thanks to digital photography. This perspective, we believe, is more in-line with what our participants actually do to manage their privacy – they enact collaborative workarounds in individual stages of a photo in service to a long-term, curated representation of themselves. We identify design opportunities and challenges to support this perspective on privacy management to produce photos with a 'healthier', more privacy-sensitive life.

6.2.1 The Power of the Photographer: Empowering the Subject and Bystanders, too

In each stage of our model, we observe that the photographer remains a powerful actor. Photographers have overwhelming power in deciding to digitally capture, alter, and disseminate a photo. In Stage 1, the workaround space is large and untenable, out of the subject's control. The photographer's actions are not moderated, and instead, it behooves the subject to alter their own physical behavior or routines to protect their privacy. In Stage 4, the photographer has already released their photo to the online world where it can be endlessly modified and disseminated, after which the photographer bears no responsibility for their digital progeny. Even in a collective network like Facebook, the only two options for subjects to deal with unflattering photos they are tagged in are to untag themselves and ask the uploader to delete the photo [23], making the subjects feel helpless to enforce their privacy preferences. In Stage 2 and 3 – when the photo is imminent and taken, respectively – the photographer is bound by social conventions to negotiate with those physically around them. Yet, the camera device, perhaps a smartphone, remains under the photographer's control. The photographer may pass their smartphone around for their

friends' review, but it is understood that the owner of the smartphone will be the one pushing the 'delete' button.

The power of the photographer lies in the sites in which both capture and sharing happen – in the hardware and the software possessed by the photographer. We suggest that designs should *dilute* the concentrated power of photography that currently resides with the photographer by spreading it across all interested actors. For instance, we should investigate technical opportunities to give power to subjects and bystanders at all stages of the photo's existence. Such solutions will need to answer difficult questions on how to *work around* conflicts. For instance, we can imagine a user toggling a 'do not share photos of me' setting on their smartphone's OS. If the photographer takes a shot in a tourist spot, with many potential subjects having turned on this feature in their phone, this may ruin the photographer's experience – it will be impossible to frame a photo without an opt-out person in the background. Should we rob the photographer of their power to take a photo for their aesthetic goals? Such solutions could rely on the *propriety* of photographers [34] to honor 'requests' sent by the subjects – even if photographers may have the ultimate power of the veto, technical mechanisms are needed to enable a more seamless negotiation than the current status quo.

6.2.2 Making Past Workarounds Visible

Once a photo has been shared (Stage 4), the user has no idea what the photo has gone through. For example, did all co-owners (photographer and the subjects) of a particular photo approve it to be shared online? With whom? Could past workarounds of a photo be visualized? What if we could see to what degree different actors' decisions allowed the photo to reach its current state? If future designs are able to automate collaborative workarounds of various stages, a system may attach to the photo visualizations that indicate its negotiated nature – key decisions made, by whom, where (physically), and at what stage. Then, the photo would bear the mark of its history. This might look like the functionality for Facebook that allows anyone who can see a published post to see its 'edit history' [22].

By making past workarounds more visible, we can empower users, and even social platforms, to better determine the appropriateness (possibly including the factualness) of the photo in terms of privacy and context collapse. If a photo shows strong vetting, the social platform could prioritize the photo's appearance in contacts' 'newsfeeds', for example. Alternatively, a user may choose to alert a social platform of a poorly vetted photo and/or have an option, themselves, to prevent its further dissemination by refusing to share that photo. Novel technical mechanisms that reveal past workarounds of a photo may thus add assurances to the platform and its users as to how the photo should be displayed or further disseminated. This also interestingly suggests that the *solution* to human workarounds does not lie simply in eliminating them via technology (which can be technically intractable and perhaps unwanted) but rather in rendering them visible – via technology – to the user.

6.2.3 Making Future Trajectories Visible

Not only should systems support making past processes and practices visible in digital photography, they should also intelligibly highlight the possible privacy consequences of photos. Although researchers have suggested that social networking sites need to learn from the online, privacy-preserving behaviors of people [25, 30], our findings suggest a need to *combine data on behaviors in both the face-to-face and online worlds in order to address privacy.* For instance, mobile photo applications now support 'augmented reality' modes, where the camera feed is annotated in real-time. Social platforms can offer a comprehensive suite of tools that include a 'privacy-respecting camera' in Stages 1 and 2 in addition to affordances in other stages. These cameras could overlay the display with indicators of potential context collapse as well as subjects' privacy preferences. Facial analysis of expressions could attempt to predict vulnerability to context collapse. Inference of activities, such as parties and whether such activities constitute grounds for self-censorship, could provide additional data to algorithms designed to reduce context collapse. Importantly, while such analyses and predictions can be performed at later stages by the social media platform, creating a 'privacy sensitive camera' offers unique opportunities for social platforms to tackle privacy at the nascent stages of a photo's life.

7. CONCLUSION

Our study shows that college students are acutely aware of pervasive photography in their lives and how photos taken out of context can impact their privacy. They engage in various 'workarounds' (where technology fails) in an attempt to manage their privacy. Young adults engage in a combination of behaviors at various stages: they know a photo can be taken at any time and adjust their behaviors in case a photo is taken; when a photo is about to be taken, they employ explicit and implicit measures to prevent a photo from being taken; after a photo is taken the photographer and subjects deliberate whether the photo should be posted to social media; and finally, if a photo is shared, friends look out for each other and attempt to remove damaging photos. By reaching theoretical saturation with coding, we believe our findings accurately capture the workarounds undergraduates enact in a world of constant photographic capture and sharing. We, however, warn against generalizing since our participants were in higher education institutions in a particular cultural setting. Future work will further test the validity of our models, perhaps through the use of surveys that will reach a wider, more representative sample.

We organize our findings on workarounds using an experience model, an established framework to facilitate design insights from fieldwork, and present a design opportunity map based on the experience model. This design opportunity map surveys current privacy systems and identifies future design opportunities for privacy management. For instance, it highlights the need for designs to support interoperability between different ecosystems, rejection of imminent photo captures, in-situ negotiation before sharing photos, and easing the psychological anxiety of photo sharing. Importantly, our map provides a holistic framework for design that aligns with the temporal, long-term nature of privacy management. A remit to protect privacy impels us to reflect upon designs that challenge the concentrated power the photographer now wields and render visible the past and future work that make pervasive photography work for, not against, people captured in photos.

8. ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under award CNS-1252697. Rashidi is funded by the College of Computers and Information Systems in Umm Al-Qura University, Saudi Arabia.

9. REFERENCES

[1] A. Acquisti and R. Gross. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Privacy Enhancing Technologies*, pages 36–58. Springer, 2006.

[2] S. Alter. Theory of Workarounds. *Communications of the Association for Information Systems*, 34(1):1041–1066, 2014.

[3] I. Altman. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. 1975.

[4] L. Andrews. *I Know Who You are and I Saw What you Did: Social Networks and the Death of Privacy*. Simon and Schuster, 2012.

[5] R. Beers and P. Whitney. From Ethnographic Insight to User-Centered Design Tools. *Ethnographic Praxis in Industry Conference Proceedings*, 2006(1):144–154, 2006.

[6] A. Besmer and H. Richter Lipford. Moving Beyond Untagging: Photo Privacy in a Tagged World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM.

[7] d. boyd. Facebook's Privacy Trainwreck. *Convergence: The International Journal of Research into New Media Technologies*, 14(1):13–20, 2008.

[8] d. boyd. *Taken Out of Context: American Teen Sociality in Networked Publics*. PhD thesis, University of California, Berkeley, 2008.

[9] d. boyd. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press, 2014.

[10] K. E. Caine. *Exploring Everyday Privacy Behaviors and Misclosures*. PhD thesis, Georgia Institute of Technology, 2009.

[11] K. E. Caine, C. Y. Zimmerman, Z. Schall-Zimmerman, W. R. Hazlewood, A. C. Sulgrove, L. J. Camp, K. H. Connelly, L. L. Huber, and K. Shankar. DigiSwitch: Design and Evaluation of a Device for Older Adults to Preserve Privacy While Monitoring Health at Home. In *Proceedings of the 1st ACM International Health Informatics Symposium*, IHI '10, pages 153–162, 2010.

[12] R. Chalfen. *Snapshot Versions of Life*. University of Wisconsin Press, 1987.

[13] R. Chalfen. Interpreting Family Photography as Pictorial Communication. *Image-based Research: A Sourcebook for Qualitative Researchers*, pages 214–234, 1998.

[14] R. M. Chalfen. Film as Visual Communication: A Sociovidistic Study in Filmmaking. 1974.

[15] E. Chell. Critical Incident Technique. In *Essential Guide to Qualitative Methods in Organizational Research*, pages 45–60. SAGE Publications Ltd, 2004.

[16] H. Cho and A. Filippova. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16, pages 503–514, New York, NY, USA, 2016. ACM.

[17] E. K. Choe, S. Consolvo, J. Jung, B. Harrison, and J. A. Kientz. Living in a Glass House: A Survey of Private Moments in the Home. In *Proceedings of the 13th International Conference on Ubiquitous Computing*, UbiComp '11, pages 41–44. ACM, 2011.

[18] S. Das and A. D. Kramer. Self-Censorship on Facebook. In *Proceedings of the International AAAI Conference on Web and Social Media*, ICWSM '13, pages 120–172, 2013.

[19] R. De Wolf, K. Willaert, and J. Pierson. Managing Privacy Boundaries Together: Exploring Individual and Group Privacy Management Strategies in Facebook. *Computers in Human Behavior*, 35:444–454, 2014.

[20] Dedoose, 2016. `http://www.dedoose.com/` Accessed Mar. 1, 2016.

[21] T. Denning, Z. Dehlawi, and T. Kohno. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2377–2386, New York, NY, USA, 2014. ACM.

[22] Facebook. How Do I Edit a Post That I've Shared From My Page?, 2018. `https://www.facebook.com/help/1376303972644600?helpref=uf_permalink`.

[23] Facebook. What If I Don't Like Something I'm Tagged In?, 2018. `https://www.facebook.com/help/196434507090362?helpref=faq_content`.

[24] L. Fasoli. Reading Photographs of Young Children: Looking at Practices. *Contemporary Issues in Early Childhood*, 4(1):32–47, 2003.

[25] P. W. Fong, M. Anwar, and Z. Zhao. A privacy Preservation Model for Facebook-style Social Network Systems. In *European Symposium on Research in Computer Security*, pages 303–320. Springer, 2009.

[26] M. Foucault. *Discipline and Punish: The Birth of the Prison*. Vintage, 1977.

[27] L. Gasser. The Integration of Computing and Routine Work. *ACM Transactions on Information Systems (TOIS)*, 4(3):205–225, 1986.

[28] E. Goffman. *The Presentation of Self in Everyday Life*. Garden City, 1959.

[29] R. Gross and A. Acquisti. Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Misc society*, WPES '05, pages 71–80, New York, NY, USA, 2005. ACM.

[30] M. Hart, R. Johnson, and A. Stent. More Content-less Control: Access Control in the Web 2.0. *IEEE Web*, 2, 2007.

[31] R. Hasan, E. Hassan, Y. Li, K. Caine, D. J. Crandall, R. Hoyle, and A. Kapadia. Viewer Experience of Obscuring Scene Elements in Photos to Enhance Privacy. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '18, pages 47:1–47:13, New York, NY, USA, 2018.

[32] E. T. Hassan, R. Hasan, P. Shaffer, D. Crandall, and A. Kapadia. Cartooning for Enhanced Privacy in Lifelogging and Streaming Videos. *CVPRW*, 1:4, 2017.

[33] B. Henne, C. Szongott, and M. Smith. SnapMe if You Can: Privacy Threats of Other Peoples' Geo-tagged Media and What We Can Do About It. In *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '13, pages 95–106, New York, NY, USA, 2013. ACM.

[34] R. Hoyle, R. Templeman, D. Anthony, D. Crandall, and A. Kapadia. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '15, pages 1645–1648, New York, NY, USA, 2015. ACM.

[35] R. Hoyle, R. Templeman, S. Armes, D. Anthony, D. Crandall, and A. Kapadia. Privacy Behaviors of Lifeloggers Using Wearable Cameras. In *Proceedings of the 16th International Conference on Ubiquitous Computing*, UbiComp '14, pages 571–582, New York, NY, USA, 2014. ACM.

[36] H. Jia and H. Xu. Autonomous and Interdependent: Collaborative Privacy Management on Social Networking Sites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4286–4297, New York, NY, USA, 2016. ACM.

[37] R. Jones. Experience Models: Where Ethnography and Design Meet. *Ethnographic Praxis in Industry Conference Proceedings*, 2006(1):82–93, Sept. 2006.

[38] S. Jones. Grass Roots Campaigning As Elective Sociality (Or Maffesoli Meets 'Social Software'): Lessons From The Bbc Ican Project. *Ethnographic Praxis in Industry Conference Proceedings*, 2005(1):31–52, 2005.

[39] D. Kirk, A. Sellen, C. Rother, and K. Wood. Understanding Photowork. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 761–770, New York, NY, USA, 2006. ACM.

[40] R. Koppel, T. Wetterneck, J. L. Telles, and B.-T. Karsh. Workarounds to Barcode Medication Administration Systems: Their Occurrences, Causes, and Threats to Patient Safety. *Journal of the American Medical Informatics Association*, 15(4):408–423, 2008.

[41] M. Korayem, R. Templeman, D. Chen, D. Crandall, and A. Kapadia. Enhancing Lifelogging Privacy by Detecting Screens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4309–4314, New York, NY, USA, 2016. ACM.

[42] K. Krombholz, A. Dabrowski, M. Smith, and E. Weippl. Exploring Design Directions for Wearable Privacy. In *Proceedings of the Workshop on Usable Security*, USEC '17, 2017.

[43] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen. We're in it Together: Interpersonal Management of Disclosure in Social Network Services. In *Proceedings of the SIGCHI Conference on human factors in computing systems*, CHI '11, pages 3217–3226, New York, NY, USA, 2011. ACM.

[44] A. Lampinen, S. Tamminen, and A. Oulasvirta. All my People Right Here, Right Now: Management of Group Co-presence on a Social Networking Site. In *Proceedings of the ACM 2009 International Conference on Supporting Group Work*, GROUP '09, pages 281–290, New York, NY, USA, 2009. ACM.

[45] M. R. Leary. *Self-presentation: Impression Management and Interpersonal Behavior*. Brown & Benchmark Publishers, 1995.

[46] E. Litt, E. Spottswood, J. Birnholtz, J. T. Hancock, M. E. Smith, and L. Reynolds. Awkward Encounters of an Other Kind: Collective Self-presentation and Face Threat on Facebook. In *Proceedings of the 17th ACM conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 449–460, New York, NY, USA, 2014. ACM.

[47] A. E. Marwick and boyd danah. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, 2011.

[48] M. Massimi, K. Truong, D. Dearman, and G. Hayes. Understanding Recording Technologies in Everyday Life. *IEEE Pervasive Computing*, 9(3):64–71, 2010.

[49] J. M. Morath and J. E. Turnbull. *To Do No Harm: Ensuring Patient Safety in Health Care Organizations*. John Wiley & Sons, 2005.

[50] A. R. Murphy, M. C. Reddy, and H. Xu. Privacy Practices in Collaborative Environments: A Study of Emergency Department Staff. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 269–282, New York, NY, USA, 2014. ACM.

[51] D. H. Nguyen, G. Marcu, G. R. Hayes, K. N. Truong, J. Scott, M. Langheinrich, and C. Roduner. Encountering SenseCam: Personal Recording Technologies in Everyday Life. In *Proceedings of the 11th International Conference on Ubiquitous Computing*, UbiComp '09, pages 165–174. ACM, 2009.

[52] C. Nippert-Eng. Privacy in the United States: Some Implications for Design. *International Journal of Design*, 1(2), 2007.

[53] C. E. Nippert-Eng. *Home and Work: Negotiating Boundaries Through Everyday Life*. University of Chicago Press, 1996.

[54] C. E. Nippert-Eng. *Islands of Privacy*. University of Chicago Press, 2010.

[55] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

[56] G. Orwell. *Nineteen Eighty-Four*. New York: Harcourt Brace, 1977 [1949].

[57] L. Palen and P. Dourish. Unpacking Privacy for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 129–136. ACM, 2003.

[58] S. Patel, J. Summet, and K. Truong. *BlindSpot: Creating Capture-Resistant Spaces*, pages 185–201. Springer London, 2009.

[59] M. Q. Patton. *Qualitative Research*. Wiley Online Library, 2005.

[60] S. Petronio. *Boundaries of Privacy: Dialectics of Disclosure*. SUNY Press, 2012.

[61] Y. Rashidi, K. Vaniea, and L. J. Camp. Understanding Saudis' Privacy Concerns When Using WhatsApp. In *Proceedings of the Workshop on Usable*

Security, USEC '16, 2016.

[62] N. Raval, A. Srivastava, A. Razeen, K. Lebeck, A. Machanavajjhala, and L. P. Cox. What You Mark is What Apps See. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '16, pages 249–261, New York, NY, USA, 2016. ACM.

[63] N. M. Richards. The dangers of surveillance. *Harvard Law Review*, 126(7):1934–1965, 2013.

[64] F. Roesner, D. Molnar, A. Moshchuk, T. Kohno, and H. J. Wang. World-Driven Access Control for Continuous Sensing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 1169–1181, New York, NY, USA, 2014. ACM.

[65] R. Sarvas, A. Oulasvirta, and G. Jacucci. Building Social Discourse Around Mobile Photos: A Systemic Perspective. In *Proceedings of the 7th International Conference on Human Computer Interaction with Mobile Devices & Services*, pages 31–38. ACM, 2005.

[66] S. Singhal, C. Neustaedter, T. Schiphorst, A. Tang, A. Patra, and R. Pan. You are Being Watched: Bystanders' Perspective on the Use of Camera Devices in Public Spaces. In *Proceedings of the SIGCHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI '16, pages 3197–3203. ACM, 2016.

[67] D. J. Solove. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, 2007.

[68] D. J. Solove. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press, 2011.

[69] A. C. Squicciarini, H. Xu, and X. L. Zhang. CoPE: Enabling Collaborative Privacy Management in Online Social Networks. *Journal of the Association for Information Science and Technology*, 62(3):521–534, 2011.

[70] A. Strauss and J. Corbin. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications, Thousand Oaks, CA, 1998.

[71] F. Stutzman and W. Hartzog. Boundary Regulation in Social Media. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, CSCW '12, pages 769–778, New York, NY, USA, 2012. ACM.

[72] F. Stutzman and J. Kramer-Duffield. Friends Only: Examining a Privacy-Enhancing Behavior in Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1553–1562, New York, NY, USA, 2010. ACM.

[73] N. M. Su and L. Wang. From Third to Surveilled Place: The Mobile in Irish Pubs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '15, pages 1659–1668, New York, NY, USA, 2015. ACM.

[74] J. M. Such, J. Porter, S. Preibusch, and A. Joinson. Photo Privacy Conflicts in Social Media: A Large-scale Empirical Study. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '17, pages 3821–3832, New York, NY, USA, 2017. ACM.

[75] TagMeNot. TagMeNot.info. `http://tagmenot.info/`, 2017.

[76] R. Templeman, M. Korayem, D. Crandall, and A. Kapadia. PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces. In *Proceedings of The 21st Annual Network and Distributed System Security Symposium*, NDSS '14, pages 23–26, 2014.

[77] M. Thibault and D. Walbert. Reading Photographs, 2006.

[78] J. Thom-Santelli and D. R. Millen. Learning by Seeing: Photo Viewing in the Workplace. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 2081–2090. ACM, 2009.

[79] J. Vitak. Balancing Privacy Concerns and Impression Management Strategies on Facebook. In *Symposium on Usable Privacy and Security*, SOUPS '15, Ottawa, Ontario, Canada, 2015.

[80] J. Vitak and J. Kim. You Can't Block People Offline: Examining How Facebook's Affordances Shape the Disclosure Process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '14, pages 461–474, New York, NY, USA, 2014. ACM.

[81] J. Vitak, C. Lampe, R. Gray, and N. B. Ellison. Why Won't you Be my Facebook Friend?: Strategies for Managing Context Collapse in the Workplace. In *Proceedings of the 2012 iConference*, iConference '12, pages 555–557, New York, NY, USA, 2012. ACM.

[82] J. B. Walther, B. Van Der Heide, S.-Y. Kim, D. Westerman, and S. T. Tong. The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep? *Human Communication Research*, 34(1):28–49, 2008.

[83] S. D. Warren and L. D. Brandeis. The Right to Privacy. *Harvard Law Review*, pages 193–220, 1890.

[84] J. Winston. Photography in the Age of Facebook. *Intersect: The Stanford Journal of Science, Technology and Society*, 6(2), 2013.

[85] P. Wisniewski, H. Lipford, and D. Wilson. Fighting for my Space: Coping Mechanisms for SNS Boundary Regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 609–618, New York, NY, USA, 2012. ACM.