# Privacy Norms and Preferences for Photos Posted Online

ANONYMIZED FOR SUBMISSION

We are surrounded by digital images. Changes in information and communication technologies (ICTs) have enabled widespread sharing of personal photos, increasing access to aspects of private life previously less open to the world. Most studies of privacy related to online information sharing explore individual privacy preferences rather than social factors like privacy norms. Here we examine both social norms, collectively-shared expectations of privacy, and individual preferences, for understanding perceptions of privacy for personal photos shared online. We conducted an online factorial vignette study on Amazon Mechanical Turk (n=279). Our findings show that people share common expectations about the privacy of online images, and these privacy norms are socially contingent and multi-dimensional. Digital technologies for images both affect the social meaning of privacy and are themselves used in ways influenced by their social context including existing privacy norms.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; • **Human-centered computing → Social content sharing**;

Additional Key Words and Phrases: Privacy, Image Sharing, Contextual Integrity

**ACM Reference Format:**
Anonymized for Submission. 2018. Privacy Norms and Preferences for Photos Posted Online. *ACM Trans. Comput.-Hum. Interact.* 9, 4, Article 39 (March 2018), 25 pages. https://doi.org/0000001.0000001

## 1 INTRODUCTION

Today we are surrounded by digital images. In 2015, Google users alone uploaded 13.7 petabytes worth of pictures to its Photos app.[1] A 2013 study found that 54% of Internet users posted original photos or videos online [18], and over two-thirds of American adults now use social media, with photo-sharing one of the most common activities [13, 66].[2] Unlike the pervasive presence of advertising and broadcast media images over the past 50 years, today's ubiquitous images are of personal lives: they include everything from traditionally photographed content such as friends at a party, babies, and foreign travel, to more novel types of content such as meal selections, "selfies,"[3] and even surreptitiously captured images from private life.

Changes in information and communication technologies (ICTs) have enabled widespread sharing of personal photos, but as sharing increases access to aspects of previously private personal life, it may affect notions of privacy. Increased access to personal lives through posting or viewing photos from inside homes or of previously private activities, whether intimate or mundane, may affect

[1] http://www.dailymail.co.uk/sciencetech/article-3619679/What-vain-bunch-really-24-billion-selfies-uploaded-Google-year.html

[2] http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/

[3] Oxford English Dictionary defines "selfies" as "a photograph one has taken of oneself, typically with a smartphone and shared via social media". In 2014, 26% of Americans had shared a selfie: http://www.pewresearch.org/fact-tank/2014/03/04/more-than-half-of-millennials-have-shared-a-selfie/.

Author's address: Anonymized for Submission.


1073-0516/2018/3-ART39 $15.00
https://doi.org/0000001.0000001

not only individuals' own preferences for sharing/viewing photos, but also how people view the appropriateness of such behavior (e.g., should it or should it not occur) [5]. That is, widespread sharing of personal photos online is likely to shape social norms about privacy, i.e. commonly-shared expectations about appropriate accessibility. According to Helen Nissenbaum [52], privacy entails "contextual integrity," such that information flows, such as via sharing personal photos, conform to social norms about what is appropriate given particular social conditions. For example, it may be innocuous to share photos of a friend dressed up to go out, but photos of a friend reading in her bedroom may be considered inappropriate.

Early studies of online photo sharing have explored users' individual privacy preferences and found that the location of the photo, as well as user concerns about privacy, influence whether images are shared or not [3, 78]. Similarly, user studies of lifelogging or self-tracking activities with wearable cameras (e.g., Google's new Clips camera[4]) suggest that images with content exposing ostensibly private information (e.g., a visible computer monitor), or private spaces (e.g., home versus work), are kept more private (i.e., shared less) by users [27, 28]. Other aspects of social context, such as the number of people in the photo, also appear to influence how lifeloggers share photos [28]. However, few studies have explored privacy norms related to images or image sharing online. While it is important to understand how users' individual privacy concerns and preferences matter for behavior, by examining privacy norms for online images, we can gain insight into the broader social dimensions of privacy and how new technologies affects fundamental patterns of social behavior.

As technologies change and new behaviors like widespread sharing of personal photos via social media become more common, privacy norms may change and new norms may be created [5, 26, 52]. To explore the role of privacy preferences and norms around today's sharing of digital images online, we conducted a large-scale online vignette study of perceptions of privacy of personal photos posted online. We examine features of the social context revealed in the image, as well as the user's relation to the image, to observe whether expectations of privacy are socially shared. In addition, while controlling for individual demographic characteristics, we also consider the role of personal privacy preferences and the various metrics for measuring them, seeking through this study to understand the role of both individual preferences and social norms in perceptions of privacy.

## 2 BACKGROUND – RELATED WORK

### 2.1 Privacy in social context: privacy norms

The concept of privacy varies across cultures and over time [4, 6, 14, 47, 61, 75, 82], and its particular definition further varies by academic discipline. We follow Anthony et al. [5] in defining privacy sociologically as the access of one social actor to another, in which access can vary along multiple dimensions including 'level' (high to low), 'mode' (e.g., online versus face-to-face), and 'type' (e.g., personal photos, health information). Much privacy scholarship examines individual privacy preferences: how much or little access (to self and others) individuals desire and value [1, 50, 76]. Other work explores how individuals vary in managing their own privacy, that is, their attempts to control access to, from, or about themselves or others (see e.g. [4, 57, 76]). For example, the introduction of electronic medical records increased the privacy concerns of some patients, who then withheld information from their physicians as a way to (attempt to) manage privacy [8].

ICTs often blur previously established understandings and expectations of privacy because ICTs can radically change dimensions of accessibility [26, 39, 40, 50, 52, 65]. For example, changes in the mechanisms used by social media sites to disseminate information [7], or by utility companies for

[4] https://store.google.com/us/product/google_clips

monitoring smart meters in homes [26], or by search engines to share personal information for commercial purposes [45], affect perceptions of privacy.

Accessibility is also shaped by social factors including culture, laws, and social norms [1, 5, 46, 50]. Laws define modes, levels, and types of access that are legal and illegal [52, 61, 67, 82]. For example, in their landmark 1898 work on the legal right to privacy, Samuel Warren and Louis Brandeis cited the invention of portable cameras as a threat to individual privacy (particularly for the wealthy [73]). In 1902, another landmark legal case in New York state involving the use of a portrait of a young woman for advertising purposes without her knowledge or consent led to statutory safeguards protecting the right to the private use of one's own image in the commercial sphere [67].

In contrast to laws, social norms are informal socially-enforced expectations about acceptable behavior [23, 25].[5] Expectations about appropriate forms of accessibility to self and others, such as what are acceptable modes, levels, or types of access, are privacy norms [5, 25, 50, 52]. Nissenbaum [51, 52] argues that ICTs disrupt the contextual integrity of privacy when they change flows of information considered appropriate in a particular social context (see also [26, 45]). Since social norms are always being "created, altered or negotiated" through behavior and interaction [16, 23], changes in technology that affect accessibility via information flows can cause the disruption of established privacy norms or the generation of new ones [26, 52].

In addition to being socially dynamic, norms are conditional, such that the same behavior can have different normative expectations depending on contextual factors [16, 23]. This variability means that privacy norms will not necessarily be uniform for a given technology or type of information, but instead may vary with other dimensions of accessibility. For example, Horne et al. [26] found that normative expectations related to smart-meter technology varied depending on the level of accessibility into the home, such that smart-meters that enabled utility companies to intervene directly in home appliances were perceived as less appropriate than those that simply monitored usage data. Martin and Nissenbaum [45] show that expectations of privacy vary not only with type of information, but also the recipient and use of information (see also [58]). Related work finds that privacy behavior is also related to contextual cues about the behavior of others [2, 33].

### 2.2 Privacy preferences

In addition to privacy norms, which express commonly-shared expectations about appropriate accessibility, individuals have personal preferences about privacy, related to how much accessibility to themselves and to others is desired. We know that individuals' preferences for privacy vary significantly [1, 42, 76]. Classic research on privacy preferences, such as Westin [75, 76], use attitude questions to create typologies categorizing individuals based on how much accessibility to, from, or about themselves they think is important, and how strongly they value control over accessibility. Others scholars have developed more extensive typologies that build indices based on multiple dimensions of privacy attitudes [42]; however, recent work questions the value and validity of such typologies, e.g. [32, 45], particularly for explaining behavior [19].

Regardless of typologies used, previous research shows that individuals do vary in their privacy preferences for sharing personal images online. Ahern et al. [3] explored image sharing online through an interview study about Flickr images, finding that social identity concerns, as well as perceptions of security and convenience, affected user sharing behavior. Wu & Zhang [78] found that users varied in geotagging photos based on the type of location, geotagging less often for private locations. Similarly, work on lifelogging [27, 28] indicates that users actively attempt to

[5]Social psychologists use the term injunctive norms to refer to the "ought-ness" of social norms, and distinguish this definition from the concept of descriptive norms, which they use to refer to perceptions of what most people do [10]. In this paper, and consistent with sociological uses of the term [25], all references to norms are to injunctive norms.

manage their (and others') privacy when possible through a range of strategies for restricting image sharing.

In seeking to understand privacy norms for sharing personal images online, we therefore must also take into account variation in individual privacy preferences.

### 2.3 Privacy and sharing digital images

Previous studies have examined not only when and how digital photographs are shared online [3, 78], but also how to enable users to better manage privacy in the context of digital images. Some research proposes mechanisms to apply protection to the overall image [71]. Similarly, Choi et al. [9] suggest that editing photos (e.g., enhancing, cropping) can sometimes subvert algorithmic attempts to identify the image location. DARKLY is a system layer developed by Jana et al. [29] that uses computer vision techniques to replace image contents with an "opaque reference" while letting apps access more private versions of the image. MarkIt is a privacy marker framework that enables users to control the pictures taken in video feeds and blur sensitive parts [59]. World Driven Access Control (WDAC) is a protocol which depends on the objects in the real world to explicitly specify their access control policies [62]. These policies can be detected by a trusted system that applies them before feeding the data for posting online or sharing.

Other work has developed techniques to blur only sensitive parts of images. For example, Thomaz et al. [70] proposed rules that can be used to blur sensitive parts in images taken by lifeloggers in the context of logging eating behaviors. And Korayem et al. [36] used computer vision techniques to detect monitors in lifelogging images and block them without the need of users to manually flag such images. Orekondy et al. [55] and Kuang et al. [37] have both developed different automated systems using image-recognition algorithms that assists a user in deciding when to share an image. Yu et al. [81] [80] [79] use deep machine learning to identify privacy-sensitive objects in shared images in order to apply a tool to automatically blur the privacy-sensitive content. Researchers have further studied the impact on the viewer's experience when transforming parts of images for enhanced privacy and the trade off between privacy and utility for various filters across different scenarios [21, 22, 38].

Other algorithmic tools might evaluate a user's preferences and take appropriate action when presented with images. Prasad et al. [58] analyzed how the privacy implications of wearable devices necessitated dynamic rather than preset preference settings. This work showed how the target audience for the shared information was sometimes different than that of regular social sharing, and therefore required new mechanisms. Other researchers have looked into how better default preferences could be generated for users, rather than relying on them to create those preferences themselves. Ravichandran et al. [60] explored using decision trees to generate default policies. Gupta et al. [20] examined whether location could be used to allow for simpler unlocking of a phone in a trusted versus an untrusted location. Toubiana and his co-authors [20] argue that geo-location information should be leveraged to automatically apply present privacy preferences when a photo is taken, while Klemperer et al. [35] contend that user-generated text tags can also be leveraged to guide automated privacy and access controls for online images. Fang and LeFevre [15] attempted to crowdsource privacy policies from a user's friends. All of these approaches improved a user's privacy, but focused on using an image's location, or the user's own or a friend's preferences, instead of considering how image content might influence normative expectations of privacy. Scholars as yet have a poor grasp of what people perceive as private for the purposes of image sharing, possibly because privacy norms related to this behavior are in flux. A better understanding of privacy norms around personal images may enable the development of technical applications that recognize and protect image content while fulfilling high expectations of privacy.

## 3 RESEARCH QUESTIONS

Prior research has focused on examining individual privacy preferences, in general and specifically related to image sharing, to understand perceptions of privacy. This work often focuses on classifying individuals into categorical groups of users with high or low preferences for privacy (e.g., Westin's classic typology) or understanding how individuals manage their own privacy. While we agree that individual privacy preferences and privacy management behavior are important, we build on the ideas of contextual integrity [45, 52] and sociology of privacy [5] to argue that privacy norms also play an important role in both perceptions and behavior but are much less understood. Here we examine privacy norms for personal images shared online, that is, common expectations about whether it is appropriate (based on privacy) for such images to be shared online or not. We explore whether privacy norms for personal images vary depending on the contextual features in the images. We expect that features in the image that increase access to previously private contexts or content will be considered systematically more private than others. For example, previous work [27, 28] has found that lifeloggers were less likely to share images of bedrooms compared to other household rooms, and those containing computer monitors/screens (including smartphone screens).

Based on these findings, we hypothesize:

**H1** Images of bedrooms will be perceived as more private/less appropriate to share online than images of other household rooms (kitchens, dining rooms, living rooms).

**H2** Images containing visible computer monitors/screens will be perceived as more private/less appropriate to share online than images without screens.

In addition to these features, the presence of people in photos affects perceptions of privacy. For example, we know that people regularly remove tags of themselves in images on social media [41]. In addition, studies of lifeloggers suggest that the number of people in the image may affect whether or not it is shared [27, 28]. Photos containing an image of a person provide a great deal of access to information about them, including not only about personal appearance (e.g., hair color, height), but may also reveal location (via geotags) or place (type of setting) or information about the person's social network (e.g., via other people in the photo). Given this increased accessibility, we expect that photos with people will be considered more private than images with no people.

**H3** Images with people (1 or more) will be perceived as more private/less appropriate to share online than images with no people.

By this logic, it may be the case that more people compared to fewer in a photo should be considered even more private, that is, perceptions of privacy will simply increase with the number of people in the image. However, more people may indicate more of a social, even public, versus private setting or situation, so it is not clear that images with more people will be perceived as more private. Below we explore whether images with two people compared to none or one are considered more or less private as an open research question rather than a specified hypothesis.

As noted above, though we seek to identify privacy norms for image sharing, we also expect individual preferences for privacy to affect perceptions of privacy for personal images shared online. A number of different attitudinal measures of privacy preferences exist and no one measure is considered to be definitive. Though there has long been concern and criticism of such attitudinal scales [32, 42], particularly for explaining individual privacy behavior [19, 77], such attitudes are expected to affect perceptions of privacy, such that:

**H4** Individuals with stronger preferences for privacy will be more likely to perceive images as private/less appropriate to share online.

In addition to individual privacy preferences as measured through privacy attitudes and concerns, we explore how the participant's relation to the image may be related to perceptions of privacy and thus shed further light on privacy norms. In the current context of social media, people have the opportunity to view the images of others, to post images they have taken, and to have images of them posted online (whether by themselves or by others). Thus online photo sharing has implications for perceptions of privacy related to oneself and to others, some of whom may be merely 'bystanders', that is, those who are unknowingly captured in an image (or by any type of sensing device) [56]. We know that bystanders express concerns about being captured by sensing devices [12]. However, in addition to being emotionally and viscerally sensitive to their own privacy [68], people express concerns about the privacy of others. For example, Hoyle and colleagues [27, 28] found that lifeloggers were concerned about and took steps to protect the privacy of bystanders. Still, we expect that images that entail more access to the participant (e.g., participant visualizes being in image) will be perceived as more private than images (of others) that participants view online.

**H5** Expectations of image privacy will vary by participant's relation to the image such that: images that the participant visualizes being in or of their home will be perceived as more private/less appropriate to share than (a) images that participants take and (b) images that participants view online.

## 4 STUDY PROCEDURES

### 4.1 Study Design

We conducted an online factorial vignette study with 279 Amazon Mechanical Turk (mTurk) workers in order to examine privacy norms, as well as individuals' privacy preferences, for digital image sharing online. Vignette studies use experimental design in which vignettes, hypothetical stories/scenarios with details corresponding to experimentally defined conditions, are deployed to test for variation in judgments either between or within subjects [30, 31]. Vignette studies have been used to explore privacy issues [26, 45, 48] by employing scenarios to explore subjects' perceptions and expectations about sharing or exposing different types of information under different conditions. Here, we employed a study design in which the experimental conditions were scenarios that contained different images shown to each subject. Subjects were asked questions about the content of the image as well as judgments about each image, specifically whether or not they thought each was private and thus not appropriate to be posted online. In addition, after the vignettes, subjects were asked questions about their online behavior and general privacy attitudes and behaviors; prior to the vignettes, subjects answered basic demographic questions.

Each subject was presented with ten "vignettes" consisting of an image that varied across conditions of: type of household room (bedrooms versus other rooms, including kitchens, living rooms or offices), whether a computer monitor/screen (including smart phone screens) was present or not, and the number of people (0, 1, or 2) (see Table 1). For each condition, we selected six images from publicly available online image-sharing sites Flickr and Google Images, searching for images with terms such as "one person in bedroom."[6]

We conducted a pilot study with 10 subjects to ensure all 60 photos captured the condition-specific characteristics (10 conditions x 6 images per condition) to determine if subjects correctly identified the experimental features of each image. Images that did not match 100% were removed and new photos added as needed until our pilot testers showed agreement on the condition-specific features for all six images per condition. During the study, subjects were asked to first identify the features in each image, i.e., the type of room, whether a monitor was visible, and the number of

[6]No photos are included with people in any stage of undress, or in any activity that might be considered "sexual" or intimate.

| Condition | Type of Household Room | Monitor / Screen | Number of People |
|---|---|---|---|
| 1 | Bedroom | None | 0 |
| 2 | Bedroom | Yes | 0 |
| 3 | Other room | None | 1 |
| 4 | Bedroom | None | 1 |
| 5 | Other room | Yes | 1 |
| 6 | Bedroom | Yes | 1 |
| 7 | Other room | None | 2 |
| 8 | Bedroom | None | 2 |
| 9 | Other room | Yes | 2 |
| 10 | Bedroom | Yes | 2 |

Table 1. Study conditions by Image characteristics
*Note: Other room = kitchen, living room, or office*

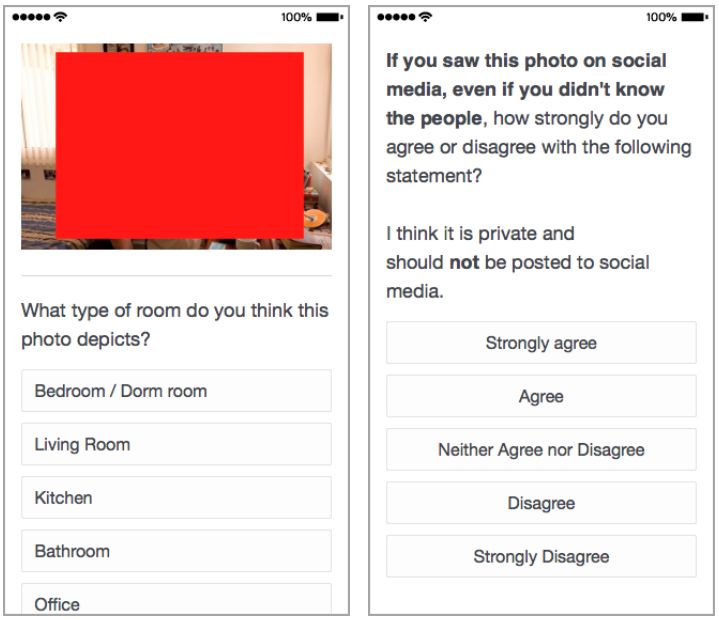



Fig. 1. Sample screenshots of the survey instrument.

people in the image (see Figure 1 for an example vignette-image and questions). Study subjects were randomized between the six images within each condition, and also randomized as to the order in which they were presented each condition.

Respondents were selected through Amazon's Mechanical Turk (mTurk) platform, targeting "Master" surveyors[7] with the description "Answer questions about what is contained in various images, and your feelings about them. The study is being conducted through XXX University (anonymized). You will be compensated $2.25 for taking the survey." Respondents were given one hour to complete the survey, though our initial pilot estimated that it should take 20 minutes, thus

[7]"Master" surveyors are those workers that have a proven track record at successfully completing a variety of tasks.

payment was at the rate of $7 per hour for compensation. Six attention-check questions were included within the survey. Respondents were paid if they successfully answered more than three of the attention questions, but their data was discarded if they failed to answer any of the attention questions. A total of 418 respondents completed the survey, with 279 (66%) completing all six of the attention check questions correctly. In addition to the main study design, all respondents were asked basic demographic information as well as questions about their technology usage and knowledge, and about privacy behavior and attitudes (described in more detail below).

### 4.2 Measures

With each image-vignette subjects were asked to consider the following questions, all with response categories on 5-point Likert scale of 5=strongly agree private to 1=strongly disagree private:

(1) If you saw this photo on social media, even if you didn't know the people, how strongly do you agree or disagree with the following statement? I think it is private and should not be posted to social media.

(2) If you were the person who took this photo, how strongly do you agree or disagree with the following statement? I think it is private and should not be posted to social media.

(3a) (for photos without people): If this photo were of your home, how strongly do you agree or disagree with the following statement? I think it is private and should not be posted to social media.

(3b) (for photos with people): If you were the/a person in this photo, how strongly do you agree or disagree with the following statement? I think it is private and should not be posted to social media.

We created three dichotomous dependent variables (saw photo, took photo, and own-home/in-photo) in which responses of "strongly agree private" and "agree private" are coded as 1, and all other responses coded as 0 for each of the questions above, collapsing own-home/in-photo responses into a single variable.

The key independent variables for measuring social context factors within images are the categories: type of household room (bedroom=1, else=0), presence of computer monitors/screen (including smart phone screens=1, no screen=0), and number of people in the photo (none, 1 Male, 1 Female, 2 Females, 1Male+1Female).[8]

In addition to the influence of social context factors in the image, we also hypothesized that individual privacy preferences will influence expectations of privacy for personal images shared online. Though no agreed upon measures of individual privacy preferences exist, we used four different measures (defined below). The components of each privacy preference measure were asked after the experimental conditions as statements in randomized order.

The best known measure of privacy preferences is probably Westin's classic privacy scale [75, 76], which we include using Westin's classic three questions, all with response categories on 5-point Likert scale of 5=strongly agree to 1=strongly disagree:

- Consumers have lost all control over how personal information is collected and used by companies.
- Most businesses handle the personal information they collect about consumers in a proper and confidential way. (Recoded response so high value = more privacy concern)
- Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. (Recoded response so high value = more privacy concern)

Subjects giving privacy-oriented answers (responses=4 or 5) to all three questions are classified, according to the original typology, as Westin-fundamentalists, those giving no privacy-oriented

[8]Images with 2 males were cut from the final analysis because of limited data.

answers are classified as Westin-unconcerned, while those in-between are classified as Westin-pragmatists.

Jensen et al. [32] proposed an update of Westin's scale based on five privacy statements more directly related to online activities. Though Jensen et al. [32] recommend creating the same 3-categories as Westin's original framework, here we create a mean of the five statements, all with 5-point Likert response categories:

- I am concerned about online identity theft.
- I am concerned about my privacy online.
- I am concerned about my privacy in everyday life.
- I am likely to read the privacy policy of an ecommerce site before buying anything. (Reverse coded)
- Privacy policies accurately reflect what companies do. (Reverse coded)

Another attitudinal measure of privacy preferences, proposed by Malhotra, Kim and Agarwal [42], is the Internet Users' Information Privacy Concerns (IUIPC) scale, which is part of their larger behavioral model for online behavior. The IUIPC includes three subscales on privacy "awareness," "collection," and "control," all with 5-point Likert response categories:[9]

Awareness:

- Companies seeking information online should disclose the way the data are collected, processed, and used.
- A good consumer online privacy policy should have a clear and conspicuous disclosure.
- It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Collection:

- It usually bothers me when online companies ask me for personal information.
- When online companies ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.
- I'm concerned that online companies are collecting too much personal information about me.

Control:

- Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
- Consumer control of personal information lies at the heart of consumer privacy.
- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

We computed the mean score for each subscale to create three variables of **IUIPC-awareness**, **IUIPC-collection**, and **IUIPC-control**.[10]

Finally, we create our own simple self-rated privacy question: "Which of these statements more accurately describes you: I am generally a private person and like to keep to myself. OR I am generally an open person who enjoys sharing with others."

We control for subject demographics (gender, race, education, and age) and the frequency of social media and mobile phone use, coded as 1=daily use and 0=less than daily use, as well as the

[9]These authors use a 7-point Likert response scale in the original model [42].

[10]Malhotra et al. [42] propose using principal component factor analysis to create one latent factor with the three subscales as component measures of it. In separate analyses (not shown), we calculate a one factor IUIPC measure (alpha=0.86) and find using the one factor IUIPC measure instead of the three reported here produces results substantively identical to those reported below, though it is never statistically significant.

| Variables | % |
|---|---|
| **Female** | 56% |
| **Non-white Race** | 19% |
| **Age** | |
| 18 – 29 years of age | 24% |
| 30 – 39 years | 37% |
| 40 – 49 years | 18% |
| 50 – 59 years | 13% |
| 60+ years | 8% |
| **Education Level** | |
| % with College degree or higher | 65% |
| **Use Social Media** | |
| several times/day (=1) | 53% |
| vs less often (=0) | |
| **Use mobile phone** | |
| several times/day (=1) | 81% |
| vs less often (=0) | |
| **Use phone for photo-sharing** | |
| few times/month or more (=1) | 57% |
| vs less often (=0) | |

Table 2. Descriptive statistics of subject characteristics, n=279

frequency of photo sharing via the phone, coded as 1=few times/month or more, and 0=less often. Table 2 shows the descriptive statistics for all subject characteristics (discussed further below in section 5.1).

### 4.3 Method of Analysis

This study employs a within-subject study design to examine privacy norms related to features of images shared online, while also analyzing whether between-subject differences in privacy preferences also influence privacy perceptions. We use an extended generalized linear mixed-model (GLMM) that allows decomposition of within and between subject effects for nonlinear outcomes using the xthybrid command with logit-link function in Stata-13 [63, 64]. Though fixed-effect models are useful for repeated-measures designs like ours, enabling estimates of within-subject variables while adjusting for subject-invariant variation, they cannot provide effect estimates for the between-subject variables. Hybrid statistical models provide estimates of both within-subject effects, that is, how on average a within-subject change in an independent variable (e.g., room type) is associated with a within-subject change in the dependent variable (expectation of privacy), as well as between-subject effects, that is, how differences in privacy preferences are associated with differences in the dependent variable (i.e., expectation of privacy). This is accomplished by: (i) specifying subject-varying independent variables as deviations from the subject (cluster) mean, and (ii) adding the means of the original subject-varying variables to the model. Thus, we can evaluate whether there are between-subject effects (by privacy preferences) in addition to the within-subject effects (of image features) on perceptions of privacy.

| Privacy Preference Measure | % or Mean (standard deviation) |
|---|---|
| **Westin Privacy Categories** | |
| Privacy Fundamentalists | 24% |
| Privacy Pragmatists | 26% |
| Privacy Unconcerned | 50% |
| **Jensen Online Privacy Mean** | 3.6 (.54) Range = 1.8, 4.8 |
| **Internet Users' Information Privacy Concerns (IUIPC) Scale** | |
| IUIPC-Awareness | 4.4 (0.01) |
| IUIPC-Collection | 4.0 (0.01) |
| IUIPC-Control | 4.1 (0.01) |
| **Self-Rated Privacy (private person=1, open person=0)** | 83% |

Table 3. Descriptive Statistics of privacy preference measures, N=279

For each dependent variable, we examine a series of models that include the within-subject image features and the different measures of privacy preferences. We report logit coefficients for the within-subject and between-subject variables, while controlling for individual-level (between subject) fixed effects of demographic characteristics and technology use. In these models, logit coefficients tell the amount of change in the predicted log odds of the dependent variable from a 1 unit increase in the predictor variable, holding all other predictors constant. Logit coefficients can be converted from log-odds to odds ratios by exponentiating the coefficient. We used a significance threshold of 0.05 to determine whether or not a variable was significant. We conducted additional analyses (not shown here) to evaluate the robustness of the findings and discuss them briefly below.

## 5 STUDY RESULTS AND DISCUSSION

### 5.1 Subject Characteristics

A total of 279 subjects completed all aspects of the study via Mechanical Turk, including correctly responding to all six attention check questions. Table 2 shows that 56% of the sample is female, and 19% were of non-white race (self-rated as one of following: African American/Black, Asian American/Pacific Islander, Hispanic; we collapse these categories into one for analysis). The majority of subjects are younger than 39 years of age, with about 20% over the age of 50 years. Consistent with the profile of master Turk users, this is a highly educated and technology-savvy sample, with two-thirds of the subjects having at least a college education. Most use a mobile phone and social media several times a day, as well as sending/receiving photos on their phones at least a few times per month. Given our study is designed to test both within and between-subject conditions rather than provide population estimates of behavior, the non-representativeness of the subject sample is not problematic. However, we discuss how the sample characteristics may be relevant for our findings below.

Table 3 shows descriptive statistics for the measures of individual privacy preference. According to the Westin scale, 24% of the sample are privacy fundamentalists, 26% are privacy pragmatists, and 50% are privacy unconcerned. For the 5 privacy statements recommended by Jensen et al. [32], the mean is 3.6 on a 5-point Likert scale (higher scores = more private), which indicates moderate-high

privacy concerns on average, with a range (1.8–4.8) including both low and high privacy scores. The Malhotra et al. [42] IUIPC awareness, collection, and control mean scores of at or above 4 on a 5-point Likert scale (higher scores = more private) indicate relatively high levels of privacy concerns in each of the three areas. Finally, the vast majority of the subjects (83%) self-rate themselves as a "private person" rather than an "open person".

### 5.2 Findings: Image characteristics

Tables 4, 5, and 6 show the results of hybrid mixed-effects GLM models with logit-link functions for each of the three dependent variables: expectations of privacy if subject saw the photo posted online (Table 4), took the photo (Table 5), or if the photo was of their home/they were in the photo (Table 6). Each table includes 5 models, in which model one has no individual privacy preferences included, model two includes the Westin privacy measures, model three includes the Jensen et al. [32] online privacy mean, model four includes the [42] IUIPC privacy measures, and model five includes our own measure of self-rated privacy. All models include controls for subject gender, race, age, education, and frequencies of mobile phone use, social media use, and phone-photo sharing.[11] Each model includes only observations (number of subjects multiplied by the number of responses to each image question) with non-missing data on all variables, so the number of subjects (the cluster variable in hybrid mixed-effects models) and the number of observations (within-subject observations) varies slightly between models.

To evaluate the first hypothesis – that images of bedrooms will be considered more private than images of other household rooms – we can look at the results in row one of each table. Across each of the dependent variables shown in Tables 4, 5, and 6, the coefficients for bedroom are never statistically significant, and we thus reject hypothesis H1.

We can evaluate hypothesis H2, that images with computer monitors/screens will be considered more private than images with no screens, by looking at the coefficients reported in row two of each of the three tables. The coefficients for monitor/screen are statistically significant in all models for all three dependent variables — however, the sign on the coefficient is negative indicating that images with computer screens are statistically less likely to be considered private than images with no screens, all else equal. This finding that images with computer screens have approximately 30% lower odds of being considered private is the opposite of hypothesis H2 and a somewhat surprising finding, given that computer screens often contain personal information that people may consider private. Not only does this result contradict hypothesis H2, it also suggests expectations about the privacy of images containing computer screens may be more complicated than simply considering the possibility of personal information exposure. We return to this issue in the discussion below.

[11] Note the hybrid mixed models allow us to include demographics as between-subject fixed effects. However, none of the demographic characteristics are significant in any of the models.

| Image characteristics | Model 1: Baseline | Model 2: Westin Privacy | Model 3: Jensen Online Privacy | Model 4: IUIPC Means | Model 5: Self-rated Privacy |
|---|---|---|---|---|---|
| **WITHIN Subjects:** | | | | | |
| Bedroom[1] | -0.18 (0.19) | -0.18 (0.19) | -0.16 (0.19) | -0.14 (0.19) | -0.18 (0.19) |
| Monitor / Screen | -0.38 (0.15)** | -0.39 (0.15)** | -0.38 (0.15)** | -0.37 (0.15)** | -0.38 (0.15)** |
| **Number of People**[2] | | | | | |
| One Male | 0.81 (0.23)*** | 0.81 (0.23)*** | 0.83 (0.23)*** | 0.84 (0.23)*** | 0.81 (0.23)*** |
| One Female | 1.26 (0.21)*** | 1.26 (0.21)*** | 1.25 (0.21)*** | 1.25 (0.21)*** | 1.26 (0.21)*** |
| Two Females | -0.35 (0.24) | -0.35 (0.24) | -0.34 (0.24) | -0.34 (0.24) | -0.34 (0.24) |
| Two: Male & Female | -1.87 (0.64)** | -1.87 (0.65)** | -1.86 (0.65)** | -1.84 (0.66)** | -1.87 (0.64)** |
| **BETWEEN Subjects: Privacy Preferences** | | | | | |
| **Westin Privacy**[3] | | | | | |
| Fundamentalists | — | 0.28 (0.25) | — | — | — |
| Unconcerned | — | 0.19 (0.26) | — | — | — |
| **Jensen Online Privacy** | — | — | 0.40 (0.24) | — | — |
| **IUIPC Scale** | | | | | |
| Awareness | — | — | — | -0.10 (0.22) | — |
| Collection | — | — | — | 0.14 (0.14) | — |
| Control | — | — | — | 0.07 (0.18) | — |
| **Self-Rated Privacy** | — | — | — | — | 1.00 (0.30)*** |
| Constant | -2.19 (1.52) | -2.20 (1.52) | -3.87 (1.80)* | -2.02 (1.54) | -2.88 (1.49)* |
| | -LL = -761.2<br>Wald $\chi^2$ = 147.6***<br>df = 22<br>N clusters = 274<br>N obs = 1,780 | -LL = -760.5<br>Wald $\chi^2$ = 155.9***<br>df = 24<br>N clusters = 274<br>N obs = 1,780 | -LL = -756.9<br>Wald $\chi^2$ = 145.6***<br>df = 23<br>N clusters = 273<br>N obs = 1,774 | -LL = -754.1<br>Wald $\chi^2$ = 146.8***<br>df = 25<br>N clusters = 270<br>N obs = 1,755 | -LL = -755.4<br>Wald $\chi^2$ = 157.3***<br>df = 23<br>N clusters = 274<br>N obs = 1,780 |

Notes: * p < .05 ** p < .01 *** p < .001. [1] vs other rooms; [2] vs zero people; [3] vs Westin privacy-pragmatists.
Each regression controls for gender, race, age, education, frequencies of mobile phone use, social media use, phone-photo sharing.

Table 4. **Coefficients for expectations of privacy if SAW photo posted online, by image and subject characteristics, using hybrid mixed-effects GLM model (with logit-link function), with robust standard errors in parentheses**

| Image characteristics | Model 1: Baseline | Model 2: Westin Privacy | Model 3: Jensen Online Privacy | Model 4: IUIPC Means | Model 5: Self-rated Privacy |
|---|---|---|---|---|---|
| **WITHIN Subjects:** | | | | | |
| Bedroom[1] | -0.04 (0.20) | -0.04 (0.20) | -0.02 (0.20) | -0.01 (0.20) | -0.04 (0.20) |
| Monitor / Screen | -0.39 (0.14)** | -0.39 (0.14)** | -0.38 (0.14)** | -0.38 (0.14)** | -0.39 (0.14)** |
| **Number of People**[2] | | | | | |
| One Male | 1.04 (0.24)*** | 1.04 (0.24)*** | 1.06 (0.25)*** | 1.07 (0.25)*** | 1.04 (0.25)*** |
| One Female | 1.37 (0.22)*** | 1.37 (0.22)*** | 1.36 (0.22)*** | 1.36 (0.22)*** | 1.37 (0.22)*** |
| Two Females | -0.19 (0.23) | -0.19 (0.23) | -0.19 (0.23) | -0.19 (0.23) | -0.19 (0.23) |
| Two: Male & Female | -1.53 (0.68)* | -1.53 (0.68)* | -1.52 (0.68)* | -1.50 (0.68)* | -1.52 (0.67)* |
| **BETWEEN Subjects: Privacy Preferences** | | | | | |
| **Westin Privacy**[3] | | | | | |
| Fundamentalists | — | 0.23 (0.24) | — | — | — |
| Unconcerned | — | 0.14 (0.25) | — | — | — |
| **Jensen Online Privacy** | — | — | 0.26 (0.22) | — | — |
| **IUIPC Scale** | | | | | |
| Awareness | — | — | — | -0.09 (0.20) | — |
| Collection | — | — | — | 0.22 (0.13) | — |
| Control | — | — | — | -0.12 (0.16) | — |
| **Self-Rated Privacy** | — | — | — | — | 1.31 (0.30)*** |
| Constant | -3.40 (1.52)* | -3.43 (1.53)* | -4.45 (1.77)** | -3.34 (1.53)* | -4.27 (1.44)** |
| | -LL = -784.8<br>Wald $\chi^2$ = 145.3***<br>df = 22<br>N clusters = 274<br>N obs = 1,783 | -LL = -784.3<br>Wald $\chi^2$ = 149.8***<br>df = 24<br>N clusters = 274<br>N obs = 1,783 | -LL = -781.6<br>Wald $\chi^2$ = 142.7***<br>df = 23<br>N clusters = 273<br>N obs = 1,777 | -LL = -776.7<br>Wald $\chi^2$ = 144.6***<br>df = 25<br>N clusters = 270<br>N obs = 1,758 | -LL = -774.2<br>Wald $\chi^2$ = 158.6***<br>df = 23<br>N clusters = 274<br>N obs = 1,783 |

Notes: * p < .05 ** p < .01 *** p < .001. [1] vs other rooms; [2] vs zero people; [3] vs Westin privacy-pragmatists.
Each regression controls for gender, race, age, education, frequencies of mobile phone use, social media use, phone-photo sharing.

Table 5. **Coefficients for expectations of privacy if TOOK Photo posted online, by image and subject characteristics, using hybrid mixed-effects GLM model (with logit-link function), with robust standard errors in parentheses**

| Image characteristics | Model 1: Baseline | Model 2: Westin Privacy | Model 3: Jensen Online Privacy | Model 4: IUIPC Means | Model 5: Self-rated Privacy |
|---|---|---|---|---|---|
| **WITHIN Subjects:** | | | | | |
| Bedroom[1] | -0.12 (0.17) | -0.12 (0.17) | -0.11 (0.18) | -0.09 (0.18) | -0.12 (0.17) |
| Monitor / Screen | -0.31 (0.15)* | -0.31 (0.15)* | -0.31 (0.15)* | -0.30 (0.15)* | -0.31 (0.15)* |
| **Number of People**[2] | | | | | |
| One Male | 0.75 (0.21)*** | 0.75 (0.21)*** | 0.76 (0.21)*** | 0.77 (0.21)*** | 0.75 (0.21)*** |
| One Female | 0.96 (0.19)*** | 0.96 (0.19)*** | 0.95 (0.19)*** | 0.95 (0.19)*** | 0.96 (0.19)*** |
| Two Females | -0.49 (0.19)** | -0.49 (0.20)* | -0.49 (0.20)* | -0.49 (0.20)** | -0.49 (0.20)** |
| Two: Male & Female | -2.72 (0.77)*** | -2.73 (0.77)*** | -2.72 (0.77)*** | -2.70 (0.77)*** | -2.71 (0.77)*** |
| **BETWEEN Subjects: Privacy Preferences** | | | | | |
| **Westin Privacy**[3] | | | | | |
| Fundamentalists | — | 0.22 (0.21) | — | — | — |
| Unconcerned | — | 0.11 (0.24) | — | — | — |
| **Jensen Online Privacy** | — | — | 0.53 (0.20) | — | — |
| **IUIPC Scale** | | | | | |
| Awareness | — | — | — | 0.06 (0.19) | — |
| Collection | — | — | — | 0.26 (0.12)* | — |
| Control | — | — | — | -0.03 (0.14) | — |
| **Self-Rated Privacy** | — | — | — | — | 1.01 (0.25)*** |
| Constant | -1.64 (1.41) | -1.66 (1.41) | -3.74 (1.63)* | -1.53 (1.40) | -2.38 (1.38) |
| | -LL = -914.3<br>Wald $\chi^2$ = 132.7***<br>df = 22<br>N clusters = 274<br>N obs = 1,788 | -LL = -913.8<br>Wald $\chi^2$ = 133.2***<br>df = 24<br>N clusters = 274<br>N obs = 1,788 | -LL = -906.9<br>Wald $\chi^2$ = 134.6***<br>df = 23<br>N clusters = 273<br>N obs = 1,782 | -LL = -902.7<br>Wald $\chi^2$ = 138.2***<br>df = 25<br>N clusters = 270<br>N obs = 1,763 | -LL = -905.5<br>Wald $\chi^2$ = 142.3***<br>df = 23<br>N clusters = 274<br>N obs = 1,788 |

Notes: * p < .05 ** p < .01 *** p < .001. [1] vs other rooms; [2] vs zero people; [3] vs Westin privacy-pragmatists.
Each regression controls for gender, race, age, education, frequencies of mobile phone use, social media use, phone-photo sharing.

Table 6. **Coefficients for expectations of privacy if IN Photo or of OWN Home posted online, by image and subject characteristics, using hybrid mixed-effects GLM model (with logit-link function), with robust standard errors in parentheses**

Hypothesis H3 considers the privacy norms related to the presence and number of people in a photo. As shown in row three in each of Tables 4, 5, and 6, we can see that images with one male or one female are always significant and positive, indicating they are significantly more likely to be considered private, compared to the suppressed category of zero people in the photo. Indeed, these images are two to three times more likely to be evaluated as private, respectively, across dependent variables. These findings support hypothesis H3. In contrast, images with two people, specifically a male and female, are consistently significantly less likely to be considered private, by 80-90%, than photos with no people across all three dependent variables. Similarly, images with two females are significantly less likely to be evaluated as private than images with no people, by about 40%, but only for scenarios in which the subject considers being in the photo (Table 6). Overall these findings show that compared to an image with no people, photos with one single person are two to three times more likely to be evaluated as private, while photos with two people, particularly a male and female, are about half as likely to be evaluated as private. This latter result suggests privacy norms for images are strongly related to social conditions, in this case the number of people, depicted in the image. We explore these findings more below, and further discuss their implications.

Hypothesis H4 considers that on top of the social privacy norms that we observe, individuals' personal privacy preferences also affect expectations of privacy. Westin's classic three categories of privacy fundamentalists, privacy pragmatists (the suppressed category) and privacy unconcerned are tested in model two for each dependent variable (shown in column two in Tables 4 5, and 6); none are ever statistically significant. These findings provide evidence consistent with previous scholarship suggesting the Westin categories do not appear to be particularly useful in understanding privacy in online contexts.

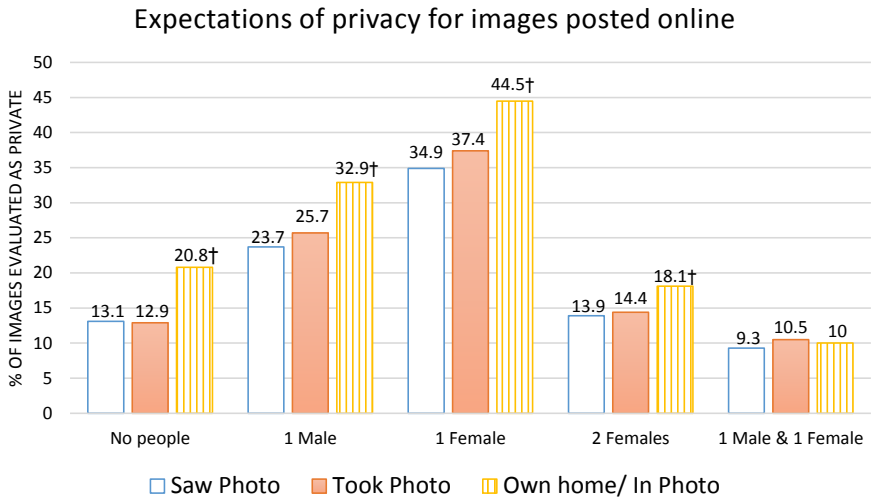
The online privacy scale recommended by Jensen et al. [32] is tested in model three for each dependent variable. As with the Westin categories, the Jensen Online Privacy mean is not significant for privacy if the subject saw photo online (Table 4) or took the photo (Table 5), but it is significant and positive for subjects imagining being in the photo or as a photo of their own home (Table 6). This latter finding shows individuals with greater privacy concerns, as measured by the Jensen Online Privacy mean, are about one and one-half times more likely to evaluate an image they are in as private, over and above the normative expectations of privacy related to the features of the image. This finding provides support for hypothesis H4.

Model 4 for each dependent variable examines the effects of the Malhotra et al. [42] IUIPC scales for awareness, collection and control. None of the IUIPC scales are significant for privacy if the subject saw the photo online (Table 4) or took the photo (Table 5), but for subjects imagining being in the photo or as a photo of their own home (Table 6), IUIPC-collection is significant and positive, indicating those subjects who are more concerned about online information collection are more likely to say a photo is private and should not be posted online. This finding for the IUIPC collection scale is consistent with the finding for the Jensen Online Privacy mean, and provides some additional support for hypothesis H4.

Finally, model 5 shows a strongly significant positive effect of our own dichotomous self-rated privacy measure for all three dependent variables, indicating that those who identify as "a private person" are two to nearly four times more likely to say that images are private and should not be posted online, even after controlling for the features of the image. This finding also supports hypothesis H4 that individual privacy preferences influence expectations of image privacy online.

To summarize findings related to hypotheses H1–H4, we find no support for hypothesis H1 that privacy expectations for images of bedrooms are greater than for other, more public household rooms. For hypothesis H2 regarding privacy norms for images showing a computer monitor/screen, the analyses show an unexpected finding that directly contradicts hypothesis H2: such photos are significantly less likely to be evaluated as private than photos without monitors/screens. We find

strong support for hypothesis H3 that images with one person are more likely to be considered private than images with no people. We also considered what the privacy expectations might be for two people in a photo and found that images with two people, particularly if a male and female, were significantly less likely to be considered private than photos with no people. Figure 2 illustrates the pattern of privacy expectations across the categories for number of people in the photo, and shows that within each dependent variable (saw photo, took photo, own home/in photo), privacy expectations are highest for photos with one person and lowest for two people, particularly a male and female.




Notes:

† Within all number-of-people categories except 1male&1female, Repeated-measures ANOVA (adjusted for between-subject characteristics) with post-hoc Bonferroni tests show own home/in photo is significantly higher privacy than saw photo ($p < 0.001$) and took photo ($p < 0.001$). There is no statistical difference between saw photo and took photo in any category except 1Female

Separately, Bonferroni tests show there are significant differences within the photo categories:

- Saw Photo: 1male and 1female images significantly more likely private ($p < 0.001$) than all other categories. No statistical difference between no-people and 2Females categories. Category with 1male&1female images significantly less likely private ($p < 0.001$) than all other categories.
- Took Photo: 1male and 1female images significantly more likely private ($p < 0.001$) than all other categories. No statistical difference between no-people and 2Females categories. Category with 1male&1female images significantly less likely private ($p < 0.05$) than all other categories.
- Own Home/In Photo: All categories are statistically different from others ($p < 0.001$): 1Female > 1Male > no-people > 2Females > 1male&1female.

Fig. 2. **Image privacy by subject's relation to the photo and number of people in the image**

### 5.3 Findings: Subject relation to photo

Figure 1 also illustrates how subjects' relation to the photo as measured through the three dependent variables influences privacy expectations as defined in hypothesis H5, in which greater access, i.e., the subject considering being in the photo or a photo of their home, will have greater expectations of privacy than the subject simply seeing a photo posted online or even taking the photo. Within each category for the number of people in image, within-subject means for the percentage of images evaluated as private are significantly higher when the subject considers an image they are in or of their home compared to either seeing the photo posted online, or taking the photo. Using Repeated-measures ANOVA (adjusted for between-subject characteristics) with Bonferroni tests shows that among images of no people, subjects are more likely to evaluate the image as private if they considered it to be an image of their own home compared to seeing it posted online or taking it themselves [20.8% compared to 12.9% and 13.1% respectively]. This pattern holds across all number-of-people image categories except those with two people consisting of a male and female. In all number-of-people categories, these tests show no statistical differences in evaluations of privacy between saw photo or took photo. Overall, these findings support hypothesis H5 that subjects' role in relation to images posted online influences expectations of privacy. Moreover, they support theoretical ideas that people are viscerally sensitive to their own privacy [68].

### 5.4 Robustness checks

We conducted a number of additional statistical tests (not shown) to evaluate the robustness of our findings. First, to evaluate whether the findings were influenced by specific images, we re-ran all models reported in Tables 4, 5, and 6 after dropping outlier images (those with the highest and lowest mean privacy rating in each condition). Our findings are substantively identical, including findings of statistically significant and non-significant relationships, to those reported in the tables.

Second, since our experimental design is not fully crossed, such that there is no condition with images of a non-bedroom with zero people, the independent variables for room type and number of people are correlated. Therefore we examine key variables (type of room, monitor presence) within each of the conditions for number of people above zero (1-2), as well as the reverse (number of people within each room/monitor condition), using the co-variates as in the self-rated privacy model (#5) for each dependent variable shown in Tables 4, 5, and 6. We find that all substantive and statistically significant relationships reported in 4, 5, and 6 hold in these sub-group analyses, indicating that our reported findings for the independent effects of room type, monitor presence, and number of people are robust.

Third, in considering our findings of significantly higher privacy for one person, and the significantly lower privacy for two, compared to none (or one), we decided to code, post-hoc (i.e., not as part of the experimental design) whether the people in the photo were looking at the camera or not. Our reasoning was that by looking at the camera, the subjects indicate they were aware the photo was being taken, while people not looking at the camera may not be aware of the photo, which could affect perceptions of privacy about the image. Subjects were looking at the camera in about half of all the images with one person, and about one third of all the images with two people. We re-ran statistical models using the co-variates as in the self-rated privacy model (#5) for each of the dependent variables, adding the variable "looking" and found that it significantly reduced the likelihood an image is perceived as private for the dependent variables Took Photo and In Photo/Own Home [coefficient = -.55 (95% CI: -.82, -.09); coefficient = -.58 (95% CI: -.95, -.21) respectively]. There was no statistically significant effect of looking in the model for Saw Photo [coefficient = -.33 (95% CI: -.71, .06)]. All other variables remained substantively and significantly the same as in the models reported in Tables 4, 5, and 6.

This post-hoc finding – that images of people looking at the camera are nearly 50% less likely to be perceived as private compared to images in which the people are not looking (all else equal) – is another indicator of socially-embedded norms about privacy and appropriate image-sharing online. However, this finding can only be considered suggestive given that it was not part of the research design. Future research should more directly test whether the gaze of subject(s) in a photo, including looking at the camera or not, influence perceptions of privacy of the image. As cameras become increasingly embedded in the environment, including being worn continuously by the people around us (e.g., through devices such as the new Google Clips camera, Snapchat Spectacles[12] or the FrontRow FR Wearable Lifestyle Camera[13]), we should expect more and more images to circulate online in which the subjects may not be aware they are captured in the photo. Such practices have implications for privacy: both individual preferences about images we share as well as privacy's broader social norms.

## 6 INSIGHTS AND DISCUSSION OF FINDINGS

Overall, our findings across multiple analyses indicate that privacy norms for personal photos posted online not only exist, but also vary according to their social context. That context includes the number of people in the image and the presence of computer monitors, and according to the subjects' role in relation to the photo (e.g., seeing or taking the photo versus being in the photo) – but not the type of household room. Our findings that expectations of privacy vary relative to the role of the subject support the theoretical claim that norms of privacy are based on variation in acceptable levels of access to oneself and others [5]. In addition to the role of social norms, we show that individual privacy preferences also matter, but that different measures of preferences have different effects. For example, the classic Westin typology used in many studies is not associated with expectations of privacy for personal images. However, other preference measures are associated with privacy expectations. The strongest and most consistent finding is from our measure of self-rated privacy as a simple statement of privacy versus openness. Those who self-rated as private were significantly more likely to rate images as private across all models. In addition, participants in the condition "Own home/ In Photo" who scored higher on the Jensen Online Privacy mean scale [32], and the IUIPC-collection measure proposed by Malhotra et al. [42] were each significantly more likely to rate images in those conditions as private. Future work should continue to test and revise measures of privacy preferences to identify valid and reliable measures.

While some measures of individual privacy preferences matter, social privacy norms for online images are robust to differences in individual preferences. Our findings are consistent with theories of privacy as socially and culturally dynamic rather than merely an individual preference. These findings also suggest that the so-called "privacy paradox," in which individual privacy management behavior appears inconsistent with stated privacy concerns, may result from the lack of complete or specific measurement and/or understanding of the social context in which behavior occurs. Put another way, it is likely that studies with statistical models that examine privacy behaviors but include little or no information about the context of behavior are likely to be under-specified (omitted variables) and so theoretical conclusions or practical implications drawn from such studies are problematic. Not only are such studies problematic from a statistical point-of-view, but they imply that preferences without reference to context or other constraints (e.g., budget) should explain behavior [17, 54]. However, the research reported here as well as other work shows that context and constraints do matter. For example, as Norcie and Camp argue, people may prefer

[12] https://www.spectacles.com
[13] https://www.frontrow.com

more privacy on Facebook, but still choose to participate in the network, and "this choice cannot be accurately described without assessment of the considerable negative externalities"; there are risks to non-participation [54]. The findings reported here for privacy of personal photos highlight the need to consider not only the preferences of the photographer, but also those of the image subject(s), as well as multiple social context dimensions, including image features like the number of people, and broader privacy norms, when considering privacy perceptions and behavior.

Our findings have implications for technology design, indicating that we need design that supports and enables behavior consistent with both privacy preferences and social norms (see also [45] [68]). They also have implications for public policy, such as how laws should require social media companies to adequately enable and inform users about information practices, such as who has access to photos posted online and the extent of tagging content in personal images, to enable them to behave in ways consistent with their preferences and normative expectations about access (e.g. [44, 49, 72]).

Prior exploratory studies of photo privacy [27, 28, 36] found that the presence of computer monitors/screens [36], the type of room depicted in the image [27], and the number of people present [27], and extrapolated from these findings to propose privacy-preserving technology design. Though we did not find that privacy expectations differed by type of room, others have used room characteristics to automatically detect room characteristics for facilitating privacy controls [69]. Though we found computer monitors in photos lower expectations of privacy, Korayem et al. [36] used computer vision techniques to detect monitors in lifelogging images and block them without the need of users to manually flag such images. However, further work is needed to understand privacy expectations for computer screens in images. If it is the case computer screens are simply so commonplace that they are not considered particularly private, then we would expect no effect on privacy at all. Furthermore, it may be the actual exposure of information via screens, and not the screen itself, that increases concerns about privacy in images.

Finally, though not an explicit focus of this study, we did include subject demographic characteristics in all models (data not shown, findings reported in Footnote 10), but did not find any significant effects on expectations of privacy by gender, race, age, or education. Nor did we find any significant effects of frequency of technology use on expectations of privacy. Though this study is not designed to produce population estimates of privacy, these findings require more explicit and direct tests to determine whether and how expectations of privacy for online images may vary by socio-demographic factors.

Overall, our results show that people share common expectations about the privacy of online images, and that such privacy norms are socially contingent and multi-dimensional. Given these findings, image content detection algorithms alone are unlikely to be adequate for enabling privacy management. At the same time these algorithms may exacerbate privacy concerns by disrupting expectations about appropriate access for personal images. Our findings also show that relying on any one dimension of accessibility — whether "type" of information, user privacy preferences, or even social conditions of use — is too limited to make sense of online behavior, since it depends on privacy norms as well as individual preferences and strategies for privacy management (see also [5, 11, 45, 58]). Instead, we must remember that privacy is contextual, multi-dimensional, and socially contingent [5, 52, 61, 67, 82]. One of the socially contingent dimensions of privacy is normative agreement about appropriate access and information flows. Disrupting privacy norms, such as through the increasing spread of digital images of personal lives, is likely to have consequences for behavior and interaction, as well as the broader cultural meaning of privacy. For example, as embedded and wearable cameras become more commonplace, expectations of privacy in public may decline, or bystander concerns may become so great that people begin to avoid certain places or people [56]. To the extent places with embedded cameras are unavoidable (such as court houses

and doctor's offices), people will not be able to act on their privacy concerns. More importantly, the consequences of such changes are not typically distributed equally across population groups [5].

## 7 LIMITATIONS

In evaluating the findings of this study it is important to consider a number of scope conditions, as well as other limitations, that affect the results and possible implications.

One scope condition was that, in seeking to use authentic personal images, this study used publicly available photos from online sources. Though having the advantage of being drawn from the real population of online photos, these photos are already shared online, suggesting they are viewed, at least by the users who posted them, as 'not private'. Thus this sample may be expected to have relatively low expectations of privacy, making it a conservative test of our hypotheses. Despite this skew, we indeed found variation in expectations of privacy depending on both image features and the subjects' relation to the photo. Future studies may want to sample both publicly available and private images to allow for greater potential variability in expectations of privacy.

Using real photos shared online also has the limitation of leaving us as researcher with less control over their specific content, and thus somewhat less precision among photos within conditions. Future work may wish to test other types of photos, including staged photos as visual vignette studies, to permit more control over the characteristics being experimentally explored. Vignette studies use hypothetical situations to examine how different conditions affect some outcome, in the case studied here, expectations about image privacy.

Another potential advantage to using staged photos would be more control over the characteristics of the people in the images, including apparent age, gender and race/ethnicity. We included photos with apparent gender of male and female, but we limited variation in age and race/ethnicity characteristics, to limit the scope conditions for this first round experimental study, by excluding all photos with children and of people with apparent race/ethnicity that was not white/Caucasian. We recognize that identifying 'apparent race/ethnicity' is problematic [24], and that this paucity of images is a limitation to the scope of our findings (in that they apply to expectations of privacy for images with white/Caucasian people only) and of the study's design. Future studies should explore explicitly whether expectations for image privacy vary depending on race/ethnicity, age, and other important socio-demographic characteristics. Future work should also consider ways to test hypotheses like those proposed here using measures of behavior rather than simply expressed expectations.

Finally, this study was conducted via Amazon's Mechanical Turk platform. While steps were taken to recruit a broad sample of respondents, and control for respondent characteristics (including limiting to U.S. respondents), this population has been shown to be different from the general population as a whole, in particular with regards to privacy preferences and sensitivity [34, 43, 74]. However, it is important to point out that our study is not seeking to provide population estimates of privacy expectations but rather to examine variation across hypothesized conditions. Mechanical Turk is widely used for such studies [45, 48]; future work, however, should explore these questions on other platforms that include different populations.

## 8 CONCLUSION AND FUTURE WORK

Overall, our findings show that in addition to having individual preferences about privacy, people share common expectations, or social norms, about the privacy of online images. Specifically, personal images with one person only are two to three times more likely to be rated as private than photos with no or two people. Also, privacy norms for personal images depend on aspects of access to oneself and others that are considered appropriate [5] such that people are much more

likely to say a photo is private if they are in it. New technologies that change current aspects of access or information flows [5, 52] can disrupt norms about privacy.

Online sharing of personal digital images is now ubiquitous in cultures around the world, and certainly in the United States, the setting of this study. High-quality digital cameras are now a standard feature in mobile smart phones. Social media platforms such as Facebook, Snapchat and Instagram (the latter used by 28% of adult Internet users in 2015, including 55% of those users between the ages of 18 and 29) provide their users with new affordances and audiences for image sharing [13]. Alongside camera-enabled smartphones, dedicated wearable cameras such as the Google Clips and Snap Spectacles, as well as lesser known products such as the YoCam,[14] and the iON SnapCam,[15], cater to dedicated photographic self-trackers/'lifeloggers', by collecting large quantities of images and automatically throughout the day, without userâĂŹs having to actively 'take a photo'. The explosion of online sharing of so many personal images, particularly images that reveal previously unobserved aspects of private lives at such scale, can alter perceptions of privacy, including privacy norms — the commonly shared expectations about aspects of access considered appropriate or not [5]. Technologies and practices that change aspects of access to ourselves and to others can disrupt what Helen Nissenbaum [52, 53] calls the contextual integrity of privacy. A better understanding of the social aspects of privacy will help to guide both the design of technical tools to assist users, as well as the policies and practices necessary to ensure that use of new technologies is consistent with our social expectations about appropriate use.

## ACKNOWLEDGMENTS

Anonymized for Submission

## REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (Jan. 2015), 509–514.
[2] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2012. The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research* 49 (April 2012), 160–174.
[3] Shane Ahern, Dean Eckles, Nathaniel Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed? - privacy patterns and considerations in online and mobile photo sharing. *CHI 2007* (2007), 357.
[4] Irwin Altman. 1977. Privacy Regulation: Culturally Universal or Culturally Specific. *Journal of Social Issues* 33, 3 (1977), 66–84.
[5] Denise Anthony, Celeste Campos-Castillo, and Christine Horne. 2017. Toward a Sociology of Privacy. *Annual Review of Sociology* 43, 1 (Aug. 2017), 1–21.
[6] Denise Anthony, Timothy Stablein, and Emily K Carian. 2015. Big Brother in the Information Age: Concerns about Government Information Gathering over Time. *IEEE Security & Privacy* 13, 4 (2015), 12–19.
[7] danah boyd and Eszter Hargittai. 2010. Facebook privacy settings: Who cares? *First Monday* 15, 8 (Aug. 2010).
[8] Celeste Campos-Castillo and Denise L Anthony. 2014. The double-edged sword of electronic health records: implications for patient disclosure. *Journal of the American Medical Informatics Association* 22, e1 (July 2014), e130–e140.
[9] Jaeyoung Choi, Martha Larson, Xinchao Li, Kevin Li, Gerald Friedland, and Alan Hanjalic. 2017. The Geo-Privacy Bonus of Popular Photo Enhancements. In *ICMR '17*. ACM Press, New York, New York, USA, 84–92.
[10] Robert B Cialdini, Carl A Kallgren, and Raymond R Reno. 1991. A Focus Theory of Normative Conduct: A Theoretical Refinement and Reevaluation of the Role of Norms in Human Behavior. Elsevier.
[11] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *CHI '05: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Portland, OR, 81–90.
[12] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses. In *the 32nd annual ACM conference*. ACM Press, New York, New York, USA, 2377–2386.
[13] Maeve Duggan. 2015. *Mobile Messaging and Social Media - 2015* . Technical Report.
[14] Amitai Etzioni. 1999. *The Limits of Privacy*. Basic Books, New York, NY.

[14] http://www.getyocam.com
[15] https://usa.ioncamera.com/snapcam/

[15] Lujun Fang and Kristen LeFevre. 2010. Privacy wizards for social networking sites. In *WWW 2010*. ACM Press, 351.
[16] Gary A. Fine. 2001. Enacting Norms: Mushrooming and the Culture of Expectations and Explanations. In *Social Norms*, Michael Hechter and Karl-Dieter Opp (Eds.). Russell Sage, New York, NY, 139–164.
[17] Vaibhav Garg, Kevin Benton, and L. Jean Camp. 2014. The Privacy Paradox: A Facebook Case Study. In *The 42nd Research Conference on Communication, Information and Internet Policy (TPRC)*.
[18] Shannon Greenwood, Andrew Perrin Social scientist, and Maeve Duggan. 2016. *Social Media Update 2016*. Technical Report.
[19] Jens Grossklags and Alessandro Acquisti. 2007. When 25 Cents is Too Much - An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. *WEIS* (2007).
[20] Aditi Gupta, Markus Miettinen, N Asokan, and Marcin Nagy. 2012. Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling. *SocialCom/PASSAT* (2012), 471–480.
[21] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer Experience of Obscuring Scene Elements in Photos to Enhance Privacy. In *2018 CHI Conference on Human Factors in Computing Systems (CHI '18), To appear*.
[22] Eman T. Hassan, Rakibul Hasan, Patrick Shaffer, David Crandall, and Apu Kapadia. 2017. Cartooning for Enhanced Privacy in Lifelogging and Streaming Videos. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshop on Computer Vision Challenges and Opportunities for Privacy and Security (CV-COPS)*. 29–38.
[23] Michael Hechter and Karl-Dieter Opp (Eds.). 2001. *Social Norms*. Russell Sage, New York, NY.
[24] Melissa R Herman. 2010. Do You See What I Am? *Social Psychology Quarterly* 73, 1 (Jan. 2010), 58–78.
[25] Christine Horne. 2001. Sociological perspectives on social norms. In *Social Norms*, Michael Hechter and Karl-Dieter Opp (Eds.). Russell Sage, New York, NY, 3–34.
[26] Christine Horne, Brice Darras, Elyse Bean, Anurag Srivastava, and Scott Frickel. 2015. Privacy, technology, and norms: The case of Smart Meters. *Social Science Research* 51, C (May 2015), 64–76.
[27] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs. In *CHI 2015*. New York, New York, USA, 1645–1648.
[28] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *UBICOMP 2014*. New York, New York, USA, 571–582.
[29] S Jana, A Narayanan, and V Shmatikov. 2013. A Scanner Darkly: Protecting User Privacy from Perceptual Applications. In *2013 IEEE Symposium on Security and Privacy (SP) Conference*. IEEE, 349–363.
[30] Guillermina Jasso. 2006. Factorial Survey Methods for Studying Beliefs and Judgments. *Sociological Methods & Research* 34, 3 (June 2006), 334–423.
[31] Guillermina Jasso and Karl-Dieter Opp. 1997. Probing the Character of Norms: A Factorial Survey Analysis of the Norms of Political Action. *American Sociological Review* 62, 6 (Dec. 1997), 947–20.
[32] Carlos Jensen, Colin Potts, and Christian Jensen. 2005. Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63, 1-2 (July 2005), 203–227.
[33] Leslie K John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Research* 37, 5 (Feb. 2011), 858–873.
[34] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara B Kiesler. 2014. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. *SOUPS* (2014).
[35] Peter F Klemperer, Yuan Liang, Michelle L Mazurek, Manya Sleeper, Blase Ur, Lujo Bauer, Nitin Gupta Cranor, Lorrie Faith, and Michael K Reiter. 2012. Tag, you can see it! - using tags for access control in photo sharing. *CHI 2007* (2012), 377.
[36] Mohammed Korayem, Robert Templeman, Dennis Chen, David Crandall, and Apu Kapadia. 2016. Enhancing Lifelogging Privacy by Detecting Screens. In *CHI '16: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM Press, New York, New York, USA, 4309–4314.
[37] Zhenzhong Kuang, Zongmin Li, Dan Lin, and Jianping Fan. 2017. Automatic Privacy Prediction to Accelerate Social Image Sharing. In *2017 IEEE Third International Conference on Multimedia Big Data (BigMM)*. IEEE, 197–200.
[38] Yifang Li, Nishant Vishwamitra, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–24.
[39] David Lyon. 1994. *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press, Minneapolis, MN.
[40] David Lyon. 2007. *Surveillance Studies: An Overview*. Polity Press, Cambridge, UK.
[41] Marry Madden. 2012. *Privacy management on social media sites*. Technical Report. Washington, D.C.
[42] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (Dec. 2004), 336–355.
[43] Jenny Marder and Mike Fritz. 2015. The Internet's hidden science factory. (Feb. 2015). https://www.pbs.org/newshour/science/inside-amazons-hidden-science-factory

[44] Kirsten Martin and Katie Shilton. 2015. Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology* 67, 8 (May 2015), 1871–1882.

[45] Kirsten E Martin and Helen Nissenbaum. 2016. Measuring Privacy: Using Context to Expose Confounding Variables. *The Columbia Science & Technology Law Review* 18 (2016), 176–218.

[46] Gary T Marx. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology.* University of Chicago Press, Chicago & New York.

[47] Barrington Moore Jr. 1984. *Privacy: Studies in Social and Cultural History.* M.E. Sharpe, Armonk, NY.

[48] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman M. Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. *SOUPS* (2017).

[49] Gina Neff and Laura Robinson. 2012. THE SOCIAL MATRIX OF THE EMERGENT WEB: GOVERNANCE, EXCHANGE, PARTICIPATION, & ENGAGEMENT. *Information, Communication & Society* 15, 4 (2012), 449–454.

[50] Christena Nippert-Eng. 2010. *Islands of Privacy: Selective Concealment and Disclosure in Everyday Life.* University of Chicago Press, Chicago, IL.

[51] Helen Nissenbaum. 2004. Will Security Enhance Trust Online, or Supplant It? In *Trust and Distrust in Organizations: Dilemmas and Approaches*, Roderick M Kramer and Karen S Cook (Eds.). Russell Sage Foundation, New York, 155–188.

[52] Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford Law Books, Palo Alto, CA.

[53] Helen Nissenbaum. 2015. Respecting Context to Protect Privacy: Why Meaning Matters. *Science and Engineering Ethics* (July 2015), 1–22.

[54] Greg Norcie and L Jean Camp. 2015. The Price Of Privacy: An Examination of the Economic Costs of Abstention from Social Network. In *Amsterdam Privacy Conference.*

[55] Tribhuvanesh Orekondy, Bernt Schiele, and Mario Fritz. 2017. Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images. (April 2017), 1–20.

[56] Alfredo J Perez, Sherali Zeadally, and Scott Griffith. 2017. Bystanders' Privacy. *IT Professional* 19, 3 (2017), 61–65.

[57] Sandra Petronio. 2002. *Boundaries of Privacy: Dialectics of Disclosure.* SUNY Press, New York, NY.

[58] Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, and David Kotz. 2012. Understanding sharing preferences and behavior for mHealth devices. *WPES* (2012), 117.

[59] Nisarg Raval, Landon Cox, Animesh Srivastava, Ashwin Machanavajjhala, and Kiron Lebeck. 2014. MarkIt: Privacy Markers for Protecting Visual Secrets. In *UbiComp '14 Adjunct.* ACM Press, New York, New York, USA, 1289–1295.

[60] Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh. 2009. Capturing Social Networking Privacy Preferences - Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden? *Privacy Enhancing Technologies* 5672, Chapter 1 (2009), 1–18.

[61] Priscilla M Regan. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy.* University of North Carolina Press, Raleigh NC and New York.

[62] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (April 2014), 88–96.

[63] Reinhard Schunck. 2013. Within and between estimates in random-effects models: Advantages and drawbacks of correlated random effects and hybrid models. *Stata Journal* 13, 1 (2013), 65–76.

[64] Reinhard Schunck and Francisco Perales. 2017. Within- and between-cluster effects in generalized linear mixed models: A discussion of approaches and the xthybrid command. *Stata Journal* 17, 1 (2017), 89–115.

[65] Stuart Shapiro. 1998. Places and Spaces: The Historical Interaction of Technology, Home, and Privacy. *The Information Society* 14, 4 (1998), 275–284.

[66] Aaron Smith. 2017. Record shares of Americans have smartphones, home broadband. (Jan. 2017). http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/

[67] Daniel J. Solove. 2008. *Understanding Privacy.* Harvard University Press, Cambridge, MA.

[68] Luke Stark. 2016. The emotional context of information privacy. *The Information Society* 32, 1 (2016), 14–27.

[69] Robert Templeman, Apu Kapadia, Roberto Hoyle, and David Crandall. 2014. Reactive security. In *the 2014 ACM International Joint Conference.* ACM Press, New York, New York, USA, 1297–1306.

[70] Edison Thomaz, Aman Parnami, Jonathan Bidwell, Irfan Essa, and Gregory D Abowd. 2013. Technological approaches for addressing privacy concerns when recognizing eating behaviors with wearable cameras. In *the 2013 ACM international joint conference.* ACM Press, New York, New York, USA, 739–10.

[71] Matt Tierney, Ian Spiro, Christoph Bregler, and Lakshminarayanan Subramanian. 2013. Cryptagram. In *the first ACM conference.* ACM Press, New York, New York, USA, 75–88.

[72] Joseph Turow, Michael Hennessy, and Nora Draper. 2015. The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation. (2015). arXiv:10.2139/ssrn.2820060

[73] Samuel D. Warren and Louis D. Brandeis. 1984. The right to privacy [The implicit made explicit]. In *Philosophical Dimensions of Privacy: An Anthology*, Ferdinand Schoeman (Ed.). Cambridge University Press, Cambridge, UK, 75–103.
[74] Jill Weinberg, Jeremy Freese, and David McElhattan. 2014. Comparing Data Characteristics and Results of an Online Factorial Survey between a Population-Based and a Crowdsource-Recruited Sample. *Sociological Science* 1 (2014), 292–310.
[75] Alan F. Westin. 1970. *Privacy and Freedom.* Athenaeum, New York, NY.
[76] Alan F. Westin. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues* 59, 2 (2003), 431–453.
[77] Allison Woodruff. 2014. Necessary, unpleasant, and disempowering - reputation management in the internet age. *CHI 2007* (2014), 149–158.
[78] Anna Wu and Xiaolong Zhang. 2011. Temporal sensitivity for location disclosure through mobile photo-sharing. In *MLBS '11*. ACM, New York, New York, USA, 67–70.
[79] Jun Yu, Zhenzhong Kuang, Zhou Yu, Dan Lin, and Jianping Fan. 2018. Privacy Setting Recommendation for Image Sharing. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 726–730.
[80] Jun Yu, Zhenzhong Kuang, Baopeng Zhang, Wei Zhang, Dan Lin, and Jianping Fan. 2018. Leveraging Content Sensitiveness and User Trustworthiness to Recommend Fine-Grained Privacy Settings for Social Image Sharing. *IEEE Transactions on Information Forensics and Security* 13, 5 (Jan. 2018), 1317–1332.
[81] J Yu, B Zhang, Z Kuang, and D Lin. 2017. iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning. *IEEE Transactions on Information Forensics and Security* 12, 5 (2017), 1005–1016.
[82] Elia Zureik, L Linda Harling Stalker, Emily Smith, David Lyon, and Yolande E Chan (Eds.). 2010. *Surveillance, Privacy, and the Globalization of Personal Information.* McGill-Queen's University Press, Montreal, QC and Kingston, ON.

## 9 PRIOR PUBLICATION NOTICE

There are no other closely related prior papers or concurrent submissions. Portions of this work appear in the primary author's doctoral dissertation.

Received February 2018; revised March 2018; accepted June 2018