Understanding People's Privacy Attitudes Towards Video Analytics Technologies

Shikun Zhang* Yuanyuan Feng*
Anupam Das† Lujo Bauer*
Lorrie Faith Cranor* Norman Sadeh*

December 2020
CMU-ISR-20-114

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

*School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA
†Department of Computer Science, North Carolina State University, Raleigh, NC, USA

This research was supported in part by grants from DARPA and AFRL under the Brandeis project (FA8750-15-2-0277) and in part by grants from the National Science Foundation (NSF) Secure and Trustworthy Computing program (CNS-1513957, CNS-1801316, CNS-1914486). The US Government is authorized to reproduce and distribute reprints for Governmental purposes not withstanding any copyright notice thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied, of DARPA, AFRL, NSF, or the US Government.

Keywords: privacy preference modeling, facial recognition, video analytics, experience sampling method

Abstract

Cameras are everywhere, and are increasingly coupled with video analytics software that can identify our face, track our mood, recognize what we are doing, and more. We present the results of a 10-day in-situ study designed to understand how people feel about these capabilities, looking both at the extent to which they expect to encounter them at venues they visit as part of their everyday activities and at how comfortable they are with the presence of such technologies across a range of realistic scenarios. Results indicate that while some widespread deployments are expected by many (e.g., surveillance in public spaces), others are not, with some making people feel particularly uncomfortable. Our results further show that people's privacy preferences and expectations are complicated and vary with a number of factors such as the purpose for which footage is captured and analyzed, the particular venue where it is captured, or whom it is shared with. Finally, we consider recent technical advances where video analytics can only be used on footage of individuals who consent to it ("opt in"). New regulations such as the General Data Protection Regulation actually mandate obtaining such consent "at or before the point of collection." Because obtaining consent from users at or before each point of collection could result in significant user burden, we use our data to explore the development of predictive models that could one day assist people in managing such consent. Our results are rather encouraging.

1 Introduction

In August of 2019, a high school in Sweden was fined for unnecessarily relying on facial recognition to track students' attendance, despite obtaining consent [3]. Over the past few years, the growing deployment of video analytics has prompted increased scrutiny from both privacy advocates and regulators [29, 24]. Yet, little is known about how people actually feel about the many different contexts where this technology is being deployed. Video analytics technologies such as facial recognition have generally become increasingly accurate thanks to recent advances in deep learning and computer vision [39], even if some deployments have also been shown to suffer from race and gender bias [74, 40]. The increasing ubiquity of video analytics is contributing to the collection and inference of vast amounts of personal information, including not only people's whereabouts, their activities, whom they are with, and information about their mood, health, and behavior. As the accuracy of algorithms improves and as data continue to be collected across an ever wider range of contexts, inferences made from this data can be expected to reveal ever more sensitive information about individuals. To make things worse, such data collection and usage often take place without people's awareness or consent. While video analytics technologies arguably have many potentially beneficial uses (e.g., law enforcement, authentication, mental health, advanced user interfaces), their broad deployment raises important privacy questions [90].

In the US, the GAO and NIST have recommended more transparency when it comes to appropriate use of facial recognition [93, 4]. New regulations such as the European Union's GDPR and the California Consumer Privacy Act (CCPA) actually mandate specific disclosure and choice requirements, which apply to the deployment of video analytics technologies (e.g., opt-in or opt-out). While these regulations are important steps towards providing data subjects with more information about and more control over their data, they do not specify how people should be notified about the presence of video analytics, or how to effectively empower them to exercise their opt-in or opt-out rights. This includes addressing questions such as when to notify users, what to notify them about, how often to notify them, how to effectively capture their opt-in or opt-out choices, and more. Our research aims to address these issues by developing a more comprehensive understanding of how people feel about video analytics deployments in different contexts, looking both at the extent to which they expect to encounter them at venues they visit as part of their everyday activities and at how comfortable they are with the presence of such technologies across a range of realistic scenarios. Our study is organized around two broad sets of questions.

The first set focuses on understanding people's privacy expectations and preferences. This includes looking for possible social norms that might extend to a larger population [67], or alternatively identifying differences in how people respond to various deployment scenarios.

The second set of questions is motivated by recent technical advances introduced by Das et al.[27], namely (1) the development of real-time face denaturing functionality that enables video analytics software to only be applied to people who provide consent, and (2) the development of a privacy infrastructure for the Internet of Things (IoT) that enables entities deploying video analytics software to publicize their data practices and allow data subjects to opt in or out of having their footage analyzed and/or shared. Using this functionality, it becomes possible to notify people in real-time as they approach areas where video analytics technologies are deployed and allow them to selectively opt in or out—as required by regulations such as GDPR or CCPA. Because expecting people to manually opt in or out of video analytics each time they come near this type of functionality would entail an unrealistically high number of privacy decisions, we use our data to explore the feasibility of developing predictive models that could assist users with their privacy decisions—with users able to review recommendations from the predictive models.

The main contributions of this work are as follows:

- We conducted a first 10-day in-situ study of people's privacy expectations and preferences across a wide range of realistic video analytics deployment scenarios. We offer an in-depth analysis of the data collected as part of a study involving 123 participants who provided us with detailed insight into their degree of awareness and comfort across a total of 2,328 deployment scenarios.

- Our analysis reveals that many people have little awareness of many of the contexts where video analytics can be deployed and also show diverse levels of comfort with different types of deployment scenarios. Notification preferences are also shown to be diverse and complex, and seem to evolve over time, as people become more sophisticated in their expectations as well as in their realization of the number of notifications they are likely to receive if they are not selective in their notification preferences.

- We use the data collected as part of our study to explore the feasibility of developing predictive models to help people cope with the large number of allow/deny decisions they would otherwise have to make each time they encountered video analytics deployments. In particular, we show that even using simple clustering techniques, it is possible to accurately predict people's privacy decisions across many deployment scenarios. We discuss different ways in which this type of technology could be configured to help people more effectively manage opt-in or opt-out privacy decisions they are entitled to under new regulations such as GDPR and CCPA.

2 Related Work

2.1 Privacy Challenges of Video Analytics

Video analytics, often equipped with facial recognition, is increasingly being integrated with the Internet of Things (IoT) systems [47, 62, 46]. Data privacy has been a central discussion in IoT [71] because IoT systems rely on the collection and use of contextual information (e.g., people, time, location, activity) in environments that often contains identifiable personal data [72, 73, 18]. Researchers have explored technical solutions to safeguard user data in IoT [30, 31, 83], including algorithms to avoid being tracked by video analytics [87, 99, 86]. However, transparency around IoT data privacy remains an unsolved issue [78, 18]. People often have no way to know the existence of video analytics deployments in their daily environments, what personal data is being collected, what purpose the footage is used for, and how long the footage will be retained. Moreover, video analytics has unique data privacy challenges. First, it can collect people's biometric data (e.g., facial features, body pose) [75], which is considered more sensitive than digital identifiers like email addresses. Second, it can be applied later to video footage already collected by existing cameras for a myriad of purposes (e.g., security, operation optimization, targeted advertising).

These challenges indicate that the privacy implications of video analytics differ greatly in real-world scenarios, and should be evaluated case by case. Nissenbaum's privacy as contextual integrity framework [67] is a theory best suited to evaluate the appropriateness of data practices of new technologies by considering important contextual factors. Under the framework, data practices can be evaluated against certain privacy norms in five information flow parameters — the sender, the recipient, the attribute, the subject, and the acceptable transmission principle. Changes to these parameters are likely to cause a privacy norm violation and must be examined closely [68]. However, privacy norms can vary across societies/cultures and may change over time, so existing privacy norms may not be suitable for new technologies like facial recognition in video analytics. Therefore, the first step to address data privacy challenges of video analytics is to establish a baseline of privacy norms by understanding people's opinions and attitudes towards the technology.

2.2 Sampling and Modeling Privacy Preferences

Researchers have made initial progress in discovering privacy norms with IoT technologies in general by sampling people's privacy expectations and preferences through vignette scenarios using large-scale online surveys [10, 65]. However, vignette studies are limited because participants have to imagine themselves in hypothetical scenarios that are not immediately relevant [6]. The experience sampling method (ESM), where both the context and content of individuals' daily life are collected as research data, better examine links between external context and the contents of the mind [42]. Particularly, mobile-based ESM can prompt participants with the actual context they are in, enabling the collection of higher quality, more valid responses [13, 25]. This motivates us to use ESM to elicit people's privacy expectations and preferences towards video analytics. As part of this study, we notify participants about realistic scenarios of video analytics deployment that could happen at the places they actually visit. Then, we ask about their privacy preferences towards these scenarios in situ, aiming to collect high quality responses to elucidate privacy norms regarding video analytics.

This study is also related to previous research on privacy preference modeling. Prior work has shown that individual privacy preferences vary greatly from one person to another and across different data collection and use scenarios [57, 51, 88]. One-size-fits-all models are often unable to capture individuals' diverse privacy preferences when it comes to the collection and use of their data by mobile and IoT technologies. Research on mobile app permission preferences has shown that it is often possible to identify common patterns among the privacy preferences of different subgroups of users [56, 63]. Similar results have been reported in the context of IoT scenarios [51, 52, 65]. Some of this work has also demonstrated the use of machine learning models to predict individuals' privacy preferences [59, 97] and help them manage their privacy decisions [58, 98].

2.3 Designing and Implementing Privacy Assistants

The past ten years have seen a proliferation of privacy settings, whether to enable users to block web trackers or to deny mobile apps access to their location. In practice however, users often struggle to configure privacy settings to match their privacy preferences, whether it is because these settings are unintelligible [84], or because the number of available settings is unmanageable [7, 88, 57, 59], or both.

To overcome these usability challenges, recent research has advocated the introduction of "privacy assistants" to (1) notify people about sensitive data collection and use practices and motivate them to manage associated privacy settings [9], and to (2) also help them configure privacy settings [58, 79]. Privacy assistants can be enhanced by incorporating machine learning models of individuals' privacy preferences to further reduce user burden [98, 57, 59, 58, 91]. For example, Liu et al. successfully demonstrated an Android privacy assistant app that relied on machine learning to generate personalized recommendations about which permission to grant or deny to different apps based on a small number of personalized questions answered by each user [58]. Users could review the recommendations and decide whether or not to accept them. The authors report on a pilot of this technology in the wild, with users indicating they saw value in the way in which this technology made it easier for them to manage a large number of privacy decisions without taking away control over their privacy decisions.

There is a growing body of research focusing on helping people manage their privacy in IoT contexts [33, 26]. This work ranges from the delivery of machine-readable privacy notices to users who are responsible for manually making all privacy decisions [44] to functionality that leverages models of individuals' privacy preferences to help them manage their privacy. The latter includes the use of machine learning to generate privacy setting recommendations that users can review and accept (or reject) [58] as well as functionality that attempts to automate some privacy decisions on behalf of users [33]. Recent work generally indicates that people appreciate privacy assistant technology that helps them manage privacy decisions, while it also reveals that not everyone feels the same way about how much control they are willing to give up in return for a lighter user burden [21]. The work reported herein is intended to supplement this prior research by providing a more in-depth understanding of individuals' privacy expectations and preferences in the context of a diverse set of video analytics scenarios. By understanding how rich and diverse people's expectations and preferences actually are across these scenarios, we aim to build a better understanding of the complexity involved in notifying people about the presence of video analytics deployments and in enabling them to effectively manage associated privacy choices.

3 Designing an Experience Sampling Study

3.1 Experience Sampling Method

Context has been shown to play an important role in influencing people's privacy attitudes and decisions (e.g., contextual integrity [68]). Studying people's privacy attitudes through online surveys is often limited because participants answer questions about hypothetical scenarios and often lack context to provide meaningful answers. Accordingly, we conducted an experience sampling study, where we collected information about people's responses to a variety of video analytics deployments (or "scenarios") in the context of their regular everyday activities. The experience sampling method [42] has been repeatedly used in clinical trials [95, 48], psychological experiments [43, 17] and human-computer interaction (HCI) studies [80, 36], yielding “a more accurate representation of the participants’ natural behaviour” [94]. This enables us to engage and survey participants in a timely and ecologically valid manner as they go about their normal daily lives [70]. Participants are prompted to answer questions about plausible video analytics scenarios at places representative of their actual whereabouts.

3.2 Selecting Realistic Scenarios

Previous research mainly surveyed participants’ privacy attitudes in the context of generic IoT scenarios, including some facial recognition scenarios [65, 52]. By systematically exploring more concrete scenarios in actual settings associated with people’s day-to-day activities, we are able to elicit significantly richer reactions from participants and develop more nuanced models of their awareness, comfort level, and notification preferences pertaining to different deployment scenarios. The scenarios considered in our in-situ study were informed by an extensive survey of news articles about real-world deployments of video analytics in a variety of different contexts (e.g., surveillance, marketing, authentication, employee performance evaluation, and church attendance tracking). These scenarios provided the basis for the identification of a set of relevant contextual attributes which were randomly manipulated and matched against the different types of venues our subjects visited to ensure that the scenarios presented to them were consistent with the scenarios identified in our survey.

Our baseline scenario described the use of generic surveillance cameras with no video analytics. All other scenarios in our study involved the use of some type of video analytics. *Security-related* scenarios included automatic detection of petty crime [81], and identification of known shoplifters and criminals in public places [45, 23, 2, 37]. Scenarios for *commercial* purposes included helping businesses to optimize operations [69, 82, 64], displaying personalized advertisements based on the detection of demographic features [34, 37, 76, 92], collecting patrons’ facial reaction to merchandise [15, 20, 85, 16], and detecting users’ engagement at entertainment facilities [60, 53, 96]. Other significant use case scenarios revolve around *identification* and *authentication*. Here, we considered two broad categories of scenarios: (1) replacing ID cards with facial authentication in schools, gyms, libraries, and places with loyalty programs [32, 66, 11, 89], and (2) attendance tracking in the workplace, at churches, and at gyms [38, 12, 11]. Lastly, we included a small number of plausible, yet hypothetical, scenarios inspired by emerging practices as discussed in news articles or as contemplated in research. This includes health insurance providers using facial recognition and emotion analysis to make health-related predictions [55, 8, 77]; employers using emotion analysis to evaluate employee performance [28, 35, 49, 54]; and hospitals using emotion recognition to make health-related predictions [1, 35, 41].

In total, we identified 16 purposes, as shown in Table 1, representative of a diverse set of video analytics scenarios. A representative list of the scenarios as well as the corresponding text shown to participants to elicit their reactions can be found in the Appendix (Table 6). The scenario text was crafted through multiple iterations to sound plausible without deceiving participants.

Attribute Name	Values
Purpose	Generic Surveillance, Petty crime detection Known criminal detection (Anonymous) people counting (Individualized) jump the line offers (Anonymized) demographic ad targeting (Individualized) ad targeting (Anonymized) sentiment-based ad targeting (Individualized) sentiment-based ad targeting (Anonymous) sentiment-based customer service evaluation (Individualized) customer engagement detection Attendance tracking Using face as IDs Work productivity predictions Health predictions - eatery visits Health predictions - medical visits
Anonymity level	No video analytics Anonymous face detection Facial recognition
Retention of raw footage	ephemeral, 30 days, unspecified
Retention of analysis results	ephemeral, 30 days, unspecified
Sharing specified	Yes, No
Detection of who people are with	Yes, No
Type of places	store, eatery, workplace, education, hospital, service, alcohol, entertainment, fitness, gas, large public places, transportation, worship, library, mall, airport, finance

Table 1: Contextual attributes: Among all the possible combinations of these attributes, our study focused on a subset of 102 scenarios representative of common and emerging deployments of video analytics technology.

3.3 Factorial Design

We employed a factorial study design and developed a taxonomy that captured a representative set of attributes one might expect to influence people's privacy attitudes. These attributes are shown in Table 1. We specified a discrete set of possible values for each attribute, taking into account our desire to cover a broad spectrum of scenarios while also ensuring that we would be able to collect a sufficiently large number of data points for each scenario. Here, we differentiate between the retention time of raw footage and of video analytics results because raw video data, containing biometrics, can be very sensitive, and possibly be exploited for additional analyses afterwards.

3.4 Study Protocol and Procedures

The 10-day study comprised the following five stages.

Stage 1: Eligible participants completed the consent forms for this study, and downloaded the study app from the Google Play Store. Upon installing the app, participants completed a pre-study survey about their perceived knowledge level, comfort level, and notification preference with regard to facial recognition.

Stage 2: Participants were instructed to go about their regular daily activities. The study app collected participants' GPS locations via their smartphones. As they visited points of interest, namely places for which we had one or more plausible deployment scenarios, the app would send them a push notification, prompting them to complete a short survey on a facial recognition scenario pertaining to their location, as illustrated in the app screenshots in Fig. 1(i)–(iv). The protocol limited the number of scenarios presented to each participant to 6 per day, though most of the time participants' whereabouts would trigger a smaller number of scenarios—closer to 3 per day.

Stage 3: On the days participants received push notifications via the app, they also received an email in the evening to answer a daily summary web survey ("evening review"). This web survey showed participants the places they visited when they received notifications, probed reasons for their in-situ answers, and asked a few additional questions. See Fig. 1(v) for an example of the evening review.

Stage 4: After completing 10 days of evening reviews, participants concluded the study by filling out a post-study survey administrated via Qualtrics. This survey contained free-response questions about their attitudes on facial recognition, their responses to three scenarios, the 10-item IUIPC scale on privacy concerns [61], as well as additional demographic questions like income, education level, and marital status.

Stage 5 (Optional): Participants who indicated they were willing to be interviewed in their post-study survey may be invited to an online semi-structured interview. The interview contained questions about study validity, perceptions of scenarios, and clarifications with regard to their earlier responses.

To maximize the contextual benefits provided by the experience sampling method [19], we designed a sophisticated payment scheme to incentivize prompt responses to in-situ notifications. Participants were compensated $2 per day for each day of the study. They received an additional 25 cents per notification they responded to within 15 minutes, or 10 cents if they responded to the notification between 15 and 60 minutes. We also compensated them $2 for the time spent on answering pre-study and post-study surveys. In total, participants could earn between $37 and $52 and were compensated with Amazon gift cards. Participants who completed the online interviews were awarded $10.

3.5 Ensuring Study Validity

Due to the complexity and the number of different components of the study framework, we conducted several pilot rounds, with initial rounds involving members of our research team and later rounds involving a small number (N=9) of external participants. Each pilot round helped identify issues that needed to be addressed, whether in the form of small refinements of our protocol or adjustment to technical components of our system (e.g., study app, web survey app, study server). Below, we briefly discuss the two most important refinements that were made as a result of this process.

Because of the limitations of location tracking functionality, we determined that we could not automatically pinpoint the location of our subjects and use that location to automatically identify a relevant video analytics scenario. Instead, we opted to use location tracking to automatically generate a drop-down list of venues near our subject. We then asked them to select the actual venue where they were. The drop-down list of venues always included three additional options: "I was somewhere else in the area," "I was passing by," and "I was not there." This ensured that our protocols also accounted for missing venues, situations where our subjects were passing by a given location (e.g., being stuck in traffic), as well as situations where location tracking was potentially inaccurate. Participants still received payments for each scenario when they selected one of these three additional choices. In other words, they had no incentive to select a place which they did not visit.

During the first pilot, we found that some participants did not seem to pay close attention to some of the scenario attributes (Table 1). This was remedied by introducing two multiple-choice attention check questions (see Figure 1(ii)). These questions required participants to correctly identify two different and randomly selected contextual attributes assumed in the scenario (attributes in Table 1, excluding type of places). Participants were only allowed to proceed with the remaining in-situ questions once they had passed the two attention checks. These attention checks proved rather effective, as discussed in the Section 4.3.

3.6 Recruitment and Ethics

We recruited participants using four methods: posts on local online forums for the Pittsburgh area (e.g., Craigslist, Reddit), posts in a university-based research participant pool, promotional ads on Facebook, and physical flyers posted on local community bulletin boards and at bus stops. Potential participants were asked to take a short screening survey to determine eligibility (age 18 or older, able to speak English, using an Android smartphone with data plan). The screening survey also displayed the consent form for the study and collected basic demographic information such as age, gender, and occupation. Recruitment materials, the consent form, and the screening survey did not mention or refer to privacy. We tried to avoid convenience samples of undergraduate college students, and purposely looked for participants with a variety of occupations.

This research was approved by our university's institutional review board (IRB) as well as the funding agency's human research protection office. As location data collected over a period of time can be particularly sensitive, we refrained from using off-the-shelf experience sampling software and developed our own system and location-aware Android app.

4 Analyzing Privacy Attitudes

4.1 Participants and Responses

A total of 164 individuals (excluding 9 pilot participants) took part in the study and downloaded our study app from the Google Play Store between May and November 2019, among which 124 completed the 10-day study. One participant was removed due to poor response quality as that person selected "I was somewhere else" for all the notifications received. Among the remaining 123 participants, 10 (8%) were 18-24 years old, 67 (54.5%) were 25-34, 29 (23.6%) were 35-44, 10 (8%) were 45-54, 4 (3%) were 55-64, and 3 (2%) were between 65 and 74. In our sample, 58% identified as female, 41% as male, and 2% as other. Most participants were highly educated: 43 (35%) had bachelor's degrees, and 46 (37%) had graduate degrees. Half of the participants were single and never married, and 42% were married or in a domestic partnership. The majority of our participants (82%) reported having no children under 18 living with them. Participants reported diverse occupations (Table 4 in the Appendix). The average IUIPC factor scores of our participants were shown in Table 2. Comparing our results with those of a large MTurk sample from another study (N=1007) [65] using Mann-Whitney U tests, we found no difference in the collection and the awareness factors, and a significant difference in the control factor with a small effect size ($r = 0.1, p < 0.01$).

	Ours Mean [SD]	MTurk Mean [SD]	Reject H0
IUIPC-Collection	5.90 [1.04]	5.79 [1.11]	No
IUIPC-Control	6.21 [0.78]	5.95 [0.90]	Yes
IUIPC-Awareness	6.53 [0.66]	6.44 [0.82]	No

Table 2: Comparison of IUIPC scores of our participants (N=123) with an MTurk sample (N=1007). H0 stipulates that two samples come from the same population. Cannot reject H0 means that 2 groups are not significantly different.

We recruited interviewees about halfway through the study. Participants were selected based on their demographics. We sent out 17 invitations and conducted online interviews with 10 participants who followed up.

In total, participants were sent 3,589 notifications, prompting them to identify their specific location (Fig. 1(i)). In the majority of cases (65%), our system was able to retrieve a scenario relevant to the location reported by the participant, such as the two different scenarios shown in Fig. 1(ii) and (iii). For the remaining 35%, the system did not have a pre-identified scenario that matched the response provided by the participant, in which case we were unable to elicit any additional information from the participant for that particular location. Based on answers provided by participants, common examples of such situations included the participant being at home or visiting a partner, friend, or relative. Other situations included the participant waiting for a bus or passing by a location. In some instances, participants reported that they did not see the location at which they were in the drop down menu shown to them (Fig. 1(i)). This seemed to most commonly occur when participants were in parks, parking lots, farmers' markets, new establishments, or small local stores.

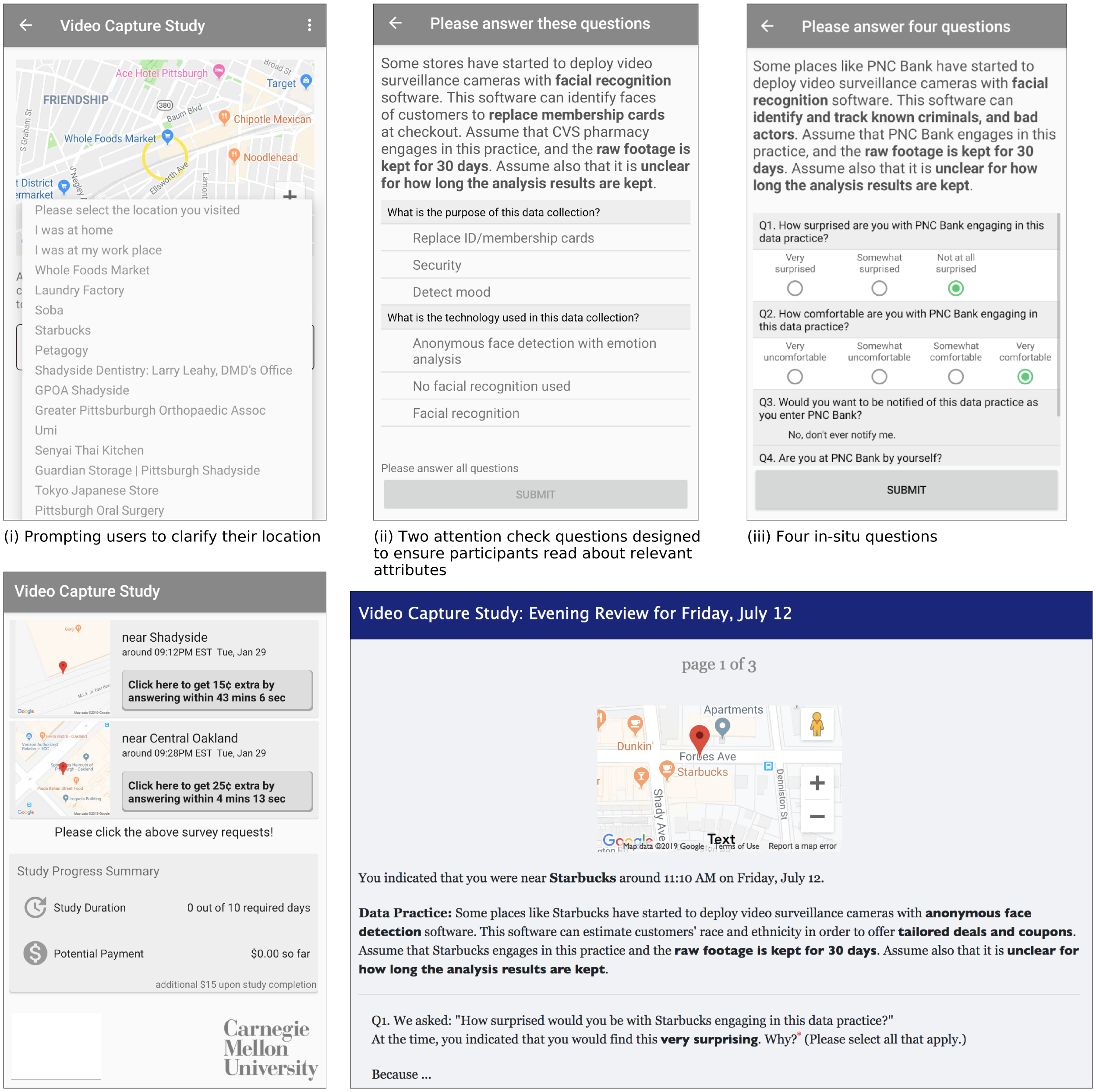
For the 65% of the 3,589 notifications, once participants had reported their location, they were presented with a plausible scenario given their reported location, and were prompted to answer a few quick questions related to that scenario (e.g., see Fig. 1(ii) and (iii)). In addition to these in-situ responses, they were also requested to answer a more complete set of questions about the scenario in the evening. As a result, we were able to collect in-situ and evening responses for a total of 2,328 scenarios. Each participant on average provided in-situ and evening responses to 19 scenarios over a 10-day period, and received an average compensation of $41.

4.2 Collecting People's Privacy Attitudes

When surveying participants' privacy responses to different facial recognition scenarios, we decided to focus on four related sets of questions, namely how surprised they were by the scenario presented to them (**surprise level**), how comfortable they were with the collection and use of their data as assumed in that scenario (**comfort level**), to what extent they would want to be notified about the deployment scenario at the location they visited (**notification preference**), and whether, if given a choice (e.g., opt-in or opt-out), they would have **allowed** or **denied** the data practices described in that scenario at that particular location at the time they visited that location (**allow/deny preference**). These questions were worded as follows—with *Controller* being a variable that would be instantiated with the name of the venue participants were visiting:

- How surprised are you with *Controller* engaging in this data practice?
  - Very surprised, Somewhat surprised, Not at all surprised
- How comfortable are you with *Controller* engaging in this data practice?
  - Very uncomfortable, Somewhat uncomfortable, Somewhat comfortable, Very comfortable
- Would you want to be notified of this data practice as you enter *Controller*?
  - Yes, notify me every time it happens.
  - Yes, but only once in a while to refresh my memory.
  - Yes, but only the first time I enter this location.
  - I don't care I am notified or not.
  - No, don't ever notify me.
- If you had the choice, would you allow or deny this data practice?
  - Allow, Deny

Fig. 2 provides a summary of collected responses organized around the 16 different categories of scenarios (or "purposes") introduced in Table 1. As can be seen, people's responses vary for each scenario. In other words, "one size fits all" would fail to capture people's diverse preferences



Video Capture Study

Please select the location you visited
I was at home
I was at my work place
Whole Foods Market
Laundry Factory
Soba
Starbucks
Petagogy
Shadyside Dentistry: Larry Leahy, DMD's Office
GPOA Shadyside
Greater Pittsburburgh Orthopaedic Assoc
Umi
Senyai Thai Kitchen
Guardian Storage | Pittsburgh Shadyside
Tokyo Japanese Store
Pittsburgh Oral Surgery

(i) Prompting users to clarify their location

Please answer these questions

Some stores have started to deploy video surveillance cameras with **facial recognition** software. This software can identify faces of customers to **replace membership cards** at checkout. Assume that CVS pharmacy engages in this practice, and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.

What is the purpose of this data collection?
Replace ID/membership cards
Security
Detect mood

What is the technology used in this data collection?
Anonymous face detection with emotion analysis
No facial recognition used
Facial recognition

Please answer all questions
SUBMIT

(ii) Two attention check questions designed to ensure participants read about relevant attributes

Please answer four questions

Some places like PNC Bank have started to deploy video surveillance cameras with **facial recognition** software. This software can **identify and track known criminals, and bad actors**. Assume that PNC Bank engages in this practice, and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.

Q1. How surprised are you with PNC Bank engaging in this data practice?

Very surprised	Somewhat surprised	Not at all surprised
○	○	●

Q2. How comfortable are you with PNC Bank engaging in this data practice?

Very uncomfortable	Somewhat uncomfortable	Somewhat comfortable	Very comfortable
○	○	○	●

Q3. Would you want to be notified of this data practice as you enter PNC Bank?
No, don't ever notify me.

Q4. Are you at PNC Bank by yourself?

SUBMIT

(iii) Four in-situ questions

Video Capture Study

near Shadyside
around 09:12PM EST Tue, Jan 29
Click here to get 15¢ extra by answering within 43 mins 6 sec

near Central Oakland
around 09:28PM EST Tue, Jan 29
Click here to get 25¢ extra by answering within 4 mins 13 sec

Please click the above survey requests!

Study Progress Summary

Study Duration	0 out of 10 required days
Potential Payment	$0.00 so far

additional $15 upon study completion

Carnegie Mellon University

(iv) Dashboard showing prompts to complete two in-situ surveys, including monetary incentives to respond as quickly as possible

Video Capture Study: Evening Review for Friday, July 12

page 1 of 3

Text

You indicated that you were near **Starbucks** around 11:10 AM on Friday, July 12.

Data Practice: Some places like Starbucks have started to deploy video surveillance cameras with **anonymous face detection** software. This software can estimate customers' race and ethnicity in order to offer **tailored deals and coupons**. Assume that Starbucks engages in this practice and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.

Q1. We asked: "How surprised would you be with Starbucks engaging in this data practice?"
At the time, you indicated that you would find this **very surprising**. Why?* (Please select all that apply.)

Because ...

(v) Partial screenshot of evening survey associated with a given scenario encountered earlier during the day

Figure 1: Screenshots of the study app and the web survey app used for the evening review

when presented with these different scenarios. At the same time, some scenarios elicit more consistent responses from participants than others. For instance, generic surveillance scenarios appear to surprise participants the least and to elicit acceptance by the most (close to 70% would agree to such scenarios if given a choice and fewer than 10% reported feeling "very uncomfortable" with such scenarios). Yet, even in the presence of such scenarios, 60% of participants reported they would want to be notified at least the first time they encounter these scenarios at a given venue and over 35% indicated they would want to be notified each time. At the other end of the spectrum, scenarios involving facial recognition for the purpose of evaluating employee productivity or tracking attendance at different venues elicited the greatest level of surprise and lowest level of comfort among our participants, with barely 20% reporting that, if given a chance, they would consent to the use of these technologies for the purpose of evaluating employee productivity. Similarly, participants expressed significant levels of surprise and discomfort with scenarios involving the use of facial recognition to make health and medical predictions or to track the attendance of individuals.

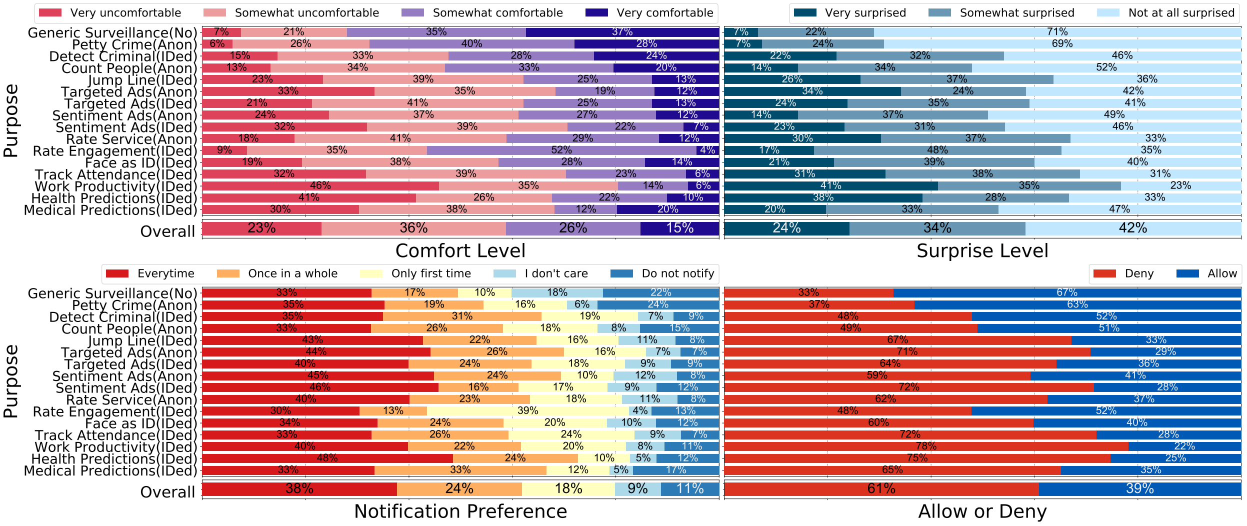


Figure 2: Summary of collected responses organized around 16 different purposes. The bottom row shows the aggregated preferences across different purposes.

4.3 Study Validity and Benefits of ESM

Below we report results on study validity, focusing on three aspects: whether participants carefully read the scenarios, whether they thought the scenarios could happen, and how the ESM helped anchor their responses to their everyday life experience.

Overall, 81% of the time participants successfully completed both attention check questions associated with the scenarios assigned to them within two attempts. Attention questions were found to be useful by 8 out of the 10 interviewees. For instance, one participant (P107) stated, *"I think you definitely had to read them [scenarios]. I think there was one or two that I saw the bold words, and thought that they were the same as older questions, so I picked the same answer, and it was a different one. So once I re-read it, I saw that it was a little different."* Five interviewees reported attention questions helping them discern between retention for raw footage, and retention for analysis results, as P55 said, *"But the first couple of times, I mixed up the raw footage with the analysis results, but after that [the attention checks] I remembered to look for the* *distinction."* The above indicates that the attention checks contributed to participants noticing the contextual attributes associated with each scenario they received. These results also suggest that the responses we collected most likely reflect privacy attitudes that take these contextual attributes into account.

Additionally, 68% of in-situ questions were answered within 15 minutes and 87% within 1 hour. In other words, the actual location visited by the participant and its context associated with the scenario were likely still fresh in their mind (e.g., what the participant was doing at that particular location, whom they might have been with). When asked about whether the scenarios matched actual video collection practices at the places participants were visiting in the exit interviews, most ($N = 7$) stated that they found the scenarios to be realistic, and *"it is entirely possible that it is happening in those places"*(P55). P107 described in details, *"I feel like they can fit in with a lot of the places, I don't know if they actually use any of the strategies right now, but they did seem to fit pretty well with the places like grocery stores offering coupons, or targeting some ads towards you."*

Furthermore, the experience sampling method provided context to participants' responses, with participants reporting that context played an important role in influencing their attitudes towards different video analytics deployments. Fig. 3 plots the reasons participants selected in the evening to explain their discomfort, many of which are directly related to the in-situ context. For instance, one interviewee (P53) specified how her attitudes were affected by the places that she was at, *"I think sometimes different places could require more privacy or more security. Depending on where I am at, I would have more concern maybe."*

4.4 Correlation Between Privacy Expectations and Allow/Deny Preferences

Prior research has shown that comfort is often correlated with the degree of surprise people express towards different data collection and use practices [56]. We compiled pairwise correlations between the four types of responses collected from our participants across the 2,328 scenarios evaluated in our study (Table 3). Correlations were calculated using the Spearman rank correlation with Bonferroni-corrected p-values. Not too surprisingly, we find a significant correlation with a large effect size between people's comfort level and whether they would allow or deny a given scenario. As reported in prior research [56], we also find a moderate correlation, between surprise about some deployment scenarios and comfort with these scenarios. On the other hand, correlation between allow/deny decisions and desire to be notified seems nearly non-existent, suggesting people's notification preferences do not simply correspond with their allow/deny preferences across different scenarios. An example of this case was mentioned in the previous section: only 30% of participants would deny data practices for generic surveillance purposes, but 60% reported that they would like to be notified.

4.5 Factors Impacting People's Privacy Attitudes

The responses collected as part of this in-situ study provide rich insight into people's awareness of the many different ways in which facial recognition is deployed, how comfortable they are with these deployments, and to what extent they would want to be notified about them. Our analysis

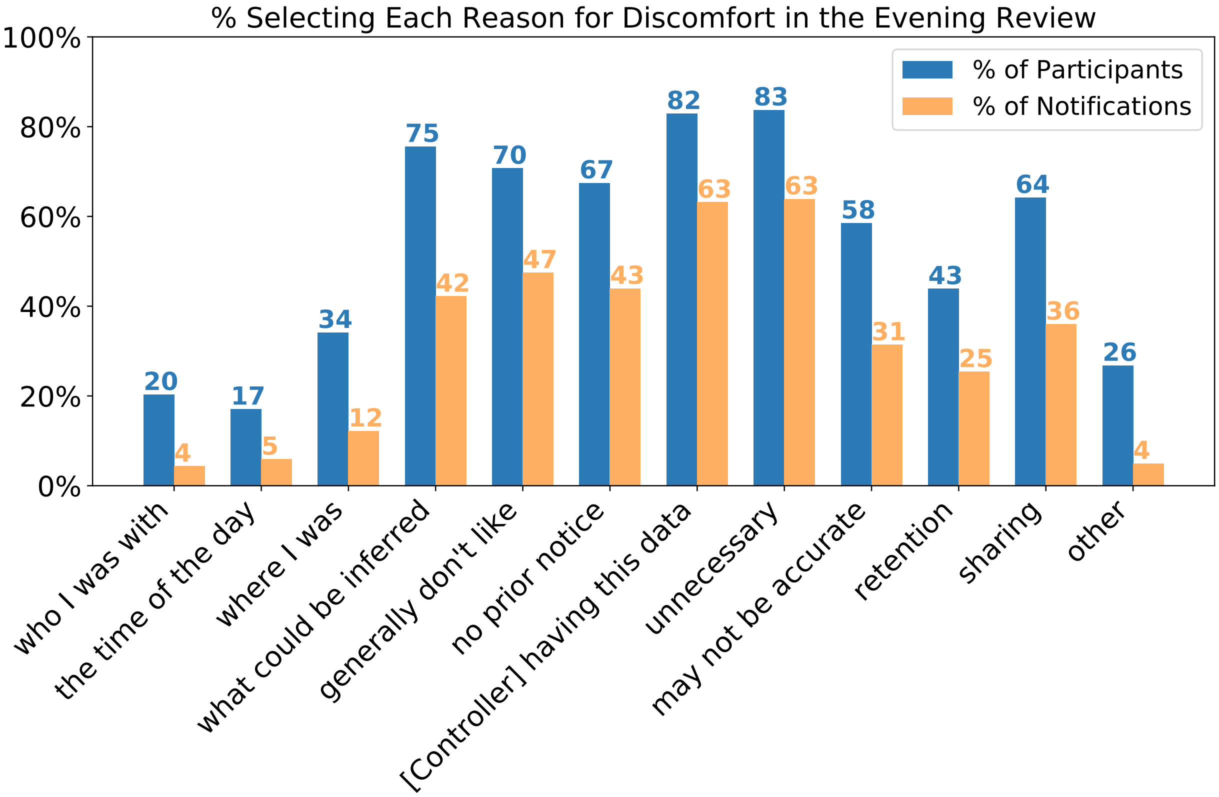


Figure 3: Percent of participants/notifications reporting specific reasons for discomfort. Participants only selected reasons for notifications that they indicated discomfort (N=1,369). N is the used as the denominator to calculate the percent of notifications.

	comfort	surprise	notification
comfort	1		
surprise	0.442	1	
notification	0.183	0.214	1
allow/deny	0.604	0.350	0.046

Table 3: Correlation matrix where indicates $p < 0.001$

is organized around the different contextual factors already identified in Table 1. On average each participant responded to a total of about 19 deployment scenarios. These 19 different scenarios covered an average of 9.9 different "purposes", as defined in Table 1, and 5.9 different types of venues, thereby offering rich insight into how people feel about facial recognition deployments across a range of different situations.

4.5.1 Allow/Deny Decisions

We first investigate whether people's decisions to allow or deny data collection have a relationship with the contextual attributes in Table 1. We constructed our model using generalized linear mixed model (GLMM) regression [14], which is particularly useful for data analysis with repeated measures from each participant. Our GLMM model was fit by maximum likelihood (Laplace approximation) treating the user identifier as a random effect, using a **logistic link** function for the binary response (allow/deny).

Among all the attributes introduced in Table 1, we find that "purpose" exhibits the strongest correlation with the decision to allow or deny data practices associated with our scenarios. In particular, when compared against "generic surveillance" scenarios, 12 out of 15 other purposes came out as being significantly more likely to result in a "deny" decision. Participants were respectively 23.5 (=$e^{3.16}$) times and 29 (=$e^{3.37}$) times more likely to respond with a "deny" to deployment scenarios for predicting work productivity, and for predicting health compared to generic surveillance scenarios with no facial recognition. The odds of participants denying purposes for targeted advertising were at least 6 (=$e^{1.87}$) times and up to 16 (=$e^{3.16}$) times greater than the odds for generic surveillance. Even for the purpose of using faces for authentication and identification, participants were still more likely to deny data practices (odds ratio = $e^{1.70}$ = 5.5). Three purposes turned out not to be significant: detecting petty crime, and using anonymous facial detection to count the number of people in the facility, and using facial emotion detection to rate engagement. The last of the three purposes, despite being relatively intrusive in comparison with the previous two, did not seem to have an important impact. We suspect that it might be partially due to the low number of occurrences ($N = 23$) of this purpose as this scenario was only associated with visits to places like movie theaters, museums, amusement parks, etc.

Contrary to our expectations, we found that whether targeted ads relied on identifying individuals or whether they treated them anonymously did not elicit substantially different responses from our participants. In fact, participants were more likely to respond with a "deny" to facial recognition scenarios used in targeted ads based on demographic features like race or ethnicity than to scenarios which involved individually targeted ads. The interview data revealed that many participants (3 out of 10) were against advertising based on demographics, seeing it as a form of profiling. For example, P106 stated, *"I do think it will divide us more if they are targeting specifically based on what you look like, not even necessarily your profile and who you are ... I think it just gives an overall weird and gross feeling, especially in today's society where it comes up a lot."*

Some of the place type attributes were also found to have an influence on participants' allow or deny decisions. When we compare different place types to the baseline of large public places (e.g., sports stadiums, parking garages, and city hall buildings), we find that participants were more likely to deny data practices at eateries (odds ratio $= e^{1.09} = 3$), at libraries (odds ratio

$= e^{1.71} = 5.5$), at gas stations (odds ratio$= e^{1.36} = 3.9$). Participants were significantly less likely to respond with a "deny" to deployment scenarios at transportation locations (buses stops, train stations, metro stations) than at the baseline (odds ratio $= e^{-1.87} = 0.23$). None of the other attributes were statistically significant ($p < 0.05$). We present the complete results from the regression in the Appendix (Table 5).

4.6 Attitude Change between Start and End of the Study

In our pre-study and post-study surveys, we asked participants the same questions about their understanding of, comfort level with, and notification preference for facial recognition. We also asked them to provide open-ended responses to why their level of concern has (not) changed. We analyzed these responses using inductive coding. Two researchers iteratively improved the codebook and independently coded all responses. Coding discrepancies were discussed and reconciled. We reported results from comparing both surveys and qualitative coding.

4.6.1 Increased Awareness

By the end of the study, we found that one third of participants reported feeling they knew less about facial recognition than they thought at the start. This situation could be explained by the Dunning-Kruger effect, a cognitive bias wherein people tend to overestimate their knowledge in areas which they have with little or no experience [50]. As participants grew more aware of possible video analytics deployments, they gained a more grounded estimate of their knowledge level. 60% of participants $(N = 73)$ conveyed their increased awareness resulting from participation in the study. They did not know facial recognition could be used for so many different purposes, at such a diverse set of venues, and with this level of sophistication. For instance, one participant (P68) wrote, *"Some of the scenarios and growth of the technology you mentioned, I had never considered. Freaked me out."* 11% of the above group reported learning the benefits of facial recognition. *"In the beginning I was very uncomfortable with the fact that this tech could be abused or that law enforcement could use it. However, as the scenarios came up in the study, I realized it could be helpful in my life as long as there are safeguards in place to prevent abuse."*, stated one participant (P106).

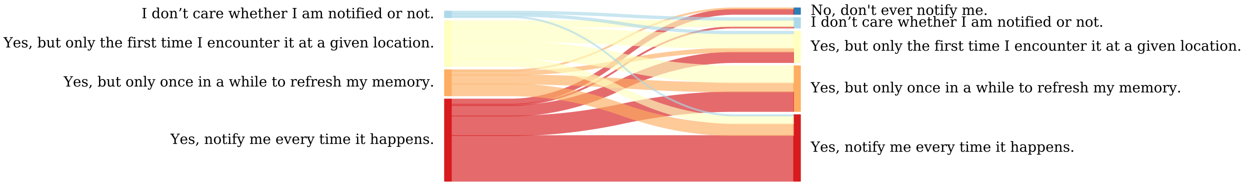


Figure 4: A Sankey diagram shows the change of participants' reported notification preferences before and after the study

4.6.2 Dynamic Notification Preferences

Before the study, 95.9% of all participants claimed that they wanted to be notified about facial recognition deployment scenarios, including 51.2% who indicated they wanted to be notified every time they came within range of facial recognition. As shown in Fig. 4, 55.3% of the participants ended up with different preferences by the time they completed the study regarding whether and how often they wanted to be notified about facial recognition deployments. Among participants who originally wanted to be notified every time, 44% of them opted for less frequent notifications. This is also supported by the descending line in Fig. 5, which plots the percentage of notifications where participants want to be notified every time or once in a while against the number of days in the study.

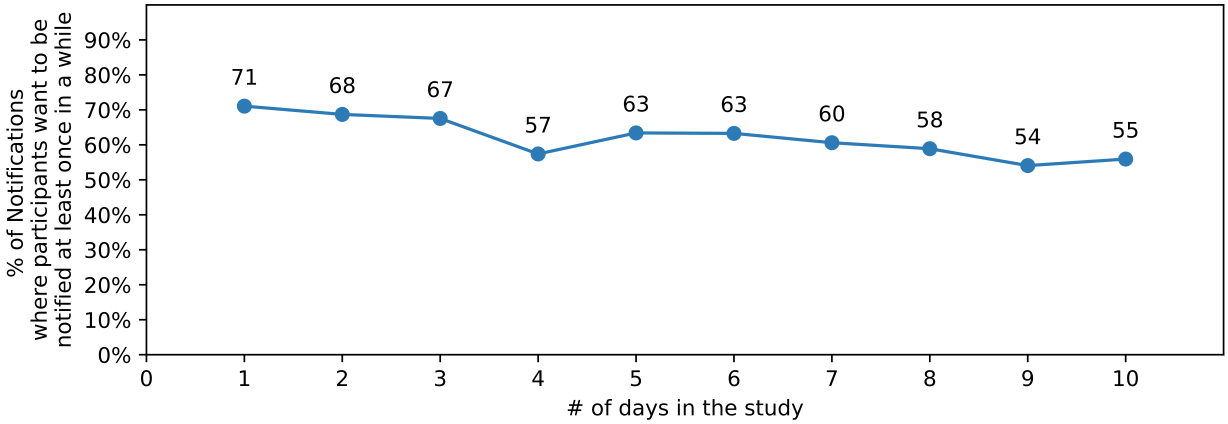


Figure 5: Participants' willingness to be notified decreases as the study progresses

One possible explanation is that people gradually developed a better appreciation for the broad deployment of these scenarios, and the possibility of receiving a large number of notifications, like P53 described, *"I think at first when I first started, I was saying once in a while and then I realized that would be really annoying to get multiple notifications."* Some participants also expressed resignation. For instance, P89 said, *"The whole concept has become normal to me. I've definitely been reminded, through the app, that cameras with facial recognition are used in many, many places. I've become desensitized to the practice, and in fact, what I had considered in some wasys[sic] to be negative because I want my privacy."*

It is also worth noting that, as can be seen in Fig. 4, a simple "Ask on First Use" approach would not accommodate most users. If anything, changes identified in participants' responses before and after the study indicate that people seem to become more sophisticated over time in their notification preferences with a substantially smaller fraction of participants requesting to be notified every time by the end of the study. The majority are looking for some type of selective notification solution.

5 Exploring the Development of Predictive Models

Under regulations such as GDPR data subjects are supposed to be notified and agree to having their footage captured by video analytics software at or before the point of collection. Because of the increasingly widespread deployment of video analytics software, if data subjects are asked to manually opt in or out of video analytics each time they encounter such functionality, they will not only face an unrealistically high number of decisions, but can quickly become annoyed or desensitized as we have observed in the 10-day study. Recent technical advances introduced in prior work by Das et. al [27] open the door to scenarios where a user, with a "privacy assistant" app running on their smartphone, would be alerted to the presence of video analytics software and would be given the choice to opt in or out of such processing. In this section, we use our data to explore the feasibility of developing predictive models to assist users in managing these privacy decisions and discuss different possible deployment strategies for such models. Specifically, we focus on the development of models to predict people's allow/deny decisions across the different types of scenarios using data collected as part of our in-situ study.

5.1 Feature Selection and Clustering

As discussed in the Section 4.5.1, purpose appears to be the most significant attribute when modeling people's allow and deny decisions. Accordingly, we develop models that use purpose as feature—it is likely that more complex models could be developed with possibly even better results. As prior work showed promising results of clustering like-minded users in the mobile app permission space [57, 58], we adopted a similar approach and applied agglomerative clustering with ward linkage on the feature vectors to cluster participants. After we obtained the resulting clusters of users, we calculated the privacy profiles of each cluster using two-thirds majority vote. If more than two thirds of participants in a given cluster allow (deny) a given data practice for a particular purpose, then the cluster profile recommends allowing (denying) that practice for that particular purpose. If there is no majority decision, or the number of data points in the cluster for the particular practice and purpose is too small, the cluster profile does not recommend allowing/denying the practice for the given purpose (i.e., no recommendation).

5.2 Predictive Power of Cluster Profiles

We want to evaluate how well the cluster profiles generated could help predict people's allow/deny decisions for incoming users not present in the clusters. We first randomly select 90% of the participants to build clusters as described in the previous section, and use the remaining 10% of participants to evaluate the predictive power of the clusters by calculating the following two metrics *accuracy* and *efficiency*. *Accuracy* is defined as the percentage of time the prediction of a cluster profile (when such prediction is available) matches the actual allow/deny decisions made by users assigned to that profile. We define *efficiency* as the percentage of allow/deny decisions made by a user for which the assigned cluster of the user offers a prediction (or recommendation). In other words, if for every allow/deny decision a user needs to make, the cluster to which the user is assigned offers a prediction, efficiency is 100 percent—theoretically the user does not need to manually make any decision, though the accuracy of the predictions could be less than 100 percent, as some predictions could be erroneous.

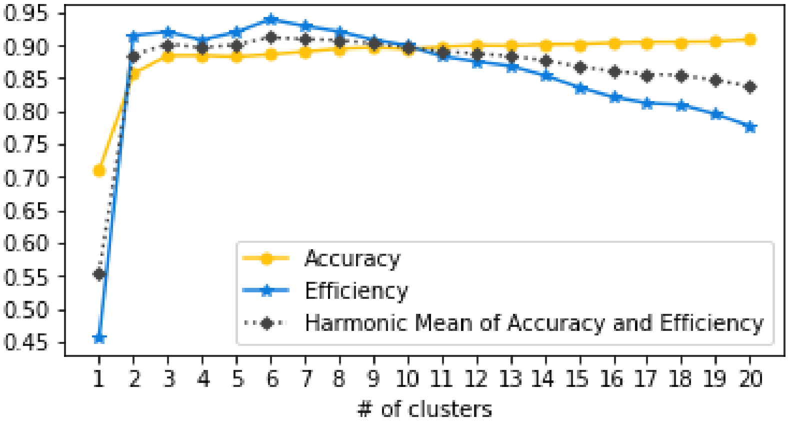
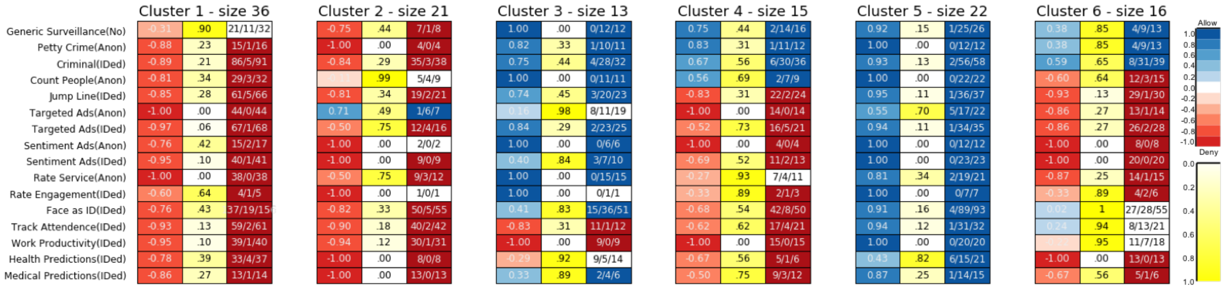


Figure 6: Accuracy and efficiency of models plotted against the number of clusters used to build them.


Allow
1.0
0.8
0.6
0.4
0.2
0.0
-0.2
-0.4
-0.6
-0.8
-1.0
Deny
0.0
0.2
0.4
0.6
0.8
1.0

	Cluster 1 - size 36			Cluster 2 - size 21			Cluster 3 - size 13			Cluster 4 - size 15			Cluster 5 - size 22			Cluster 6 - size 16		
Generic Surveillance(No)	-0.31	.90	21/11/32	-0.75	.44	7/1/8	1.00	.00	0/12/12	0.75	.44	2/14/16	0.92	.15	1/25/26	0.38	.85	4/9/13
Petty Crime(Anon)	-0.88	.23	15/1/16	-1.00	.00	4/0/4	0.82	.33	1/10/11	0.83	.31	1/11/12	1.00	.00	0/12/12	0.38	.85	4/9/13
Criminal(IDed)	-0.89	.21	86/5/91	-0.84	.29	35/3/38	0.75	.44	4/28/32	0.67	.56	6/30/36	0.93	.13	2/56/58	0.59	.65	8/31/39
Count People(Anon)	-0.81	.34	29/3/32	-0.11	.99	5/4/9	1.00	.00	0/11/11	0.56	.69	2/7/9	1.00	.00	0/22/22	-0.60	.64	12/3/15
Jump Line(IDed)	-0.85	.28	61/5/66	-0.81	.34	19/2/21	0.74	.45	3/20/23	-0.83	.31	22/2/24	0.95	.11	1/36/37	-0.93	.13	29/1/30
Targeted Ads(Anon)	-1.00	.00	44/0/44	0.71	.49	1/6/7	0.16	.98	8/11/19	-1.00	.00	14/0/14	0.55	.70	5/17/22	-0.86	.27	13/1/14
Targeted Ads(IDed)	-0.97	.06	67/1/68	-0.50	.75	12/4/16	0.84	.29	2/23/25	-0.52	.73	16/5/21	0.94	.11	1/34/35	-0.86	.27	26/2/28
Sentiment Ads(Anon)	-0.76	.42	15/2/17	-1.00	.00	2/0/2	1.00	.00	0/6/6	-1.00	.00	4/0/4	1.00	.00	0/12/12	-1.00	.00	8/0/8
Sentiment Ads(IDed)	-0.95	.10	40/1/41	-1.00	.00	9/0/9	0.40	.84	3/7/10	-0.69	.52	11/2/13	1.00	.00	0/23/23	-1.00	.00	20/0/20
Rate Service(Anon)	-1.00	.00	38/0/38	-0.50	.75	9/3/12	1.00	.00	0/15/15	-0.27	.93	7/4/11	0.81	.34	2/19/21	-0.87	.25	14/1/15
Rate Engagement(IDed)	-0.60	.64	4/1/5	-1.00	.00	1/0/1	1.00	.00	0/1/1	-0.33	.89	2/1/3	1.00	.00	0/7/7	-0.33	.89	4/2/6
Face as ID(IDed)	-0.76	.43	137/19/156	-0.82	.33	50/5/55	0.41	.83	15/36/51	-0.68	.54	42/8/50	0.91	.16	4/89/93	0.02	1	27/28/55
Track Attendence(IDed)	-0.93	.13	59/2/61	-0.90	.18	40/2/42	-0.83	.31	11/1/12	-0.62	.62	17/4/21	0.94	.12	1/31/32	0.24	.94	8/13/21
Work Productivity(IDed)	-0.95	.10	39/1/40	-0.94	.12	30/1/31	-1.00	.00	9/0/9	-1.00	.00	15/0/15	1.00	.00	0/20/20	-0.22	.95	11/7/18
Health Predictions(IDed)	-0.78	.39	33/4/37	-1.00	.00	8/0/8	-0.29	.92	9/5/14	-0.67	.56	5/1/6	0.43	.82	6/15/21	-1.00	.00	13/0/13
Medical Predictions(IDed)	-0.86	.27	13/1/14	-1.00	.00	13/0/13	0.33	.89	2/4/6	-0.50	.75	9/3/12	0.87	.25	1/14/15	-0.67	.56	5/1/6

Figure 7: Profiles associated with a 6-cluster model. Each cluster profile contains 3 columns: the left one displays the average mean value (deny=-1, allow=1), and the right column represents the cluster profile, where the blue color represents an allow decision, red means a deny, and white means no decision, either because not enough data points are available or for lack of a two-thirds majority. The middle column shows the variances, ranging from 0 to 1. The 3 numbers (D/A/T) in each entry in the the right column represent the distribution of deny (”D”) and allow (”A”) collected for members of the cluster for the corresponding purpose, with T=D+A representing the total number of decisions collected for the given purpose from members of the cluster.

We repeated 10 times the process of generating clusters from randomly drawing 90% of participants, and of evaluating the predictive power of these clusters using allow/deny decisions of the remaining 10% of participants. Average *accuracy* and *efficiency* results are shown in Fig. 6. As can be seen, there is a substantial increase in both accuracy and efficiency when we move from a global one-size-fits-all profile (single cluster) to models with two or more clusters. We can observe the trade-off between efficacy and accuracy as the number of clusters grows. Accuracy increases with the number of clusters, as these clusters become more targeted. Yet, efficiency decreases given that, as the number of clusters increases, the size (or population) of each cluster decreases, eventually making it more difficult to generate predictions as some entries have too few data points to obtain majority voting. The results for six clusters seem to provide the highest harmonic mean of accuracy and efficiency. It is worth noting that a model with 6 clusters achieves an efficiency of 93.9%, namely the clusters are able to predict 93.9% of the allow/deny decisions our participants had to make with an accuracy of 88.9%. It is likely that with additional data, more complex models, taking into account additional features beyond just purpose, could achieve even greater predictive power.

5.3 Example of Cluster Profiles

As shown in Fig. 6, one-size-fits-all models based on lumping all users in a single cluster fail to capture the rich and diverse responses towards facial recognition deployments captured in our study. However, models obtained by organizing participants in a small number of clusters seem to achieve much higher predictive power. Here we look at the profiles associated with a 6-cluster model, (see Fig. 7), namely the model that yielded the highest harmonic mean in the previous section, and discuss what these profiles tell us about how people report feeling towards different deployment scenarios.

As can readily be seen, participants in Cluster 1 and Cluster 5 represent polar extremes, with participants in Cluster 5 indicating they would largely respond with an “Allow” to all the deployment scenarios covered in our study, whereas participants in Cluster 1 would largely respond with a “Deny” to all these scenarios. It is worth also noting the low variances found in these two clusters for most deployment scenarios, indicating that people’s responses in these clusters tend to be particularly homogeneous. All other clusters also exhibit low variances for many scenarios, though each of these other 4 clusters has a few scenarios for which responses are less homogeneous, with each of these other 4 clusters having one or more deployment scenarios where the model is unable to make a prediction (e.g., “Rate Service (Anon)” in the case of Cluster 4). Comparing Cluster 3 with Cluster 5, we see that like in Cluster 5, participants in Cluster 3 tend to respond with an “Allow” to scenarios associated with a variety of different purposes, except when it comes to sensitive purposes like tracking attendance or evaluating work productivity. They tend to also be more reticent in the presence of facial recognition scenarios designed to support health predictions. Members of Cluster 2 exhibit significantly more conservative responses and are generally uncomfortable with a much larger set of deployment scenarios than members of Cluster 3, though they appear to be fine with the use of facial recognition to capture demographic information in support of anonymous targeted advertising scenarios (e.g., adjusting the ad shown in a store window based on demographic features of the person looking at the window [34, 37, 76, 92]). In comparison, members of Cluster 4 seem to exhibit somewhat different sensitivities. While they too object to many deployment scenarios, they appear to be fine with the use of facial recognition to fight crime and to also anonymously count people.

5.4 Possible Application in the Context of Privacy Assistants

The above analysis sheds some light on how different groups of people share many privacy preferences when it comes to opting in or out of different video analytics scenarios and how these preferences vary across different groups. The privacy profiles can also function as meaningful default settings in privacy assistants. The analysis also suggests that it might be possible to predict many privacy decisions a user would otherwise have to manually make if given functionality to systematically opt in or out of video analytics. While it is unlikely that people would want to fully delegate such decisions to software, as this would result in a significant loss of agency, it is easy to imagine configuring privacy assistant functionality where predictive models could be used to recommend some decisions and/or to automatically take care of otherwise tedious and repetitive decisions.

6 Discussion

6.1 Limitations

We would like to start by acknowledging some limitations of our study. Our sample population skews young and more educated, which could have induced bias in our results. Since our participants were recruited only from a mid-sized city in the United States, we do not claim that our results are fully representative of the general population. Our analyses were conducted using data provided by participants when presented with plausible deployment scenarios, rather than based on observations in the presence of actual deployments. While our use of an in situ methodology was intended to mitigate this issue, it is always possible that some of the data collected is not fully representative of participants' actual preferences, concerns and behaviors. We also acknowledge that more sophisticated predictive models could be built with even better performance, but believe that our results are sufficient to demonstrate the potential benefits of using such models.

6.2 Lack of Awareness and Desire for Greater Transparency

Our results clearly indicate that many people were taken by surprise when encountering a variety of video analytics scenarios considered in our study. While many expect surveillance cameras to be widely deployed, few are aware of other types of deployments such as deployments for targeted advertising, attendance, productivity and more. These less expected scenarios are also those that generally seem to generate the greatest discomfort among study participants and those for which, if given a chance, people would often opt out (or not opt in). These results make a strong case for the adoption of more effective notification mechanisms than today's typical "this area under camera surveillance" signs. Not only are people likely to miss these signs, but even if they don't, these signs fail to disclose whether video analytics is being used, for what purpose, who has access to the footage and results, and more. Our study shows that many of these attributes have a significant impact on people's comfort level and their desire to be notified for deployments of video analytics. And obviously, these signs do not provide people with the ability to opt in or out of these practices. Our findings support new disclosure requirements under regulations like GDPR, which mandates the disclosure of this information at or before the point of collection. Our findings also demonstrate the need to give people the ability to choose whether or not to allow the collection and processing of their data, as people express diverse levels of comfort with these scenarios with many not feeling comfortable with at least some of them. These findings are also consistent with new requirements introduced by regulations such as GDPR or CCPA.

6.3 Privacy Preferences Are Complex and Context-Dependent

Our findings show that people's privacy preferences are both diverse and complex. They depend on a number of contextual attributes such as the purpose for using video analytics, who has access to the results, how long the data is retained, but also where the user is at the time of collection and more. As such, our findings are another illustration of contextual integrity principles introduced by Nissenbaum [67]. The importance of purpose information identified in our study (i.e., for what purpose video analytics is being applied) is also consistent with results reported in earlier publications. This includes earlier work conducted by Lin et al. [57] and Smullen et al. [91] in their studies of people's privacy preferences when it comes to configuring mobile app permission setting. This also includes prior work by Emami-Naeini et al.[65], looking at people's privacy preferences across a number of IoT scenarios. In contrast to these earlier studies, our work did not rely on responses to online vignettes. Instead, in our work, people's privacy attitudes were collected in situ in the context of their regular everyday activities. And obviously, our study takes a more systematic approach to exploring a range of video analytics scenarios, varying the type of analysis being carried out, the purpose for which the analysis is conducted, whether information is being shared with other entities, the venue where video analytics is deployed; those factors all have an impact on people's privacy attitudes.

6.4 Implications for the Design of Privacy Assistants

Das et al. have introduced a privacy infrastructure for the Internet of Things, where users rely on "privacy assistant" mobile apps to discover nearby IoT resources such as cameras running video analytics software [26]. Using these privacy assistants, users can access opt-in or opt-out functionality made available by these IoT resources to indicate whether they agree or not to the collection and processing of their data. Das et al. have also reported customizing this infrastructure specifically for video analytics scenarios, including accommodating situations where some people provide consent and others do not, with denaturing software being applied in near real-time to obfuscate the faces of those people who did not provide consent [27]. Such functionality would effectively enable people to exercise those privacy rights granted to them under regulations such as GDPR or CCPA when it comes to video analytics scenarios. However, given the growing deployment of cameras, taking advantage of such functionality would still be hampered by the number of decisions a typical person would have to make each day when passing within range of cameras. Our work on developing models of people's privacy preferences when it comes to granting permissions or not to the collection and processing of data by video analytics software under different scenarios, as presented in Section 5, opens the door to the development of technology that could assist users with such decisions. Specifically, we demonstrated the feasibility of using simple clustering techniques to develop privacy profiles that could be used to accurately predict the majority of a user's privacy decisions. These results are in line with prior research on helping users configure mobile app privacy permissions on their smartphones [57, 58, 91]. In the case of video analytics, such functionality could recommend to users privacy settings that could be repeatedly used to make allow/deny decisions on their behalf each time they encounter facial recognition with available opt-in/opt-out choices, saving them the effort to make these decisions manually each time. A recent study by Colnago et al. suggests that many people would see benefits to having this type of functionality, though not all of them would want to configure it the same way. In Colnago's study some people express a desire to actually delegate many decisions while others indicate they would value the recommendations but would want to more closely control each decision [21]. Further work is needed to identify a simple set of configuration options to accommodate these different sensitivities.

6.5 Evolving Notification Preferences

In our study, we observed that participants' notification preferences evolved over time with people generally opting for somewhat less frequent notifications as time passes. This change in preferences is attributed to some level of fatigue as people got a better appreciation for the number of times they were likely to be notified about the same or similar scenarios, and as their level of surprise in the face of some of these scenarios also diminished over time. Even taking into account this general trend in receiving less frequent notifications over time, it is clear that people's notification preferences are not adequately met if one relies on a simple "Ask on First Use" approach - as is typically the case today when dealing with mobile app permissions, for instance. People's notification preferences are more complex and also more diverse, ultimately requiring a more sophisticated set of configurations that users could choose from - and also modify over time, as their preferences evolve. Here again we see opportunities for the use of AI-based privacy assistants [58, 22] that would adapt to their user's preferences over time, possibly through a combination of nudges designed to motivate users to think about options available to them [5, 9] and dialogues designed to capture people's evolving preferences.

7 Conclusions

We reported on a 10-day experience sampling study designed to help understand people's privacy attitudes related to increasingly diverse video analytics scenarios. Our study collected in-situ responses for a total of 2,328 deployment scenarios from 123 participants as they went about their regular daily activities, presenting them with video analytics scenarios that could realistically be deployed at the venues they visited. The study was informed by a systematic review of recent articles describing existing use of video analytics in support of a range of different purposes. The data collected through this study provides rich insight into people's awareness of, comfort with, and notification preferences associated with these deployments. Our study shows that people's privacy preferences are complex and diverse, and also seem to evolve over time. We show that using clustering techniques, it is often possible to accurately predict people's allow/deny decisions when it comes to authorizing the collection and use of their footage in the context of different facial recognition scenarios. With new regulations requiring to expose opt-in or opt-out choices to users, our results suggest that such models could one day help users more effectively take advantage of these choices without overwhelming them with an unmanageable number of privacy decisions.

References

[1] Augmented mental health: Revolutionary mental health care using emotion recognition. `https://www.augmentedmentalhealth.com/blog/augmented-mental-health-revolutionary-mental-health-care-using-emotion-` May 2018. Accessed: 2020-12-15.

[2] Chinese man caught by facial recognition at pop concert. `https://www.bbc.com/news/world-asia-china-43751276`, April 2018. Accessed: 2020-12-15.

[3] Facial recognition: School ID checks lead to GDPR fine. `https://www.bbc.com/news/technology-49489154`, August 2019. Accessed: 2020-12-15.

[4] Facial recognition technology: Ensuring transparency in government use. `https://www.nist.gov/speech-testimony/facial-recognition-technology-ensuring-transparency-government-use`, June 2019. Accessed: 2020-12-15.

[5] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017.

[6] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International Workshop on Privacy Enhancing Technologies*, pages 36–58. Springer, 2006.

[7] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[8] Marshall Allen. Health insurers are vacuuming up details about you — and it could raise your rates. `https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-y` July 2018. Accessed: 2020-12-15.

[9] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*, pages 787–796, 2015.

[10] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(2), July 2018.

[11] Rachel Bachman. Your gym's tech wants to know you better. `https://www.wsj.com/articles/your-gyms-tech-wants-to-know-you-better-1497281915`, June 2017. Accessed: 2020-12-15.

[12] Sarah Pulliam Bailey. Skipping church? Facial recognition software could be tracking you. `http://www.washingtonpost.com/news/acts-of-faith/wp/2015/07/24/skipping-church-facial-recognition-software-could-be-tracking-you/`, July 2015. Accessed: 2020-12-15.

[13] Lisa Feldman Barrett and Daniel J Barrett. An introduction to computerized experience sampling in psychology. *Social Science Computer Review*, 19(2):175–185, 2001.

[14] Douglas Bates, Martin Mächler, Ben Bolker, and Steve Walker. Fitting linear mixed-effects models using lme4. *Journal of Statistical Software*, 67(1):1–48, 2015.

[15] Bloomberg News. Mannequins collect data on shoppers via facial-recognition software. `https://www.washingtonpost.com/business/economy/mannequins-collect-data-on-shoppers-via-facial-recognition-software/2012/11/22/0751b992-3425-11e2-9cfa-e41bac906cc9_story.html`, November 2012. Accessed: 2020-12-15.

[16] David Burrows. Facial expressions show Mars the adverts that will drive sales. `https://www.foodnavigator.com/Article/2017/03/23/Facial-expressions-show-Mars-the-adverts-that-will-drive-sales`, May 2017. Accessed: 2020-12-15.

[17] Laura L Carstensen, Bulent Turan, Susanne Scheibe, Nilam Ram, Hal Ersner-Hershfield, Gregory R Samanez-Larkin, Kathryn P Brooks, and John R Nesselroade. Emotional experience improves with age: Evidence based on over 10 years of experience sampling. *Psychology and Aging*, 26(1):21, 2011.

[18] Richard Chow. The last mile for IoT privacy. *IEEE Security & Privacy*, 15(6):73–76, 2017.

[19] Tamlin Conner Christensen, Lisa Feldman Barrett, Eliza Bliss-Moreau, Kirsten Lebo, and Cynthia Kaschub. A practical guide to experience-sampling procedures. *Journal of Happiness Studies*, 4(1):53–78, 2003.

[20] Liat Clark. Mannequins are spying on shoppers for market analysis. `https://www.wired.co.uk/article/mannequin-spies-on-customers`, November 2012. Accessed: 2020-12-15.

[21] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing System (CHI '20)*, pages 1–13, 2020.

[22] Jessica Colnago and Hélio Guardia. How to inform privacy agents on preferred level of user control? In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16)*, pages 1542–1547, 2016.

[23] Ben Conarck. Florida court: Prosecutors had no obligation to turn over facial recognition evidence. `https://www.jacksonville.com/news/20190123/florida-court-prosecutors-had-no-obligation-to-turn-over-facial-recogni` January 2019. Accessed: 2020-12-15.

[24] Kate Conger, Richard Fausset, and Serge F. Kovaleski. San Francisco bans facial recognition technology. `https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html`, May 2019. Accessed: 2020-12-15.

[25] Sunny Consolvo and Miriam Walker. Using the experience sampling method to evaluate ubicomp applications. *IEEE Pervasive Computing*, 2(2):24–31, 2003.

[26] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the Internet of Things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, 2018.

[27] Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang, Norman Sadeh, and Mahadev Satyanarayanan. Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1387–1396. IEEE, 2017.

[28] Bobby J Davidson. How your business can benefit from facial recognition technology. `https://percentotech.com/how-your-business-can-benefit-from-facial-recognition-technology/`, November 2019. Accessed: 2020-12-15.

[29] Dean DeChiaro. New York City eyes regulation of facial recognition technology. `https://www.rollcall.com/news/congress/new-york-city-eyes-regulation-of-facial-recognition-technology`, October 2019. Accessed: 2020-12-15.

[30] Benchaa Djellali, Kheira Belarbi, Abdallah Chouarfia, and Pascal Lorenz. User authentication scheme preserving anonymity for ubiquitous devices. *Security and Communication Networks*, 8(17):3131–3141, 2015.

[31] Yitao Duan and John Canny. Protecting user data in ubiquitous computing: Towards trustworthy environments. In *International Workshop on Privacy Enhancing Technologies*, pages 167–185. Springer, 2004.

[32] Melanie Ehrenkranz. Burger joint teams up with surveillance giant to scan your face for loyalty points. https://gizmodo.com/burger-joint-teams-up-with-surveillance-giant-to-scan-y-1821498988, December 2017. Accessed: 2020-12-15.

[33] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung. A contextual-adaptive location disclosure agent for general devices in the internet of things. In *38th Annual IEEE Conference on Local Computer Networks - Workshops*, pages 848–855. IEEE, 2013.

[34] Darrell Etherington. Baidu and KFC's new smart restaurant suggests what to order based on your face. https://techcrunch.com/2016/12/23/baidu-and-kfcs-new-smart-restaurant-suggests-what-to-order-based-on-you December 2016. Accessed: 2020-12-15.

[35] Ingrid Fadelli. Analyzing spoken language and 3-D facial expressions to measure depression severity. https://techxplore.com/news/2018-11-spoken-language-d-facial-depression.html, December 2019. Accessed: 2020-12-15.

[36] Denzil Ferreira, Jorge Goncalves, Vassilis Kostakos, Louise Barkhuus, and Anind K Dey. Contextual experience sampling of mobile application micro-usage. In *Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices & Services (MobileHCI '14)*, pages 91–100, 2014.

[37] Chris Frey. Revealed: how facial recognition has invaded shops—and your privacy. https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto, March 2016. Accessed: 2020-12-15.

[38] Sarah Fister Gale. Employers turn to biometric technology to track attendance. https://www.workforce.com/news/employers-turn-to-biometric-technology-to-track-attendance, March 2013. Accessed: 2020-12-15.

[39] Patrick Grother, Mei Ngan, and Kayee Hanaoka. Ongoing face recognition vendor test (FRVT) part 2: Identification. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf, November 2018. Accessed: 2020-12-15.

[40] Patrick Grother, Mei Ngan, and Kayee Hanaoka. Face recognition vendor test (FRVT) part 3: Demographic effects. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, December 2019. Accessed: 2020-12-15.

[41] Yaron Gurovich, Yair Hanani, Omri Bar, Guy Nadav, Nicole Fleischer, Dekel Gelbman, Lina Basel-Salmon, Peter M Krawitz, Susanne B Kamphausen, Martin Zenker, Lynne M Bird, and Karen W Gripp. Identifying facial phenotypes of genetic disorders using deep learning. *Nature Medicine*, 25(1):60–64, 2019.

[42] Joel M Hektner, Jennifer A Schmidt, and Mihaly Csikszentmihalyi. *Experience sampling method: Measuring the quality of everyday life*. Sage, 2007.

[43] Wilhelm Hofmann, Roy F Baumeister, Georg Förster, and Kathleen D Vohs. Everyday temptations: An experience sampling study of desire, conflict, and self-control. *Journal of Personality and Social Psychology*, 102(6):1318, 2012.

[44] Jason I Hong and James A Landay. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys '04)*, pages 177–189, 2004.

[45] Timothy Johnson. Shoplifters meet their match as retailers deploy facial recognition cameras. `https://www.mcclatchydc.com/news/nation-world/national/article211455924.html`, May 2018. Accessed: 2020-12-15.

[46] Eiman Kanjo, Luluah Al-Husain, and Alan Chamberlain. Emotions in context: examining pervasive affective sensing systems, applications, and analyses. *Personal and Ubiquitous Computing*, 19(7):1197–1212, 2015.

[47] Douglas Korgut and Daniel Fernando Pigatto. An internet of things-based house monitoring system. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 01149–01152, June 2018.

[48] Ingrid Kramer et al. A therapeutic application of the experience sampling method in the treatment of depression: a randomized controlled trial. *World Psychiatry*, 13(1):68–77, 2014.

[49] Sarah Krouse. The new ways your boss is spying on you. `https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604`, July 2019. Accessed: 2020-12-15.

[50] Justin Kruger and David Dunning. Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, 77(6):1121–1134, 1999.

[51] Hosub Lee and Alfred Kobsa. Understanding user privacy in internet of things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, 2016.

[52] Hosub Lee and Alfred Kobsa. Privacy preference modeling and prediction in a simulated campuswide IoT environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 276–285, 2017.

[53] Stephen Lepitak. Disney's Dumbo and Accenture Interactive collaborate for the movie poster of the future. `https://www.thedrum.com/news/2019/03/10/disneys-dumbo-and-accenture-interactive-collaborate-the-movie-poster-th` March 2019. Accessed: 2020-12-15.

[54] David Levine. What high-tech tools are available to fight depression? `https://health.usnews.com/health-care/patient-advice/articles/2017-10-06/what-high-tech-tools-are-available-to-fight-depression`, October 2017. Accessed: 2020-12-15.

[55] David Levine. What your face may tell lenders about whether you're creditworthy. `https://www.wsj.com/articles/what-your-face-may-tell-lenders-about-whether-youre-creditworthy-115602` June 2019. Accessed: 2020-12-15.

[56] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (Ubicomp '12)*, pages 501–510. ACM, 2012.

[57] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS '14)*, pages 199–212, 2014.

[58] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS '16)*, pages 27–41, 2016.

[59] Bin Liu, Jialiu Lin, and Norman Sadeh. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help? In *Proceedings of the 23rd International Conference on World Wide Web (WWW '14)*, pages 201–212, New York, NY, USA, 2014.

[60] Brain Logan. Pay-per-laugh: the comedy club that charges punters having fun. `https://www.theguardian.com/stage/2014/oct/14/standup-comedy-pay-per-laugh-charge-barcelona`, October 2014. Accessed: 2020-12-15.

[61] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[62] Leandro Y. Mano et al. Exploiting IoT technologies for enhancing health smart homes through patient identification and emotion recognition. *Computer Communications*, 89-90:178–190, 2016.

[63] Kirsten Martin and Katie Shilton. Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*, 32(3):200–216, 2016.

[64] Darren Murph. SceneTap app analyzes pubs and clubs in real-time, probably won't score you a Jersey Shore cameo. `https://www.engadget.com/2011/06/12/scenetap-app-analyzes-pubs-and-clubs-in-real-time-probably-won/`, June 2011. Accessed: 2020-12-15.

[65] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS '17)*, pages 399–412, 2017.

[66] NEC Corporation. New biometric identification tools used in theme parks. `https://www.nec.com/en/global/about/mitatv/03/3.html`, 2002. Accessed: 2020-12-15.

[67] Helen Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79(1):119, 2004.

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

[69] PCMag Stuff. NEC unveils facial-recognition system to identify shoppers. `https://www.pcmag.com/archive/nec-unveils-facial-recognition-system-to-identify-shoppers-305015`, November 2012. Accessed: 2020-12-15.

[70] Veljko Pejovic, Neal Lathia, Cecilia Mascolo, and Mirco Musolesi. *Mobile-Based Experience Sampling for Behaviour Research*, pages 141–161. Springer International Publishing, 2016.

[71] Charith Perera, Rajiv Ranjan, Lizhe Wang, Samee U Khan, and Albert Y Zomaya. Big data privacy in the internet of things era. *IT Professional*, 17(3):32–39, 2015.

[72] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, 16(1):414–454, 2013.

[73] Pawani Porambage, Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Athanasios V. Vasilakos. The quest for privacy in the internet of things. *IEEE Cloud Computing*, 3(2):36–45, 2016.

[74] Jon Porter. Federal study of top facial recognition algorithms finds 'empirical evidence' of bias. `https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investig` December 2019. Accessed: 2020-12-15.

[75] Salil Prabhakar, Sharath Pankanti, and Anil K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2):33–42, March 2003.

[76] Press Association. Tesco's plan to tailor adverts via facial recognition stokes privacy fears. https://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces, November 2013. Accessed: 2020-12-15.

[77] Emilee Rader. Most Americans don't realize what companies can predict from their data. https://bigthink.com/technology-innovation/most-americans-dont-realize-what-companies-can-predict-from-their-data-
February 2019. Accessed: 2020-12-15.

[78] Edith Ramirez, Julie Brill, Maureen K Ohlhausen, Joshua D Wright, and Terrell McSweeny. Data brokers: A call for transparency and accountability. Technical report, Federal Trade Commission, May 2014.

[79] Bahman Rashidi, Carol Fung, and Tam Vu. Dude, ask the experts!: Android resource access permission recommendation with RecDroid. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 296–304, 2015.

[80] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*, pages 1–13, 2018.

[81] Timothy Revell. Computer vision algorithms pick out petty crime in CCTV footage. https://www.newscientist.com/article/2116970-computer-vision-algorithms-pick-out-petty-crime-in-cctv-footage
January 2017. Accessed: 2020-12-15.

[82] David Rosen. Disney is spying on you! https://www.salon.com/test/2013/01/17/disney_is_spying_on_you/, January 2013. Accessed: 2020-12-15.

[83] T. Scott Saponas, Jonathan Lester, Carl Hartung, Sameer Agarwal, and Tadayoshi Kohno. Devices that tell on you: Privacy trends in consumer ubiquitous computing. In *16th USENIX Security Symposium (USENIX Security '07)*, pages 55–70, 2007.

[84] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15)*, pages 1–17, 2015.

[85] E. J. Schultz. Facial-recognition lets marketers gauge consumers' real responses to ads. https://adage.com/article/digital/facial-recognition-lets-marketers-gauge-real-responses/298635, May 2015. Accessed: 2020-12-15.

[86] Shawn Shan, Emily Wenger, Jiayun Zhang, Huiying Li, Haitao Zheng, and Ben Y. Zhao. Fawkes: Protecting privacy against unauthorized deep learning models. In *29th USENIX Security Symposium (USENIX Security '20)*, pages 1589–1604, August 2020.

[87] Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, pages 1528–1540, 2016.

[88] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. Privacy tipping points in smartphones privacy preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*, pages 807–816, 2015.

[89] Ed Silverstein. New Konami casino facial recognition technology could rival reward cards. `https://www.casino.org/news/new-konami-casino-facial-recognition-technology-could-rival-reward-card` October 2019. Accessed: 2020-12-15.

[90] Arron Smith. More than half of U.S. adults trust law enforcement to use facial recognition responsibly. Technical report, Pew Research Center, September 2019.

[91] Daniel Smullen, Yuanyuan Feng, Shikun Zhang, and Norman M. Sadeh. The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proc. Priv. Enhancing Technol.*, 2020(1):195–215, 2020.

[92] Benjamin Snyder. This beer ad only works when women pass by. `https://fortune.com/2015/05/21/astra-beer-ad/`, May 2015. Accessed: 2020-12-15.

[93] U.S. Government Accountability Office. Face recognition technology: FBI should better ensure privacy and accuracy. `https://www.gao.gov/assets/680/677098.pdf`, May 2016. Accessed: 2019-11-22.

[94] Niels Van Berkel, Denzil Ferreira, and Vassilis Kostakos. The experience sampling method on mobile devices. *ACM Computing Surveys (CSUR)*, 50(6):1–40, 2017.

[95] Simone JW Verhagen, Laila Hasmi, Marjan Drukker, Jim van Os, and Philippe AEG Delespaul. Use of the experience sampling method in the context of clinical trials. *Evidence-based Mental Health*, 19(3):86–89, 2016.

[96] Jason Whitely. How facial recognition technology is being used, from police to a soccer museum. `https://www.wfaa.com/article/features/originals/how-facial-recognition-technology-is-being-used-from-police-to-a-soccer` `287-618278039`, November 2018. Accessed: 2020-12-15.

[97] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. The feasibility of dynamically granted permissions: Aligning

mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy*, pages 1077–1093, 2017.

[98] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*, pages 1–13, 2018.

[99] Zuxuan Wu, Ser-Nam Lim, Larry S. Davis, and Tom Goldstein. Making an invisibility cloak: Real world adversarial attacks on object detectors. In Andrea Vedaldi, Horst Bischof, Thomas Brox, and Jan-Michael Frahm, editors, *Computer Vision – ECCV 2020*, pages 1–17. Springer International Publishing, 2020.

A Appendix

Occupation	%	Occupation	%
Business, or sales	12.2	Legal	3.3
Administrative support	9.8	Other	3.3
Scientist	8.9	Graduate student	2.4
Service	8.1	Homemaker	2.4
Education	8.1	Skilled labor	2.4
Computer engineer or IT	7.3	Retired	2.4
Other salaried contractor	7.3	Government	1.6
Engineer in other fields	6.5	Prefer not to say .	1.6
Medical	6.5	Art or writing	.8
Unemployed	4.1	College student	.8

Table 4: Occupation of participants and respective %

B GLMM Table for Allow/Deny

Factors	Est.	Std. Err	Z	p
Intercept	-1.79965	0.60789	-2.96	0.003072
purpose:baseline = Generic Surveillance				
Petty Crime(Anon)	0.57922	0.52134	1.111	0.266563
Criminal Detection(IDed)	1.08567	0.43613	2.489	0.012799
Count People(Anon)	0.54011	0.56511	0.956	0.339187
Jump Line(IDed)	2.12133	0.53749	3.947	7.92E-05
Targeted Ads(Anon)	2.77327	0.56614	4.899	9.66E-07
Targeted Ads(IDed)	1.87295	0.5265	3.557	0.000375
Sentiment Ads(Anon)	2.03323	0.70039	2.903	0.003696
Sentiment Ads(IDed)	2.7837	0.59923	4.645	3.39E-06
Rate Service(Anon)	1.92574	0.55494	3.47	0.00052
Rate Engagement(IDed)	0.9621	0.92536	1.04	0.298478
Face as ID(IDed)	1.70491	0.51797	3.292	0.000997
Track Attendence(IDed)	2.56281	0.60284	4.251	2.13E-05
Work Productivity(IDed)	3.15627	0.63879	4.941	7.77E-07
Health Predictions(IDed)	3.37146	0.58706	5.743	9.30E-09
Medical Predictions(IDed)	1.92103	0.7824	2.455	0.014077
Raw retention:baseline=30 days				
Ephemeral	0.10859	0.3799	0.286	0.775005
Unspecified	0.23487	0.4079	0.576	0.564742
Analytics retention:baseline=unspecified				
Ephemeral	-0.02068	0.81819	-0.025	0.979836
30 days	-0.22812	0.30495	-0.748	0.454423
Association: baseline=No				
associationID	0.27251	0.18042	1.51	0.130937
Shared: baseline=No				
sharedID	-0.09074	0.26258	-0.346	0.729666
dayIndex	0.79628	0.27167	2.931	0.003378
placeType:baseline=large public places				
store	0.73456	0.42748	1.718	0.085732
eatery	1.09194	0.41956	2.603	0.009252
work	0.46835	0.50123	0.934	0.350094
education	-0.48813	0.50161	-0.973	0.330493
hospital	1.11144	0.65184	1.705	0.088178
service	0.67614	0.52179	1.296	0.195037
alcohol	0.81001	0.4635	1.748	0.08053
entertainment	0.80385	0.61804	1.301	0.193377
fitness	1.06873	0.66162	1.615	0.10624
gas	1.36253	0.58379	2.334	0.019598
transportation	-1.48697	0.5998	-2.479	0.013171
worship	-0.27275	0.81689	-0.334	0.738463
library	1.71228	0.71968	2.379	0.01735
mall	1.19774	0.89793	1.334	0.182241
airport	0.08364	0.96362	0.087	0.930832
finance	-1.13355	1.16506	-0.973	0.33058

Table 5: Generalized Linear Mixed Model Regression with Logit Link. A positive coefficient(estimate) shows likeliness of participants' to deny a data collection

Purpose	**Scenario Text**
Generic Surveillance	Some places like %s have started to deploy video surveillance cameras to **deter crime**. (This footage can be shared with **law enforcement**.) Assume that you are captured by such a camera, and the **raw footage is kept for 30 days**.
Petty Crime	Some places like %s have started to deploy video surveillance cameras to **deter crime**. These cameras are equipped with software that can automatically **detect and record petty crime** (e.g. pickpocketing, car break-ins, breaking store windows). When a suspicious scene is believed to have been detected, it is **recorded for further analysis (possibly including facial recognition) and kept for 30 days. Otherwise the data is immediately discarded**. Assume that you are captured by such a camera.
Known Criminal	Some places like %s have started to deploy video surveillance cameras with **facial recognition** software. This software can **identify and track known shoplifters, criminals, and bad actors**. Assume that %s engages in this practice, and the **raw footage is discarded immediately**, with the **analysis results being kept for 30 days**.
Count people	Some places like %s have started to deploy video surveillance cameras with **anonymous face detection** software. This software can estimate the number of customers in the facility in order to **optimize operation**, such as personnel allocation. Assume that %s engages in this practice and it is **unclear for how long all the data (raw footage and analysis results) is kept**.
Jump Line	Some places like %s have started to deploy video surveillance cameras with **facial recognition** software. This software can identify patrons in line and push individualized offers to **skip the wait-line for a fee**. This software can also record your presence and **who you are with**. Assume that %s engages in this practice and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.
Targeted Ads(Anon)	Some places like %s have started to deploy video surveillance cameras with **anonymous face detection** software. This software can estimate customers' race and ethnicity in order to offer **tailored deals and coupons**. Assume that %s engages in this practice and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.
Targeted Ads(IDed)	Some places like %s have started to deploy video surveillance cameras with **facial recognition** software. This software can match detected faces against individual customer profiles in order to offer **tailored deals and coupons**. Assume that %s engages in this practice and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.

Sentiment Ads(Anon)	Some places like %s have started to deploy video surveillance cameras with **anonymous face detection** and **emotion analysis** software. This software can estimate customers' age, gender and ethnicity, and analyze their reactions to items displayed. This software is used to generate **tailored deals and coupons** for different demographic groups. Assume that %s engages in this practice and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.
Sentiment Ads(IDed)	Some places like %s have started to deploy video surveillance cameras with **facial recognition** and **emotion analysis** software. This software recognizes people, and analyzes their reactions to items displayed. Then the software matches detected faces against individual customer profiles to send **tailored deals and coupons** to their phones. Assume that %s engages in this practice and the **raw footage is kept for 30 days**, and it is **unclear for how long the analysis results are kept**.
Rate Service	Some places like %s have started to deploy video surveillance cameras with **anonymous emotion analysis** software. This software can **gauge customer satisfaction** with the service provided by its employees. They can use the results for **employee evaluation and training purposes**. Assume that %s engages in this practice and it is **unclear for how long all the data (raw footage and analysis results) is kept**.
Rate Engagement	Some places like %s have started to deploy video surveillance cameras with **facial recognition** and **emotion analysis** software. This software can identify each patron, and **measure their engagement** at the facility. This software can be used to record your presence and also identify **who you are with**. Assume that %s engages in this practice and the **raw footage is kept for 30 days**, and it is **unclear for how long the analysis results are kept**.
Face as ID	Some stores have started to deploy video surveillance cameras with **facial recognition** software. This software can identify faces of customers to **replace membership cards** at checkout. Assume that %s engages in this practice, and the **raw footage is discarded immediately**. Assume also that it is **unclear for how long the analysis results are kept**.
Track Attendance	Some companies have started to deploy video surveillance cameras with **facial recognition** software. This software can track the work time **attendance of its employees**. This software can also identify how long you participate in different activities and **who you hang out with**. Assume that your workplace engages in this practice, and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.

Word Productivity	Some companies have started to deploy video surveillance cameras with **emotion analysis** and **facial recognition** software. This software can detect the mood of its employees, and **predict their productivity**. Assume that your workplace engages in this practice, and it is **unclear for how long all the data (raw footage and analysis results) is kept**.
Health Predictions	Some eatery chains like %s have started to deploy video surveillance cameras with **emotion analysis** and **facial recognition** software. This software can detect your mood, and record data about your orders. This information can be shared with health insurance providers. The health insurance providers could use such data to estimate your **likelihood of developing depression, diabetes, and obesity**, which can impact your **health insurance premium**. Assume that %s engages in this practice, and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.
Medical Predictions	Some medical facilities have started to deploy video surveillance cameras with **emotion analysis** and **facial recognition** software. This software can automatically detect some physical and mental health problems. This information can be shared with health insurance providers, and impact your **health insurance premium**. Assume that %s engages in this practice, and the **raw footage is kept for 30 days**. Assume also that it is **unclear for how long the analysis results are kept**.

Table 6: Scenarios text shown to participants