A First Look into Users' Perceptions of Facial Recognition in the Physical World

Sovantharith Seng[a,i], Mahdi Nasrullah Al-Ameen[b] and Matthew Wright[a]

[a] *Rochester Institute of Technology, Rochester, New York, USA*

[b] *Utah State University, Logan, Utah, USA*

ARTICLE INFO

Keywords:
Facial recognition
Online study
Privacy
User's perceptions
Vignette study

ABSTRACT

Facial recognition (FR) technology is being adopted in both private and public spheres for a wide range of reasons, from ensuring physical safety to providing personalized shopping experiences. It is not clear yet, though, how users perceive this emerging technology in terms of usefulness, risks, and comfort. We begin to address these questions in this paper. In particular, we conducted a vignette-based study with 314 participants on Amazon Mechanical Turk to investigate their perceptions of facial recognition in the physical world, based on thirty-five scenarios across eight different contexts of FR use. We found that users do not have a binary answer towards FR adoption. Rather, their perceptions are grounded in the specific contexts in which FR will be applied. The participants considered a broad range of factors, including control over facial data, the utility of FR, the trustworthiness of organizations using FR, and the location and surroundings of FR use to place the corresponding privacy risks in context. They weighed the privacy risks with the usability, security, and economic gain of FR use as they reported their perceptions. Participants also noted the reasons and rationals behind their perceptions of facial recognition, which let us conduct an in-depth analysis of their perceived benefits, concerns, and comfort with using this technology in various scenarios. Through this first systematic look into users' perceptions of facial recognition in the physical world, we shed light on the tension between FR adoption and users' concerns. Taken together, our findings have broad implications that advance the Privacy and Security community's understanding of FR through the lens of users, where we presented guidelines for future research in these directions.

DOI: https://doi.org/10.1016/j.cose.2021.102227

1. Introduction

Although technology aims to improve the lives of people, it may introduce new privacy, security, or usability issues if not handled with care. Facial recognition technology (abbreviated as FR in this paper) is no exception. With recent advancements in sensor technology and computing algorithms, FR has started to establish its place in various spheres of everyday life, including its use in authentication, identification, tracking, and providing customers with personalized service. The rise of FR, however, has also led to major privacy concerns, such as its use against protesters in Hong Kong (Doffman, 2019; Mozur, 2019), and even shareholders of major tech companies worried about the use of FR (Singer, 2019).

Legislation surrounding FR technology is still lagging behind, with the government and private entities struggling to draw the line regarding when this technology should be allowed and how much control the user should have over their data collection (Daniels, 2019; King, 2019; Del Rey, 2019; Ghaffary, 2019; Browne, 2019). Surveys conducted by Smith (2019) at Pew Research, the Center for Data Innovation (Castro and McLaughlin, 2019), and the Ada Lovelace Institute (2019) looked into people's trust in law enforcement agencies using FR. There is still a major gap, however, in understanding people's perceptions of the use of FR in everyday life.

We addressed this gap in our work by conducting a vignette-based study with 314 participants on Amazon Mechanical Turk, where we examined thirty-five different vignettes (i.e., scenarios) under eight broad contexts of camera-based FR use in the physical world. We asked the participants about their perceptions of the usefulness of FR and their comfort level with FR being used in different scenarios.

[i] Principal corresponding author
ORCID(s):

Our analysis reveals a mix of concerns and hope about this technology. Participants have a clear idea about their preferences for FR-based identification, authentication, tracking, and services. Many of them reported concern that their individuality and autonomy might be at risk if exposed to FR without being informed and giving explicit consent. Participants did not just report a single feeling about FR adoption. Rather, their perceptions of the benefits of FR, their concerns about it, and their comfort with its use are grounded in the specific context in which it will be applied. For example:

- For unlocking personal devices, participants prefer to use FR as a standalone authentication method instead of using it as a two-factor authentication technique along with entering passwords.
- Participants perceive that FR would be useful for identification (whether accompanied with showing physical ID card or not) to receive in-person service at a financial institution.
- Participants have a preference for FR use based on location and purpose, where they reported less comfort with FR used to show targeted ads at a gas station than FR used to offer personalized service in a library.
- Participants found FR to be more useful and reported being more comfortable with tracking in public gatherings when the reasons for tracking (e.g., public safety and law enforcement) were explained to them.[1].

Our findings, which provide insights into different contexts of FR use, suggest that each use-case of FR should be considered individually, both by government agencies when crafting regulations on the use of FR and by businesses considering to adopt FR. We shed light on the challenges for FR adoption through the lens of users, and examined their perceptions in light of privacy concepts and theories.

2. Background and Related Work

Facial recognition (FR) has experienced a sharp improvement in recent years due to improvements in both hardware and algorithms (Materese, 2018; Phillips, Yates, Hu, Hahn, Noyes, Jackson, Cavazos, Jeckeln, Ranjan, Sankaranarayanan, Chen, Castillo, Chellappa, White and O'Toole, 2018). The failure rate in facial recognition has decreased from 5% to 0.2% over the last eight years (2010 to 2018) (Materese, 2018), and in several instances, FR has been found more effective than manual efforts to successfully recognize a human face (Lu and Tang, 2015).

2.1. A Look into the History of FR

The first reported use of FR dated back to the 1960s, when Woodrow Wilson Bledsoe developed the RAND tablet, which could be used to manually record the coordinate locations of various facial features, including the eyes, nose, hairline, and mouth (Gates, 2004; Ballantyne, Boyer and Hines, 1996). During the 1970s, Goldstein, Harmon, and Lesk (1971; 1972) made important contributions to improve the accuracy of FR. They used 21 specific subjective markers, including lip thickness and hair color, to automatically identify faces, where actual biometrics had to be manually computed. During the late 1980s and the early 1990s, linear algebra was applied to facial recognition, known as the Eigenface Approach, that searches for a low-dimensional representation of facial images (Davis West, 2017; Turk and Pentland, 1991b). Built upon this approach, Turk and Pentland (1991b; 1991a) discovered how to detect faces within images, a significant breakthrough in proving the feasibility of automated facial recognition.

To encourage the commercial face recognition market, the Face Recognition Technology (FERET) program was rolled out by DARPA and NIST during the 1990s and 2000s (NIST, 2017; Davis West, 2017). The project involved creating a database of facial images with the hope that the creation of a large database of test images for FR would contribute to inspire innovation, resulting in a more powerful facial recognition technology. Building on FERET and Face Recognition Vendor Tests, NIST were able to provide law enforcement agencies and the U.S. government with necessary information to identify the best possible ways of deploying FR technology (NIST, 2017; Davis West, 2017). The first use of FR for crime control was reported during the Super Bowl event in 2001 (McCullagh, 2001; Rogers, 2016).

[1] Our study was conducted in 2019, before the George Floyd protests in the US.

2.2. FR in Today's World: Scopes and Risks

FR is used in a wide-range of scenarios at present and the presence of FR is becoming nearly ubiquitous, with more devices that we interact with every day are becoming smart. For example, it is used to unlock personal devices (Finnegan and Kapo, 2018; Tengyuen, 2017; Chmielewski, 2015) and physical space (Wollerton, 2019; Karantzoulidis, 2019); for in-person/on-site (Kwan, 2019; Peter, Glory, Arguman, Nagarajan, Devi and Kannan, 2011; France-Presse, 2019) and online financial transactions (Kan, 2015; Petroff, 2016; Knight, 2017); for identification at the customer service of financial and non-financial organizations (Mejia, 2019; Davis West, 2019; Wang, 2018); to provide personalized services, special offers, or advertisements in the retail store, restaurant, library, and gas station (Pearson, 2018; Bates, 2017; Association, 2013; Romero, 2019); for tracking people at a retail store or public gathering (Davis West, 2018; Brant, 2017; Bates, 2017; Wolfe-Robinson, 2019); while boarding a flight (Oliver, 2019; Wallace, 2018); and to record students' class attendance (Toor, 2017).

As a result, there is growing discussion in the media about the use of FR in everyday life. Recent news indicates that people are in favor of using FR when retailers have to prevent shoplifting (Davis West, 2018) or to help a celebrity identify her stalkers (Castro, 2019). On the other hand, there are concerns about the use of FR, including its biased accuracy. For example, the evaluation of three commercial gender classification systems indicate that darker-skinned females are the most mis-classified group, with error rates of up to 34.7%, while the maximum error rate for lighter-skinned males is 0.8% (Buolamwini and Gebru, 2018).

There are also other security and privacy risks involved with the use of FR (Zhang, Chen, Xue and Wei, 2015; Prabhakar, Pankanti and Jain, 2003; Venkatraman and Delpachitra, 2008). Recently, 27.8 million biometric records were leaked by Biostar (Baraniuk, 2019), where the exposed information include users' fingerprints and facial recognition data that were used to access protected buildings. While many FR systems store *templates* – condensed representations of facial data rather than full facial images – there are several ways to conduct an attack by exploiting a stolen template (Jain, Ross and Uludag, 2005). Worse still, biometric templates are unchangeable and cannot be reissued in the same manner as passwords if compromised (Jain, Nandakumar and Nagar, 2008). Thus, the widespread reliance on FR as a primary authenticator could pose significant security risks (Nandakumar and Jain, 2015; Mehmood and Selwal, 2020).

In public settings, as Bowyer (2004) argues, the use of FR could result in the violation of the right to privacy. The American Civil Liberties Union raised concerns regarding the use of FR at the Super Bowl (Union, 2001). More recently, the shareholders of Amazon demanded that, before the organization sells its FR system to the Government agencies, a thorough investigation should be conducted on how FR could threaten civil, human, and privacy rights of people, and how it would affect the company's reputation and finances (Singer, 2019).

Based on these myriad issues, it is important to systematically investigate how users perceive FR. The findings should help inform government agencies and business entities about the appropriate measures they should take to address the concerns of end-users whose facial information is collected.

2.3. Prior Studies

Zimmerman and Gerber (2017) compared users' perceptions of several biometric and non-biometric authentication schemes, not including FR, and found that participants were most concerned about their privacy in fingerprint-based authentication. In another study, Normalini and Ramayah (2017) examined users' perceptions of biometric authentication in online banking, where authors found a relation between users' trust and the efficacy of an authentication scheme. As reported in this study (Normalini et al., 2017), users are concerned about the reliability of facial recognition, because the changes in ambient light could affect the authentication process. Although these studies (Zimmermann and Gerber, 2017; Normalini et al., 2017) provide insights into the usability and privacy issues of biometric authentication, there lacks a systematic investigation into users' perceptions of FR use in different scenarios of everyday life.

A survey conducted by Pew Research Center focused on people's trust in law enforcement agencies regarding the use of facial recognition to identify suspected criminals (Smith, 2019). It found that more than half of U.S. adults trust law enforcement agencies with the sensible use of FR. In similar contexts, the Center for Data Innovation conducted a survey to learn about people's expectations for the U.S. government in controlling the use of FR, which showed that few people in the U.S. want the Government to limit its use (Castro and McLaughlin, 2019). In the U.K., however, the majority of people want the government to impose restrictions on law enforcement agencies with the use of FR (Institute, 2019). These surveys (Smith, 2019; Castro and McLaughlin, 2019; Institute, 2019) examined trust in law enforcement agencies with the use of FR. However, there is still a large gap in understanding users' perceptions of FR in everyday life. We addressed this challenge in our work, where we considered thirty-five different scenarios under eight broad contexts of camera-based FR use. To the best of our knowledge, this is the first systematic study focused on understanding people's perceptions of the use of FR in the physical world.

3. Methodology

We conducted a vignette-based survey on Amazon Mechanical Turk (MTurk). Vignettes are short stories about hypothetical characters in specified circumstances, to whose situation participants are invited to respond (Finch, 1987). Vignettes are versatile and could be used in a wide-range of studies (Finch, 1987; Barter and Renold, 2000; Anast Seguin and Ambrosio, 2002). For example, vignettes have been used to study different privacy and security contexts, including users' privacy perceptions of emerging technologies (Naeini, Bhagavatula, Habib, Degeling, Bauer, Cranor and Sadeh, 2017; Blythe, Coventry and Little, 2015; Martin, 2012; Martin and Nissenbaum, 2016; Seng, Kocabas, Al-Ameen and Wright, 2019).

3.1. Vignette Design

We designed our vignettes based on the guidelines from prior research, where a vignette should include realistic scenarios and avoid unusual events and characters (Barter and Renold, 2000; Finch, 1987; Anast Seguin and Ambrosio, 2002). In our study, we included those real-world scenarios using FR as reported in news reports and articles.

We carefully reviewed articles reporting the current use of FR in different scenarios, and analyzed multiple reports to have a clear understanding of those use cases. We then arranged focus-group discussions among the researchers involved in this project to categorize the reported use cases into broader *contexts*. We categorized the current use of FR into eight contexts: i) Unlocking Personal Devices; ii) Unlocking a Physical Space; iii) Financial Transactions; iv) Identification at Customer Service; v) Personalized Service and Ads; vi) Tracking People; vii) Boarding; and viii) Recording Attendance. Each of these contexts could include one or multiple *setting*. For example, the context of financial transaction might include settings like ATM transaction, payment at cash register, and online payment. We have considered a total 17 settings across eight contexts based on the reported use of FR (e.g., (Finnegan and Kapo, 2018; Tengyuen, 2017; Chmielewski, 2015; Wollerton, 2019; Karantzoulidis, 2019; Kwan, 2019; Peter et al., 2011; Pearson, 2018; Bates, 2017; Mejia, 2019; Davis West, 2019; Wang, 2018; Oliver, 2019; Wallace, 2018; France-Presse, 2019; Kan, 2015; Petroff, 2016; Knight, 2017; Davis West, 2018; Brant, 2017; Wolfe-Robinson, 2019; Association, 2013; Romero, 2019; Toor, 2017)).

We denote the use of FR as "active" when users consciously interact with the system for the purpose of identification or authentication (e.g., unlocking a personal device). On the other hand, "passive" use of FR does not need a conscious interaction with the system, e.g., for tracking people in a public place.

For each setting, we have considered one or more *scenarios*. In an "active" setting, each scenario represents a way of using FR, like using it as a standalone tool, or combining FR with one of the existing tools applicable to a setting. For example, while unlocking a personal device like a laptop, FR could be used as a single authentication method (scenario: "Laptop A"), or be combined with a traditional password (scenario: "Laptop B"). In a setting where we already have two-factor authentication in place (e.g., debit card and PIN at self-service ATM), we have combined FR with at least one other existing authentication technique in the respective scenarios.

Users understand the purpose of using FR in "active" settings where they consciously interact with this technology. However, in "passive" settings, the purpose of using FR might remain unclear to users unless they are explicitly informed. In each "passive" setting (e.g., "Retail" under the context: "Tracking People"), we have designed scenarios so that we could investigate participants' perceptions of FR based on whether they are informed of the reasons behind collecting their facial information (scenario: "Retail B" and "Retail C") or not (scenario: "Retail A").

3.2. Survey Instrument

There are thirty-five vignettes considered in this study, each presenting a "scenario" within one of seventeen "settings" across eight broad "contexts". Table 1 presents the summary of scenarios (see Table 8 in Appendix for further details). To limit participant fatigue, we used the observations from our pilot study (also see §3.4) to select the number of vignettes for each participant. In this study, we presented each participant with fourteen vignettes, where each vignette was randomly chosen from a distinct setting. No participant was presented with multiple vignettes from the same setting. For example, if a participant was presented with scenario: "Laptop A", she did not get the scenario: "Laptop B", however, she might get the scenario: "Library A" or "Library B". To control for ordering effects, we presented the vignettes to participants in random order.

Context	Setting	Scenario
Unlocking Personal Devices (Finnegan and Kapo, 2018; Tengyuen, 2017; Chmielewski, 2015)	Laptop	**A:** FR is used instead of entering a password to unlock a laptop.
		B: FR is used in conjunction with entering a password to unlock a laptop.
	Smartphone	**A:** FR is used instead of entering a pin/pattern to unlock a smartphone.
		B: FR is used in conjunction with entering a pin/pattern to unlock a smartphone.
Unlocking a Physical Space (Wollerton, 2019; Karantzoulidis, 2019)	Smart Lock	**A:** FR is used instead of physical lock and key to unlock the door at home.
		B: FR is used in conjunction with physical lock and key to unlock the door at home.
Financial Transactions (Kwan, 2019; Peter et al., 2011; France-Presse, 2019; Kan, 2015; Petroff, 2016; Knight, 2017)	ATM	**A:** FR and the debit card are used to make a transaction, where PIN is not required.
		B: FR and 4-digit PIN are used to make a transaction, where debit card is not required.
		C: FR, debit card, and 4-digit PIN are used to make a transaction.
	Cash Register	**A:** FR is used instead of debit/credit card to make a payment at the cash register.
		B: FR is used in conjunction with debit/credit card to make a payment at the cash register.
	Online	**A:** FR is used instead of entering a password to log into the application for making an online payment, where debit/credit card information is linked to that application.
		B: FR is used in conjunction with entering a password to log into the application for making online payment, where debit/credit card information is linked to that application.
Identification at Customer Service (Mejia, 2019; Davis West, 2019; Wang, 2018)	Finance	**A:** FR is used instead of ID card at the service desk.
		B: FR is used in conjunction with ID card at the service desk.
	Non-Finance	**A:** FR is used instead of ID card at the service desk.
		B: FR is used in conjunction with ID card at the service desk.
	In-store Pickup	**A:** FR is used instead of ID card to pick up an item at the store, which was ordered online.
		B: FR is used in conjunction with ID card to pick up an item at the store, which was ordered online.
Personalized Service and Ads (Pearson, 2018; Bates, 2017; Association, 2013; Romero, 2019)	Retail Checkout	**A:** FR, placed at the checkout, is used to keep records of the purchased items of customers (*unstated*).
		B: Same as **A**, but the *stated* reason is to inform them in the future about the deals and offers on items they generally buy (*stated*)
	Restaurant	**A:** FR is used instead of a loyalty card or password to authenticate a loyalty member.
		B: FR is used in conjunction with a loyalty card or password to authenticate a loyalty member.
	Library	**A:** FR, not linked to the user's account, correlates demographic information to book selection (*unstated*).
		B: Same as **A**, but the *stated* reason is to improve book recommendations.
	Gas Station	**A:** FR, not linked to the user's account, is used to identify the user's demographic traits while refueling the vehicle (*unstated*).
		B: Same as **A**, but the *stated* reason is to show the user tailored advertisements on the small TV screen while refueling the vehicle.
Tracking People (Davis West, 2018; Brant, 2017; Bates, 2017; Wolfe-Robinson, 2019)	Retail	**A:** FR is used to track customers during shopping (*unstated*).
		B: Same as **A**, but the *stated* reason is to inform them in the future about deals on items they buy or show interest in (*stated*).
		C: FR is used to track customers during shopping to prevent shoplifting and in-store violence (*stated*).
	Public	**A:** FR is used to track people attending a public event (*unstated*).
		B: FR is used to track people attending a public event for safety and law enforcement (*stated*).
Boarding (Oliver, 2019; Wallace, 2018)	Flight	**A:** FR is used instead of a boarding pass.
		B: FR is used in conjunction with a boarding pass.
Attendance (Toor, 2017)	Classroom	FR is used to facilitate automated attendance tracking in class.

Table 1
Summary of Scenarios Representing the Use of FR (see Table 8 in the Appendix for further details) [Note: *stated* indicates that the reason for using FR was stated to the participants, while *unstated* indicates that it was not]

For each vignette, we presented participants with 7-point Likert-scale questions, which directly asked them to report their perceived usefulness and comfort level with using FR in a scenario presented within that vignette. Along with each Likert-scale question, participants were asked open-ended questions to gain further insight into their perceptions. They also reported if they believed they had encountered the presented scenarios in real-life.

Participants answered demographic questions about gender, age, race, and education (adapted from existing literature (Keeter and Christian, 2012; Funk and Rainie, 2015; Madden and Rainie, 2015)). At the end, we included questions about familiarity with privacy concepts and tools (Kang, Dabbish, Fruchter and Kiesler, 2015; Rao, Schaub, Sadeh, Acquisti and Kang, 2016), and the 10-item IUIPC scale to assess online privacy concern (Malhotra, Kim and Agarwal, 2004). As a data quality control (Peer, Vosgerau and Acquisti, 2014; Kung, Kwok and Brown, 2018), attention checks were distributed throughout the survey.

3.3. Participant Recruitment

The participants were recruited via Amazon Mechanical Turk. MTurk is a crowd-sourcing web service that manages the supply and demand of tasks requiring human intelligence to complete. Requesters post small tasks called Human Intelligence Tasks (HIT) that are then selected and completed by the MTurk workers for a small payment based on the requesters' set rate (Paolacci, Chandler and Ipeirotis, 2010; Ipeirotis, 2010).

3.3.1. MTurk as a Survey Platform

Because of the diversity and representativeness of sample workers (Mortensen and Hughes, 2018; Dupuis, Endicott-Popovsky and Crossler, 2013; Kapelner and Chandler, 2010), MTurk is considered an efficient and reliable platform for experimental and survey-based academic research, including work investigating participants' perceptions of security and privacy (Tan, Bauer, Christin and Cranor, 2020; Habib, Naeini, Devlin, Oates, Swoopes, Bauer, Christin and Cranor, 2018; Ur, Bees, Segreti, Bauer, Christin and Cranor, 2016; Kang, Brown, Dabbish and Kielser, 2014; Kelley, 2010). An analysis by Redmiles et al. (2019) sheds light on the generalizability of security and privacy user studies administered on MTurk. Their study shows that the responses of MTurk participants regarding their security and privacy perceptions are even more representative of the U.S. population as compared to the responses from a census-representative panel. They further found that MTurk participants' responses remain stable over time, which is encouraging for the continued use of MTurk to recruit participants in security and privacy research. Overall, MTurk is considered as good as, if not better, than traditional methods of participant recruitment (Redmiles et al., 2019; Mortensen and Hughes, 2018; Kelley, 2010).

3.3.2. Maximizing Data Quality

While MTurk workers may not always pay close attention to the instructions or survey materials (Oppenheimer, Meyvis and Davidenko, 2009), we followed the following guidelines from prior works (Peer et al., 2014; Kung et al., 2018) to increase the quality of responses in our study.

3.3.2.1 Limits on participation

We set limits on which MTurk workers could take part in our survey. According to the guidelines from prior research (Peer et al., 2014), our survey required that the participants had above a 90% HIT approval rate, and had *Masters Qualifications* granted (Masters qualification is granted by Amazon Mechanical Turk platform to only the top MTurk workers who have consistently demonstrated success in a wide-range of tasks[2]). We limited participation to MTurk workers who lived in the United States or Canada.

3.3.2.2 Attention checks

We interspersed attention-check questions (Kung et al., 2018) throughout the survey to screen for inattentive respondents. Our attention-check questions are composed of two parts. The first part is a statement or a question relating to the FR. The second part reveals that it is an attention-check question and prompts the participant to choose a specific response or skip answering the question. For example, one of the questions was: 'How do you rate the impact of facial recognition technology on human civilization? Please select four as your response to this attention-check question.' For the purpose of analysis, we only considered data from those participants who had passed all of the attention checks.

3.4. Procedure

The survey instrument was implemented in Qualtrics[3]. To test the efficacy of our survey questions, we administered pilot testing on MTurk during the months of April and May in 2019 with a nearly identical survey instrument. We collected data from eleven participants during our pilot testing to validate, refine, and assess the reliability of our survey instrument. We conducted our final study between June 18 and July 29 in 2019. The advertisements on MTurk presented the purpose of our study, procedures, anticipated completion time, and compensation. Prior to participation in the survey, participants were asked to read an informed consent document, where we informed them that they

[2] https://www.mturk.com/worker/help

[3] Qualtrics is an online survey platform used to create, distribute, collect, and analyze survey data (`www.qualtrics.com`)

would only receive payment if they could successfully pass attention checks throughout the survey. We also informed participants that we would not collect any personally identifying information (e.g., names, address, etc.) in connection with survey responses.

Once participants gave their informed consent, we provided them with a link to complete the Qualtrics survey via the MTurk platform. Since FR is an emerging technology that many users might not have encountered in real-life, participants were presented with an image-based tutorial on the basic functionality of FR. Participants were allowed to take as much time as they needed to understand the tutorial before they moved forward with completing the survey. Participants were compensated with $2.50 for completing the study, and the average completion time was about 20 minutes. The entire study was reviewed and approved by our Institutional Review Board.

3.5. Analysis

We compared (through one-way ANOVA or T-tests) the underlying settings in a context, and the underlying scenarios in a setting, in terms of participants' perceived usefulness and comfort with FR.

For one-way ANOVA tests, we also conducted Tukey Tests (Gluck, Schaub, Friedman, Habib, Sadeh, Cranor and Agarwal, 2016; Ayalon and Toch, 2019) as post-hoc analysis. We consider a difference to be statistically significant if the p-value is less than 0.05. If there is a significant difference, we also report the statistical power and effect size.

We performed thematic analysis (Braun and Clarke, 2006; Boyatzis, 1998) on the open-ended responses (i.e., qualitative data) from our participants. We conducted multiple passes through the data in which we iteratively identified and clustered themes or codes present in the data. Two researchers independently developed codes, compared them, and then iterated again until we had developed a consistent codebook. After all qualitative data had been coded, both researchers spot-checked the other's codes and did not find any inconsistencies. Finally, we further organized and taxonomized our codes into higher-level categories.

4. Results

In this section, we present the findings from our user study. For consistency, we use these terms based on the frequency of comments in participants' responses to open-ended questions in each scenario: *a few* (0-10%), *several* (10-25%), *some* (25-40%), *about half* (40-60%), *most* (60-80%), and *almost all* (80-100%). The results of significance tests are presented in Table 3.

4.1. Participants

A total of 357 participants completed the study. As we filtered out 43 participants who failed an attention check question, we got 314 participants whose data are considered for analysis and reported in this paper. About 50% of our participants are female, and the age of our participants ranged between 22 and 72 (average: 41). More than 85% of our participants have continued their education after high school. About 80% of participants identified as White/Caucasian (see Table 2 for further details). All of our participants are from the United States.

4.1.1. Encountering FR in Real Life

FR is a relatively new technology and had been encountered by our participants at different rates for different scenarios (see Table 6 in the Appendix). Thus, we are interested to learn if past encounters with FR have any effect on users' comfort level.

Overall, we found that participants who had encountered a FR scenario in real life perceive FR to be more useful in that scenario ($t = 8.21$, $p < 0.001$, statistical power = 1.0, effect size = 0.5) and reported higher comfort with FR use ($t = 9.04$, $p < 0.001$, statistical power = 1.0, effect size = 0.5), as compared to the participants who had not encountered it (see Table 7 in the Appendix for detailed statistics by scenario).

4.1.2. Privacy Concern and Familiarity

The average self-reported score of the participants was 6.04 (out of 7) in IUIPC online privacy concern scale (Malhotra et al., 2004), and 3.81 in response to the 5-point Likert-scale questions about familiarity with privacy concepts and tools (Kang et al., 2015; Rao et al., 2016) (see Table 4 and 5 in Appendix for further details).

4.1.3. Perceived Usefulness and Comfort with FR

Figure 1 and Figure 2, respectively, illustrate the perceived usefulness of FR and comfort level of participants in different scenarios of FR use. Using Pearson's correlation test, we found a positive correlation between perceived

Demographics		Percentage of Participants
Gender	Male	50.00%
	Female	49.36%
	Other	0.64%
Age	18-24	0.96%
	25-34	28.66%
	35-44	41.08%
	45-54	15.61%
	55-64	10.51%
	65+	3.18%
Race	White	79.62%
	Black/African American	6.37%
	Asian/Pacific Islander	8.92%
	Hispanic/Latino	3.18%
	Multi-racial	1.59%
	Other	0.32%
Education Level	Less than High School	0.32%
	High School Graduate	13.06%
	Some College	34.08%
	4-Year College	39.17%
	Some Post Graduate	3.18%
	Post Graduate	10.19%

Table 2
Demographic Information of the Participants (N = 314)

usefulness and comfort level of participants (r = 0.76), which means that if a participant considers FR to be useful in a given scenario, she is more likely to report higher comfort with the use of FR in that scenario. Overall, the perceived usefulness and comfort level of participants did not significantly vary across their gender, age, race, or educational background.

In the following, we present our findings on the perceptions of participants in different contexts of FR use.

4.2. Unlocking Personal Devices

4.2.1. Perceived Usefulness

Participants consider FR as a more useful authentication technique than traditional password for accessing their personal device, including laptop and smartphone. For instance, P29 noted her experience of using FR in laptop, '...I find it [FR] easier than entering passwords and it is much quicker.' Similarly, P60 is excited to use FR for authenticating to her smartphone, 'It would be incredibly easier than typing manually password every time. I need to access my phone dozens of times a day so this would be awesome.' P105 identified both security and usability benefits in using FR for unlocking smartphone, 'Having your face recognized gives me comfort that no one else will be able to access my phone. I hate to change or use multiple passwords.'

Due to participants' concern about the usability of traditional passwords, using FR as a standalone authentication method seems more useful to them than using it in conjunction with a traditional password ($t = 2.32$, $p < 0.05$, statistical power = 0.7, effect size = 0.5 for Laptop; and $t = 2.66$, $p < 0.01$, statistical power = 0.8, effect size = 0.5 for Smartphone). Also, a few participants reported perceiving using both FR and a traditional password for unlocking a device as "too much security."

While participants found FR to be useful for unlocking personal devices, we got mixed opinions from them about their level of comfort. Some participants indicated that knowing that the authentication information for FR is stored locally in their personal devices makes them feel comfortable with it. On the other hand, participants reported multiple concerns contributing to their discomfort with using FR, as discussed below.

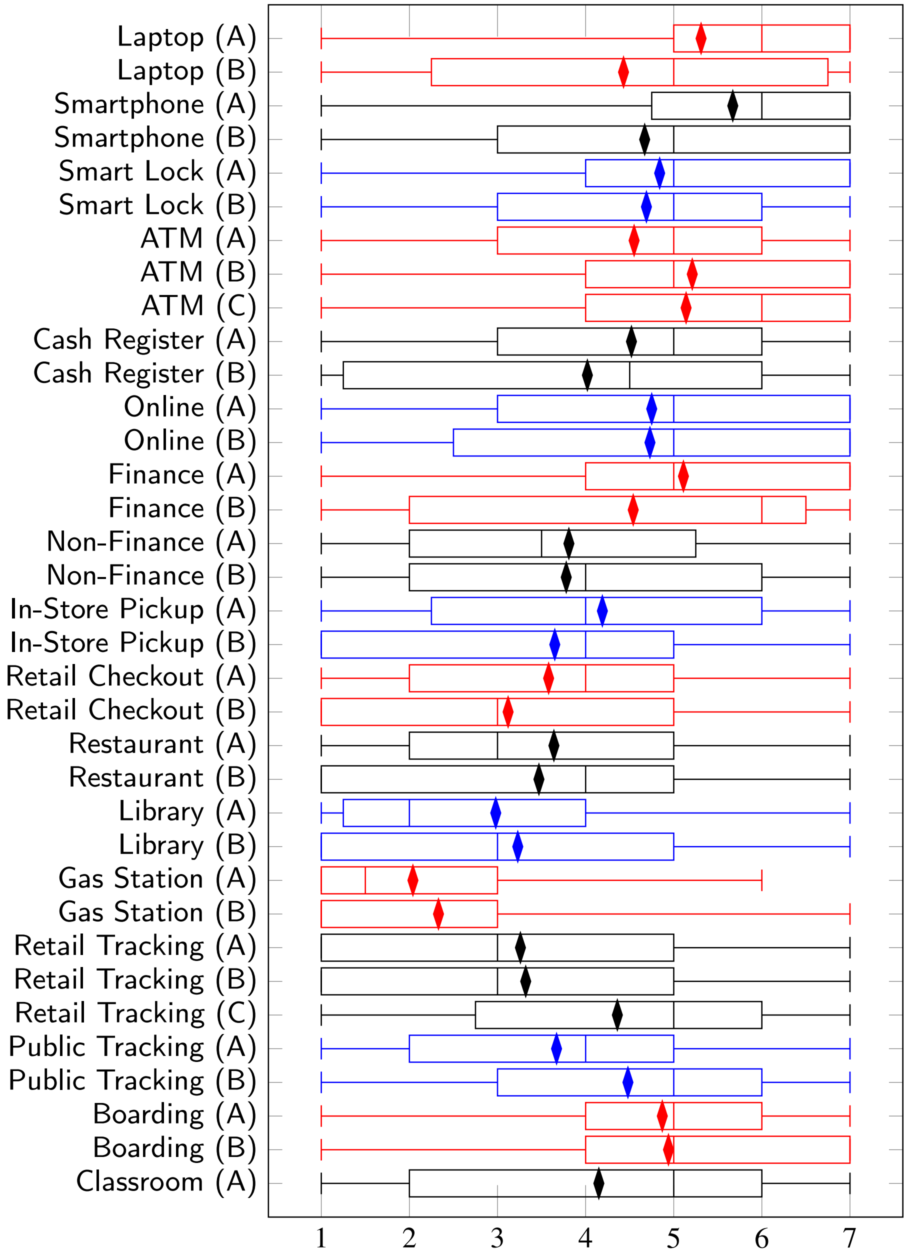

Figure 1: Participants' Perceived Usefulness of FR in Different Scenarios [1: Not useful at all; 7: Very useful]

4.2.2. Users' Concerns

Several participants reported concerns with using FR due to inconvenience of sharing authentication secrets. P82 mentioned, 'The only problem [of using FR] would be if someone like one of my kids or grandchildren want to use my laptop when I am not home, or if something happens to me like being hospitalized and they need an access to something [in my laptop].' Also, participants reported their uncertainty about data protection and privacy. For instance, P290 is not comfortable with using FR for personal devices, as she is not sure about how her facial information would be used and if it would be sold to third parties.

Some participants are not sure yet about the efficacy of this new technology to authenticate them successfully. We speculate, habituation could help with accepting a new authentication technique. For instance, P292 is willing to use FR for her laptop, since she did not face any problems using FR for her smartphone.

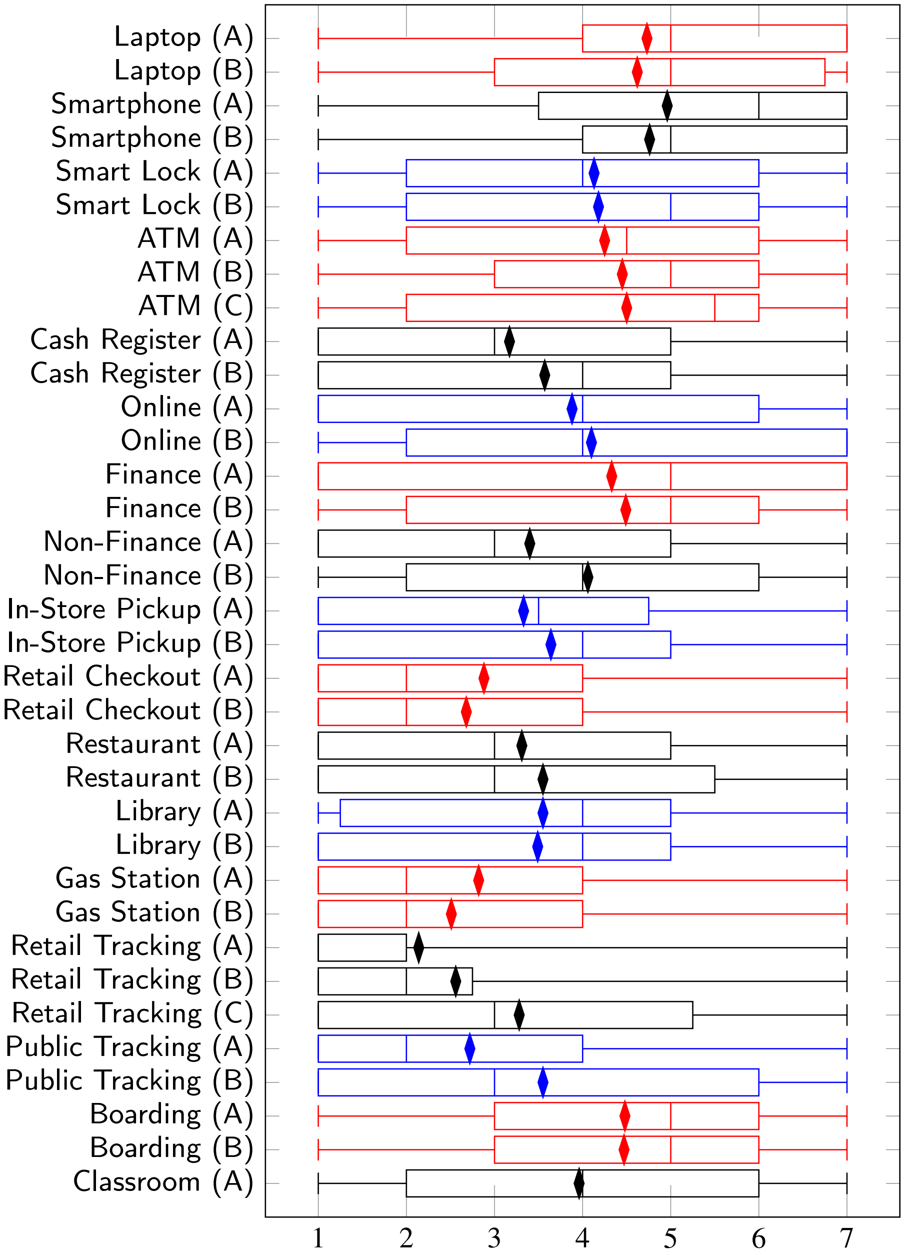

Figure 2: Participants' Comfort Level with FR in Different Scenarios [1: Not comfortable at all; 7: Very comfortable]

4.3. Unlocking a Physical Space

4.3.1. Perceived Usefulness

Our participants mentioned about the usability issues associated with carrying a physical key while they reported interest in using FR as part of a smart lock system in their home; P92 added, 'I think that this is a great idea if it would only recognize the people living in the home. Especially when your hands are full and you don't have to fumble around for a key.' Some of the participants are willing to use FR in conjunction with a physical key to unlock their home, where P16 noted, 'It would help to protect your home if you lose your keys, where someone else couldn't use them to get into your house.'

4.3.2. Users' Concerns

Participants reported their discomfort with using FR to unlock their home for multiple reasons. Some participants consider their belongings at home quite valuable that they do not trust technology to protect their physical properties. For example, P64 mentioned, 'My home and my possessions are very important to me so I wouldn't want any type of technology to be able to unlock my door for anyone. I don't trust technology that much yet.' We also found, few

		Usefulness		Comfort Level	
FR is used...	**Comparison**	F/t-**value**	p-**value**	F/t-**value**	p-**value**
To unlock a laptop	with vs. **without** (entering a password)	2.3242	**0.0220**	0.2758	0.7833
To unlock a smartphone	with vs. **without** (entering a password)	2.6646	**0.0089**	0.4590	0.6472
To unlock a door	with vs. without (a physical lock and key)	0.3948	0.6938	0.0194	0.8896
For financial transactions at an ATM	ANOVA	1.3600	0.2611	0.1395	0.8699
	*with debit card vs. 4-digit PIN		0.3089		0.8999
	*with debit card vs. debit card & 4-digit PIN		0.3774		0.8619
	*with 4-digit PIN vs. debit card & 4-digit PIN		0.8999		0.8999
For financial transactions at a cash register	with vs. without (debit/credit card)	1.4851	0.2256	0.9923	0.3214
For app-based online payment	with vs. without (entering a password for the app)	0.0525	0.9582	0.2302	0.6323
For identification at a financial organization	with vs. without (ID card)	1.5200	0.1311	0.3977	0.6915
For identification at a non-financial organization	with vs. without (ID card)	0.0735	0.9414	1.6137	0.1096
For identification during in-store pickup	with vs. without (ID card)	1.8563	0.1758	0.6257	0.4306
To authenticate a loyalty member at a restaurant	with vs. without (loyalty card/password)	0.1695	0.6815	0.2711	0.6037
To offer personalized deals/service/advertisements (reason stated to the participant)	ANOVA	3.2612	**0.0408**	3.9444	**0.0212**
	*retail store vs. library		0.8999		0.0707
	*retail store vs. gas station		0.0952		0.8795
	***library** vs. gas station		0.0509		**0.0281**
To offer personalized deals/service/advertisements (reason is not stated to the participant)	ANOVA	12.1972	**0.000011**	2.3291	0.1005
	*retail store vs. library		0.1392		0.1756
	***retail store** vs. gas station		**0.0010**		0.8999
	***library** vs. gas station		**0.0082**		0.1332
For tracking people at a retail store	ANOVA	3.0963	**0.0495**	2.6694	0.0741
	*stated (informing about deals) vs. unstated		0.89999		0.6734
	*stated (law enforcement) vs. unstated		0.07302		0.0630
	*stated: informing about deals vs. law enforcement		0.10142		0.3276
For tracking people at a public gathering	**stated (law enforcement)** vs. unstated	2.1580	**0.0332**	1.9929	**0.0488**
For boarding a flight	with vs. without (boarding pass)	0.1788	1.9818	0.0013	0.9718

Table 3
The Results of Significance Tests (ANOVA or T-tests) [Notes: (i) For the ANOVA test, we reported adjusted p-value based on post-hoc Tukey test (marked with '*'); (ii) We bold the p-value where we found a significant difference ($p < 0.05$), where the bold text in 'Comparison' column represents the scenario with higher mean]

participants perceive FR as an advanced technology that is not needed for a regular home, as P160 noted: 'Unless I have a fortress what is the point [of using FR]?'

4.4. Financial Transactions

4.4.1. In-person / On-site Transactions

4.4.1.1 Perceived Usefulness

Participants reported their interest in using FR in combination with debit card at self-service ATM to gain security guarantee in case they loose physical access to their card. For example, P4 noted, 'I am comfortable with this use of facial recognition because I would feel more secure knowing that my account would be harder to break into if my card is lost or stolen.' On the other hand, some of our participants mentioned about the usability advantage of not carrying a credit/debit card if they use FR to make in-person payment at a cash register without the need of presenting/swiping their card.

Participants who are willing to use FR in conjunction with entering a PIN, noted higher security guarantee as the reason behind their choice, for instance, P88 mentioned, 'Two layers [PIN and FR] is better than one.' However, several participants would prefer to use FR instead of PIN during ATM transaction, because they would not have to worry about someone stealing their PIN. Being afraid of stealing, P105 regularly changes her PIN for debit card, which poses memorability challenges for her; she mentioned, 'It [PIN] is hard to remember because I change them on a regular basis.' Including P105, several participants reported it to be difficult to remember PIN for debit card and, thus, consider FR as a more usable and faster option for ATM transaction.

4.4.1.2 Users' Concerns

Some of our participants are satisfied with the usability and security of 4-digit PIN, and do not see a need to replace it with FR for ATM transaction; P175 further added, 'A PIN isn't hard to enter and seems more private.' Also, several participants are not comfortable yet to use FR as a replacement to presenting/swiping a physical card at register, with P284 remarking, 'It's a level of convenience that is not worth the security risk.'

4.4.2. Online Payment

4.4.2.1 Perceived Usefulness

Instead of entering the debit/credit card information to make an online payment, using FR through a smartphone app (linked to the user's financial account) was reported as seeming convenient to the participants, where P17 commented, 'The ease of access overrides any potential negative, I think.' In the scenario where FR is used instead of entering a password to log into that app, P216 mentioned, '[FR] eliminates the need for passwords and usernames, just scan your face and you are set [to make online payment], I much prefer this.'

4.4.2.2 Users' Concerns

Some of our participants were concerned that the increased ease in making online payments could lead to overspending or accidental spending. P93 worried that it would be difficult for her to dispute to financial organization if adversary gets access to her smartphone and fools the FR technology for making an online transaction. Several participants indicated a lack of trust in the overall security guarantee provided by smartphone apps, who were concerned that those apps would not securely store their biometric data; P201 further added, 'You can get a new credit card if it's stolen, you can't as easily get a new face if these images are stolen and used maliciously.' Here, P301 worried about third-party apps, who would be comfortable to use FR for online payment if the app is directly affiliated with her financial organization.

4.5. Identification at Customer Service

4.5.1. Perceived Usefulness

Participants are willing to use FR for identification at the customer desk in financial organizations (e.g., bank). Some of our participants consider FR as a more secure approach for identification than using physical identification card, like driving license. As they perceive, making a fake identification card is easier for an attacker than fooling a FR system. In this regard, several participants would prefer to use FR in combination with presenting an identification card (e.g., driving license) at the financial organization; P34 added, 'I think that it would be good for a bank to have this type of security measure [FR] so that they are able to make 100% sure who is having access to financial information.'

Some of our participants see benefits in using FR as they perceive it to be a faster method of identification as compared to showing an identification card at the service desk. A few participants believe that FR would also contribute to reducing human bias related to the demographic traits of customers. P270 remarked, 'It [FR] likely cuts down on human bias in which people who are not white or people who present as poorer, less mentally stable, etc., are demanded to show extra IDs or told they're lying.'

For identification of customers to pick up online-ordered items at the store, our participants find FR to be useful when the items are expensive. P96 mentioned, 'I do not feel that this is needed for something like a grocery purchase'. Several participants reported that they would be more comfortable if both FR and identification card are required for picking up expensive items at a retail store.

4.5.2. Users' Concerns

Participants reported concern about the risks of identity spoofing and privacy breach at non-financial organizations. For example, P248 commented, 'Right now, I can show my driver's license for proof of who I am, and it works. Adding in facial recognition is confusing because it's not necessary [at non-financial organization]. Just like the other scenarios, whoever has control of the system could somehow record my face and sell it to criminals or use it in some other way that could harm my privacy and security. I have no control over what they do with my face.' Also, a few of the participants expressed fears about their privacy when using FR for identification at a bank, but were willing to make the trade-off for better protection of their financial accounts. This was highlighted by P106, who noted, 'For financial activities, I am willing to give up some privacy for a security trade off.'

4.6. Personalized Service and Ads

4.6.1. Perceived Usefulness

We studied the perceptions of participants about the use of FR in providing them with personalized offers, services, or advertisements at different places, including retail stores, restaurants, libraries, and gas stations. When FR, placed at the checkout of a retail store, is used to keep records of customers' purchase behavior to inform them in the future about deals and offers on the items they generally buy, our participants reported that it would provide them with economic benefit and enhance their shopping experience. For example, P197 noted, 'This could help me to save money on items I frequently purchase'; P157 added, 'I think it is really convenient and could help improve my shopping experience by directing me to sales and items I may like.' P299 sees a benefit for retailer when FR is used to record customer's purchase behavior: 'This is similar to a small store owner noting my behavior or purchasing habits and using it to improve their business.'

Referring to the use of FR to authenticate a loyalty member in the restaurant, P145 noted, 'It would be a nice add-on to more personalized service, makes people feel somewhat special'. P93 added, 'I see a clear benefit of having my meal credited and my food choices immediately recognized.' A few of our participants mentioned about the usability benefit of using FR at a restaurant that they would not need to carry the loyalty card with them or recall the password of loyalty account to receive the membership benefits.

Most of the participants who consider FR to be useful for getting book recommendations in a library or to be shown targeted advertisements at a gas station based on their demographic traits, perceive this technology as a way of enhancing customer service. P53 reported comfort with FR showing demographics-based targeted ads during fueling at a gas station, where he also mentioned, 'It doesn't invade my privacy. Anyone else at the gas station can get the same information if they looked at me.'

4.6.2. Users' Concerns

Several participants reported concern that receiving deals and offers (e.g., through postal mail, mobile app, email, etc.) based on purchase behavior could be privacy invasive and affect their personal and social relationships. P71 commented, '...what if I want to buy a sex toy.' In these cases, participants want to have control over sharing information about their purchase behavior in a retail store.

P13 recalled a story to explain how information collection through FR could be privacy invasive for customers, 'I remember when Safeway was getting sued by a guy who fell on a slick floor. They used his points card that tracked his purchases to say he was an alcoholic based on his purchase behavior.' Several participants saw it as an invasion of privacy if FR data is collected without providing them with clear explanation. They reported wanting to know more about how their FR data would be used in process of providing them with the personalized offer, book recommendations, or targeted advertisements. For example, P93 mentioned, 'I would need to see how it affects me in a positive way before I would be happy just letting the system scan and record my image.'

Our results indicate that participants have a mental model of organizations and vendors using FR that influence their perceptions of the need of this technology in a certain scenario. P11 noted, 'This [FR in restaurant] seems unnecessary and I would only want important institutions to have this kind of access.' Also, some participants want to limit the use of technology, such as P287: 'Having this technology [FR] invade every part of one's life could be overwhelming. It would be nice to be able to enjoy a restaurant meal without having to be identified by some faceless AI or scanned like one would be at an airport or a hospital. In this scenario, I would prefer a good old-fashioned loyalty card system instead of a robotic records-keeper.'

Some participants reported their doubts about the efficacy of FR technology to recommend them the items of interest. P235, for instance, noted, 'It may result in the retailer making false assumptions about me and recommend items that do not pertain to me.' P68 reported being unsure if FR-based systems could choose books for her based on demographic traits: 'It wouldn't be bad necessarily, but I don't thing [sic] I'd follow the recommendations.' Similarly, P144 indicated that demographic profiling is not always accurate: 'Just because I'm a 30 something male doesn't mean I'll want advertisements on beer and cigarettes anyway.' Furthermore, participants are annoyed with the prevalence of advertisements in today's digital mediums, where they reported concern that FR would make the situation even worse for them; P110 expressed his perceptions, 'I would not want to have facial recognition used to show me ADS! That would make me very angry.'

When the reason of using FR is stated to the participants, we found differences between the locations where FR is deployed (retail store, library, gas station) in terms of their perceived usefulness ($F = 3.26$, $p < 0.05$) and comfort level ($F = 3.94$, $p < 0.05$). According to the post-hoc tests, participants are less comfortable with FR use in a gas station as compared to a library ($p < 0.05$, statistical power = 0.7, effect size = 0.5). We also found that participants' perceived usefulness ($F = 12.19$, $p < 0.001$) differ between the locations when the reason of using FR is not stated to them. Here, post-hoc tests show that participants found FR to be less useful in a gas station as compared to a retail store ($p < 0.01$, statistical power = 1.0, effect size = 0.9) and compared a library ($p < 0.01$, statistical power = 0.9, effect size = 0.6).

4.7. Tracking People

4.7.1. In Retail Stores: Perceived Usefulness and Users' Concerns

When we asked participants about their perceptions of using FR to track customers in a retail store to keeps records of the items they purchased and those they showed interest in but did not purchase (without explaining in the vignette how FR-data would be used by the retailer), participants reported concern that such tracking would hurt their shopping experience, for instance, P101 noted, 'I feel like shopping is an art and an exploration so I don't want some system messing around with that.'

As we explained in a separate vignette that FR-data would enable a retailer to let customers know about future deals on their items of interest (either purchased or not), several participants reported that FR technology would be useful in enhancing their shopping experience, where P95 commented, 'A store is free to use any conceivable data collection system on store premises to learn about customer preference; this is functionally no different than having an employee hired to perform the same sort of task.' P168 reported being comfortable in this case, as she considers tracking through FR in a retail store 'is less intrusive than most things these days.'

P286 expressed her opinion that FR should be used not only to track the customers but also the employees in a retail store, where she shared her past experience, 'I worked with loss prevention for a major department store for years and the majority of loss is from employee theft.' On the other hand, a few participants do not see the need of using FR to prevent shoplifting in a retail store, rather they believe that a visual alert sign would be enough to prevent such crime; P13 further added, 'I will never shop in a place like this [uses FR to track customers].'

In terms of perceived usefulness, we found differences ($F = 3.09$, $p < 0.05$) between three vignettes with different reasons for using FR: (i) no reason provided, (ii) to inform customers about targeted deals, and (iii) for law enforcement. Since the post-hoc test did not show significant differences between specific vignettes, however, the effect may be spurious or at best small.

4.7.2. At Public Gatherings: Perceived Usefulness and Users' Concerns

In the vignette where we did not explain how the FR-data would be used, participants reported discomfort of being tracked through FR in a public gathering, where they were unsure of how general people would be benefited in this case. For example, P6 mentioned, 'I do not see how this system would benefit the public relative to the amount of intrusiveness it contains.' A few participants considered tracking in a public space to be acceptable though, where P95 commented, 'When in public, there should be no expectation of privacy. Consequently, the use of computer vision to locate and track individuals in public is acceptable; it's functionally no different from being noticed and tracked by a human agent paid to serve the same purpose.' Also, participants mentioned about multiple attacks in the past including Boston bombing and referred to FR as an essential technology to prevent such incidents, where P138 noted, 'In public places and big events, something like this [FR] would be a must have to protect people.'

On the other hand, several participants reported concern about tracking through FR in a public space due to their lack of trust on the entities collecting their facial information, for instance, P60 mentioned, 'I don't really feel comfortable with large entities being able to track me...Why should I trust them to be able to track all people all the time?'; P129 further added, 'It feels like something out of a dystopian novel, too invasive.' In this regard, P303 considers the reward of physical safety to be higher than the risks of privacy invasion: 'Lets say, the user is abducted or gets in some type of problem. This technology [FR] will help law officers to know exactly what happened. This actually could save someone...Any invasion of privacy issues wouldn't bother me because the reward/risk ratio is way up in the positive ratings.'

As we explained in a vignette that FR-based tracking is used for law enforcement in public gatherings, participants found FR to be more useful ($t = 2.16$, $p < 0.05$, statistical power = 0.6, effect size = 0.4) and reported being more comfortable with such tracking (t = 1.99, $p < 0.05$, statistical power = 0.5, effect size = 0.4), as compared to a vignette where we did not state the reason behind FR-based tracking at public gatherings.

4.8. Boarding a Flight

4.8.1. Perceived Usefulness

Some of our participants consider FR to be useful for increasing the security at an airport. Additionally, some participants believe that boarding process would be faster if FR is used as a replacement to showing a boarding pass. For example, P111 noted, 'That is safety oriented and it speeds up the process, allowing the security people to focus on other things. I mean unless you're up to something...this feels like a win-win for everyone'. P35 added, 'I actually think this might be good since it would be hard for terrorists, for example, to foil this situation'. We found that a few participants are willing to use FR in combination with showing a boarding pass.

4.8.2. Users' Concerns

Several participants worried that the use of FR would complicate and delay the boarding process, where P86 mentioned, 'Having a boarding pass and ID has always been good enough in the past, and I see no reason why it shouldn't work instead of an overly complicated system like this [FR].' Several of them mentioned about their lack of trust on the overall system management at the airport where replacing or adding new mechanism, like FR might offer limited or no benefit at all; P95 added, 'Airport security is an incompetent kabuki production; any new security measures would only increase delays and decrease real security.'

4.9. Recording Attendance

4.9.1. Perceived Usefulness

Some of the participants perceive that if FR is used for recording class attendance it would reduce the burden of teachers and save time for lectures. Several participants consider FR as a better way for access control, allowing only registered students to attend a class, where a teacher might not know all of the students in a large classroom. P127 suggested that FR is also beneficial to the students, as it would help a student to prove her past attendance in case she is accused of being absent.

4.9.2. Users' Concerns

Some participants reported concern that using FR to record attendance would have negative impact on their grade. P287 added, 'Perhaps I'm not going to be in class, but I've made arrangements to be responsible for the material; the facial recognition wouldn't know that. It would only know that I'm not there, and that may not be helpful.' A few participants worried that recording attendance through FR might hurt their overall experience in a class. P63 mentioned, 'It seems obtrusive as well as devaluing of the student/teacher experience.'

5. Discussion

In this section, we examine users' perceptions of FR through the lens of privacy concepts and theories (Posner, 1981; Bloustein, 1964; Rachels, 2017; Thomson, 1975; Moore, 1998, 2003, 2000, 2010, 2015). Based on our findings, we provide a visual representation of users' concerns about FR adoption (see Figure 3). We conclude this section with describing the limitations of our study and scope for future work.

5.1. A Closer Look into Users' Perceptions

5.1.1. Dignity, Autonomy, and Independence

Blousetin (1964) describes privacy as having aspects of individual dignity, integrity, and personal autonomy and independence. Our findings support this perspective in multiple instances. For example, participants demanded the ability to compartmentalize their personal information, where they reported concern about the exposure of purchase behavior that could hurt their social image with respect to dignity and integrity. Even when FR is not connected to users' personal account or information, but is in place to offer personalized service based on their demographic traits, participants demanded to know the reasons and benefits of using FR before their face is scanned.

Personal autonomy and independence are important to our participants. They reported comfort with the scenarios where FR information is stored in their personal devices, which gives them a sense of control over their sensitive data. Further, they want to preserve the independence of placing a border for technology use in everyday life, where they do not prefer to be identified or tracked by any entities in the wild without their consent. Some of them are even

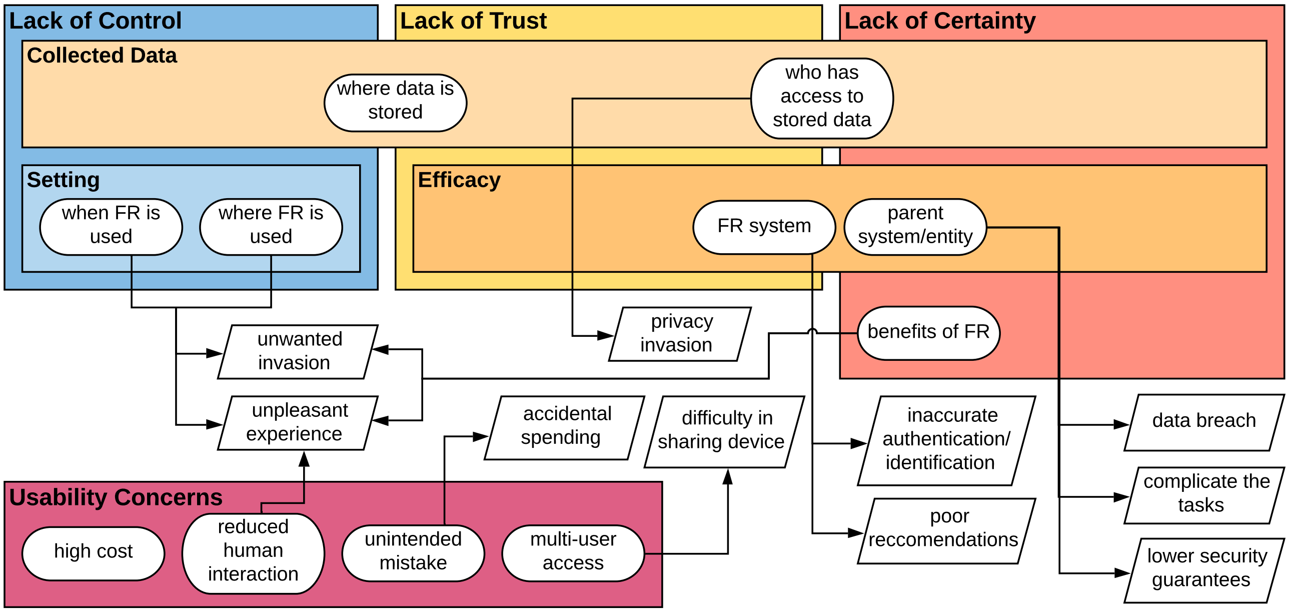

Figure 3: Concerns about FR Adoption [Entities within the boxes represent what the participants are concerned about. Entities outside the boxes represent why participants are concerned about the entities within the boxes.]

concerned that the identification and tracking through FR might degrade the pleasure of experiences such as shopping or having dinner with family.

5.1.2. Control and Trust

Participants want to control access to their personal data since leaked information might lead to misjudgement by the society, which is in line with Rachels' (2017) argument on privacy stating the importance of preserving individual's private information to maintain and control social relationship with others. Rachels' analysis also shed light on the importance of protecting one against the deleterious consequences of information leaks (Rachels, 2017). Participants reported their lack of control and trust in FR-based authentication, where they are afraid that such technology would mistakenly authenticate adversaries allowing them access to valuable information and belongings. This lack of trust on efficacy is also one of the reasons why participants see a limited benefit in using FR to get personalized offers.

FR poses further concerns, as it deals with sensitive biometric information, where participants are unsure how of their data would be used and if third-party entities would have access to their facial information. Thus, they are worried about tracking in public gathering, especially in cases where they are not familiar with the entities collecting their information.

Participants' sense of control and trust are influenced by their mental model of the entities storing their FR information. Financial organizations seem more reliable to participants, which helps explain their reported comfort with using FR at a financial organization or during an ATM transaction. Although participants have concerns about the privacy policy of smartphone apps, knowing that an app using FR is affiliated with a financial organization contributes to their comfort with using this technology.

5.1.3. Protecting One's Private Sphere

As we look into users' perceptions through the lens of Thomson's Reductionism (1975), where privacy is defined as the right to secure one's physical property, we identified a lack of trust in technology for protecting privacy. Here, participants consider the present reality to discern whether FR introduces any further privacy risks than what they are already exposed to. For example, with the use of FR in smart lock at home, participants reported concern about technology malfunction allowing unauthorized access to their private space, which could lead to property loss or incur physical danger to their family members.

5.1.4. Usability Factors

We identified instances where the perceptions of usability gain (e.g., easier and faster identification, authentication, or transaction) positively influenced participants' view towards adopting FR in place of existing mechanisms that use passwords, physical cards (e.g, identification card, debit/credit card), or keys. In cases where participants are concerned about the security of an existing system but are satisfied with its usability (e.g., 4-digit PIN), they prefer to combine it with FR for two-factor authentication.

Some participants looked at the usability of FR from a different point of view, worrying that using FR would make an online payment so simple and fast that it might lead to accidental spending. Participants also reported concerns about the flexibility of multi-user access to shared devices, since FR does not allow users to share their authentication secret. Also, FR-based systems might fail to consider exceptional situations that could be only resolved through offline communication and mutual understanding; for this reason, participants are hesitant about adopting FR to record class attendance.

5.1.5. Individual Privacy vs. Public Safety

According to Moore (1998; 2003; 2000), individual privacy often needs to be sacrificed for the greater good, such as for public safety. This argument is in line with Himma's argument on social contract theory, which states that being a part of a society, the citizen must submit to the state for national security (Moore, 2010, 2015). The participants understand the importance of physical safety, where they referred to a series of past incidents of bombings and physical harm in public gatherings or on airplanes. These past events influenced participants' opinion to adopt FR for tracking in public space or identifying passengers during boarding a flight to provide for more safety and security. However, poor experiences with airport security made several participants skeptical about gaining significant safety and security benefits from FR.

5.1.6. Privacy Preferences vs. Business Opportunities

From an economic perspective, Posner (1981) argues that privacy should be protected only when the access to information would reduce its value. He suggests that individual privacy is less of a concern, since it is not related to economic advancement. Our findings indicate, however, that the failure to conform with privacy preferences could lead retailers to lose their customers. On the other hand, using FR to provide targeted offers to customers could help companies get more sales. Here, participants prefer to maintain a degree of anonymity when exposed to FR. For example, keeping personal account information separated from FR-based tracking in a retail store helps users feel more comfortable with adopting this technology. Thus, retailers should provide their customers with the choice of whether they want to connect the tracking data to their online account. Our findings suggest that this would contribute to their customers' feeling of privacy and satisfaction with the use of FR. In addition, businesses should be careful about the extent of FR use, where the annoyance with the prevalence of digital advertisements negatively affected our participants' interest in FR-based targeted ads.

5.2. Limitations and Future Work

In this paper, we focused on camera-based facial recognition in the physical world. Facial recognition is also used in online platforms, such as for auto-tagging the people in a photo uploaded to a social networking site (Stone, Zickler and Darrell, 2008; Michelson and Ortiz, 2006). It would be an interesting avenue for future research to investigate users' perceptions of automated facial recognition in these settings.

In security and privacy studies, the responses from MTurk and the general population in U.S. are quite similar for respondents who are younger than 50 or who have some college education (Redmiles et al., 2019). All of our participants are from the United States, where 80% of them were younger than 50, and more than 85% of our participants at least have attended some college. We believe that our findings provide valuable insights into the perceptions of the U.S. population, especially for adults between 18 and 50 years old who have attended college. We encourage future studies to examine the perceptions of older and less educated Americans. We did not capture many variables that could impact users' privacy awareness, like their socio-economic status (Redmiles, Kross and Mazurek, 2016), where adults with higher income are more likely to have heard about government surveillance, and thus, are more likely to have concerns about privacy (Rainie, 2016). This means, some of our results likely do not generalize to all people around the world, and the variables that we did not consider could affect our findings. We plan to extend the findings from this study in our future work through recruiting participants from different countries in the world, to gain insights into the impacts of culture, social norms, socio-econmic status, and geographic location on FR adoption.

Given the non-random selection of our research participants, there may have been some self-selection bias. Also, we cannot rule out the possibility of some amount of gaming the MTurk system. That said, we are reassured by prior work that finds MTurk participants to be ethical and have a strong commitment to accurate self-reporting (Mason and Suri, 2012; Shapiro, Chandler and Mueller, 2013). Nevertheless, a valuable avenue for future work involves following up on our survey with in-depth qualitative interviews and field studies.

There are surely additional uses of FR outside of the 35 scenarios considered in this study, and new scenarios will emerge over time. This survey was conducted at a specific moment in time, and users' perceptions and behaviors are ever evolving. Perceptions of FR will likely shift with changes in technology, privacy and security policies, and major news stories about FR. Thus, building on this first look into users' perceptions of FR, future studies would be able to capture the changes in their perceptions with respect to time and events.

6. Conclusion

FR is becoming a part of our everyday life, where the landscape of public discussion and views of privacy are undergoing a stage of evolution. Few U.S. states have started to look into the scopes of building a legislation to regulate its use (Daniels, 2019; King, 2019), where several tech organizations are in the process of developing their own regulations for FR use (Del Rey, 2019; Ghaffary, 2019; Browne, 2019). Therefore, it is paramount to understand the perceptions of users with regard to adopting this technology. We reported users' perceived usefulness and comfort with FR in different scenarios of everyday life, where our analysis looked into the underlying concerns of participants. We identified that users' perceptions of FR vary across the contexts of use, where they considered a wide-range of factors to weigh the benefits of FR use with the corresponding privacy risks. They have a clear say about the contexts where they are willing to use FR or not, which should be carefully considered by the government agencies and business entities while building a legislation or making a decision to expand or regulate the use of FR. Our findings indicate that users who do not find a clear benefit of using FR in a scenario might consider this technology as an invasion of privacy. So, users' consent should be taken when they are exposed to FR [3], where informing them about the benefits of using FR in the given context would make them comfortable to adopt the technology.

7. Acknowledgement

We would like to thank the reviewers for their valuable feedback. This material is based upon work supported by the National Science Foundation under Awards No. CNS-1949699 and CNS-1949694.

References

Anast Seguin, C., Ambrosio, A.L., 2002. Multicultural vignettes for teacher preparation. Multicultural Perspectives 4, 10–16.

Association, P., 2013. Tesco's plan to tailor adverts via facial recognition stokes privacy fears. The Guardian URL: https://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces.

Ayalon, O., Toch, E., 2019. Evaluating users' perceptions about a system's privacy: differentiating social and institutional aspects, in: Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS '19), USENIX Association, Santa Clara, CA. URL: https://www.usenix.org/conference/soups2019/presentation/ayalon.

Ballantyne, M., Boyer, R.S., Hines, L., 1996. Woody bledsoe: His life and legacy. AI magazine 17, 7.

Baraniuk, C., 2019. Biostar security software 'leaked a million fingerprints'. BBC URL: https://www.bbc.com/news/technology-49343774.

Barter, C., Renold, E., 2000. 'i wanna tell you a story': exploring the application of vignettes in qualitative research with children and young people. International journal of social research methodology 3, 307–323.

Bates, D., 2017. Face recognition technology set to transform retail. Forbes URL: https://www.forbes.com/sites/sap/2017/11/08/face-recognition-technology-set-to-transform-retail/.

Bloustein, E.J., 1964. Privacy as an aspect of human dignity: An answer to dean prosser. New York University Law Review 39, 962.

Blythe, J.M., Coventry, L., Little, L., 2015. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors, in: Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15), pp. 103–122.

Bowyer, K.W., 2004. Face recognition technology: security versus privacy. IEEE Technology and Society Magazine 23, 9–19. doi:10.1109/MTAS.2004.1273467.

Boyatzis, R.E., 1998. Transforming qualitative information: Thematic analysis and code development. SAGE Publications, Thousand Oaks, CA.

Brant, T., 2017. China battles toilet paper thieves with facial recognition. Entrepreneur URL: https://www.entrepreneur.com/article/290978.

[3] Users' privacy consent could be taken in different ways based on the contexts of technology use (Schaub, Balebako, Durity and Cranor, 2015).

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology 3, 77–101. URL: https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa, doi:10.1191/1478088706qp063oa.

Browne, R., 2019. Microsoft CEO says facial recognition technology needs to be regulated. CNBC URL: https://www.cnbc.com/2019/01/24/davos-microsofts-nadella-says-facial-recognition-needs-regulation.html.

Buolamwini, J., Gebru, T., 2018. Gender shades: Intersectional accuracy disparities in commercial gender classification, in: Proceedings of the First Conference on Fairness, Accountability and Transparency (FAccT '18), PMLR, New York, NY, USA. pp. 77–91. URL: http://proceedings.mlr.press/v81/buolamwini18a.html.

Castro, D., 2019. Americans support musicians like Taylor Swift using facial recognition to spot stalkers at concerts. Center for Data Innovation URL: https://www.datainnovation.org/2019/01/americans-support-musicians-like-taylor-swift-using-facial-recognition-to-spot-stalkers-at-concerts/.

Castro, D., McLaughlin, M., 2019. Survey: Few Americans want government to limit use of facial recognition technology, particularly for public safety or airport screening. Center for Data Innovation URL: https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/.

Chmielewski, D., 2015. Apple to use selfies to unlock phones? Vox URL: https://www.vox.com/2015/3/31/11560978/apple-to-use-selfies-to-unlock-phones.

Daniels, J., 2019. California Senate considers ban on facial recognition software for police body cams. CNBC URL: https://www.cnbc.com/2019/05/21/calif-senate-to-consider-facial-recognition-ban-on-police-body-cams.html.

Davis West, J., 2017. History of face recognition & facial recognition software. FaceFirst Face Recognition Software URL: https://www.facefirst.com/blog/brief-history-of-face-recognition-software/.

Davis West, J., 2018. Survey: Americans favor face recognition to prevent retail crime. FaceFirst Face Recognition Software URL: https://www.facefirst.com/blog/new-survey-finds-americans-favor-face-recognition-combat-rising-retail-theft-violence/.

Davis West, J., 2019. 5 ways face recognition can transform customer loyalty. FaceFirst Face Recognition Software URL: https://www.facefirst.com/blog/ways-face-recognition-can-transform-customer-loyalty/.

Del Rey, J., 2019. Amazon is creating facial recognition regulations that it wants Congress to adopt. Vox URL: https://www.vox.com/recode/2019/9/25/20884427/jeff-bezos-amazon-facial-recognition-draft-legislation-regulation-rekognition.

Doffman, Z., 2019. Hong Kong exposes both sides Of China's relentless facial recognition machine. Forbes URL: https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/.

Dupuis, M., Endicott-Popovsky, B., Crossler, R., 2013. An analysis of the use of amazon's mechanical turk for survey research in the cloud, in: Proceedings of the International Conference on Cloud Security Management (ICCSM '13), Academic Conferences Limited. p. 10.

Finch, J., 1987. The vignette technique in survey research. Sociology 21, 105–114.

Finnegan, M., Kapo, M., 2018. What is Windows Hello? Microsoft's biometrics security system explained. Computerworld URL: https://www.computerworld.com/article/3244347/what-is-windows-hello-microsofts-biometrics-security-system-explained.html.

France-Presse, A., 2019. Smile-to-pay: Chinese shoppers turn to facial payment technology. The Guardian URL: https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology.

Funk, C., Rainie, L., 2015. Public and scientists' views on science and society. Pew Research Center Science & Society URL: http://www.pewinternet.org/2015/01/29/public-and-scientists-views-on-science-and-society/.

Gates, K., 2004. The past perfect promise of facial recognition technology. ACDIS Occasional Paper .

Ghaffary, S., 2019. Amazon is trying to regulate itself over facial recognition software — before Congress does. Vox URL: https://www.vox.com/technology/2019/2/7/18216125/amazon-regulation-facial-recognition-software.

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L.F., Agarwal, Y., 2016. How short is too short? implications of length and framing on the effectiveness of privacy notices, in: Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS '16), USENIX Association, Denver, CO. pp. 321–340. URL: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck.

Goldstein, A.J., Harmon, L.D., Lesk, A.B., 1971. Identification of human faces. Proceedings of the IEEE 59, 748–760.

Goldstein, A.J., Harmon, L.D., Lesk, A.B., 1972. Man-machine interaction in human-face identification. Bell System Technical Journal 51, 399–427.

Habib, H., Naeini, P.E., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N., Cranor, L.F., 2018. User behaviors and attitudes under password expiration policies, in: Fourteenth Symposium on Usable Privacy and Security (ˆSOUPS‘ 2018), pp. 13–30.

Institute, A.L., 2019. Beyond face value: public attitudes to facial recognition technology. Ada Lovelace Institute URL: https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/.

Ipeirotis, P.G., 2010. Analyzing the amazon mechanical turk marketplace. XRDS: Crossroads, The ACM Magazine for Students 17, 16–21.

Jain, A.K., Nandakumar, K., Nagar, A., 2008. Biometric template security. EURASIP J. Adv. Signal Process 2008. URL: https://doi-org.ezproxy.rit.edu/10.1155/2008/579416, doi:10.1155/2008/579416.

Jain, A.K., Ross, A., Uludag, U., 2005. Biometric template security: Challenges and solutions, in: 2005 13th European signal processing conference, IEEE. pp. 1–4.

Kan, M., 2015. Alibaba uses facial recognition tech for online payments. Computerworld URL: https://www.computerworld.com/article/2897117/alibaba-uses-facial-recognition-tech-for-online-payments.html.

Kang, R., Brown, S., Dabbish, L., Kielser, S.B., 2014. Privacy attitudes of mechanical turk workers and the us public., in: Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS '14), pp. 37–49.

Kang, R., Dabbish, L., Fruchter, N., Kiesler, S., 2015. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security, in: Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15), pp. 39–52.

Kapelner, A., Chandler, D., 2010. Preventing satisficing in online surveys, in: Proceedings of CrowdConf.

Karantzoulidis, S., 2019. This smart lock has a built-in facial recognition camera. Security Sales & Integration URL: https://www.securitysales.com/news/smart-lock-facial-recognition-camera/.

Keeter, S., Christian, L., 2012. A comparison of results from surveys by the pew research center and google consumer surveys. Pew Research Center for the People and the Press URL: http://www.people-press.org/2012/11/07/a-comparison-of-results-from-surveys-by-the-pew-research-center-and-google-consumer-surveys/.

Kelley, P.G., 2010. Conducting usable privacy & security studies with amazon's mechanical turk, in: Proceedings of the Fifth Symposium on Usable Privacy and Security (SOUPS '10).

King, K., 2019. New York City lawmakers look to regulate facial-recognition tools. Wall Street Journal URL: https://www.wsj.com/articles/new-york-city-lawmakers-look-to-regulate-facial-recognition-tools-11570485799.

Knight, W., 2017. In China, you can pay for goods just by showing your face. MIT Technology Review URL: https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/.

Kung, F.Y., Kwok, N., Brown, D.J., 2018. Are attention check questions a threat to scale validity? Applied Psychology 67, 264–283. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/apps.12108, doi:10.1111/apps.12108, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/apps.12108.

Kwan, C., 2019. NEC and E.Sun create ATM with facial recognition. ZDNet URL: https://www.zdnet.com/article/nec-and-e-sun-create-atm-with-facial-recognition/.

Lu, C., Tang, X., 2015. Surpassing human-level face verification performance on lfw with gaussianface. Proceedings of the 29th Conference on Artificial Intelligence (AAAI '15) .

Madden, M., Rainie, L., 2015. Americans' attitudes about privacy, security and surveillance. Pew Research Center: Internet, Science & Tech URL: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. Information systems research 15, 336–355.

Martin, K., Nissenbaum, H., 2016. Measuring privacy: an empirical test using context to expose confounding variables. Colum. Sci. & Tech. L. Rev. 18, 176.

Martin, K.E., 2012. Diminished or just different? a factorial vignette study of privacy as a social contract. Journal of Business Ethics 111, 519–539.

Mason, W., Suri, S., 2012. Conducting behavioral research on amazon's mechanical turk. Behavior Research Methods 44, 1–23.

Materese, R., 2018. NIST evaluation shows advance in face recognition software's capabilities. NIST URL: https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

McCullagh, D., 2001. Call it super bowl face scan i URL: https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/.

Mehmood, R., Selwal, A., 2020. Fingerprint biometric template security schemes: Attacks and countermeasures, in: Singh, P.K., Kar, A.K., Singh, Y., Kolekar, M.H., Tanwar, S. (Eds.), Proceedings of ICRIC 2019, Springer International Publishing, Cham. pp. 455–467.

Mejia, N., 2019. Facial recognition in banking - current applications. Emerj URL: https://emerj.com/ai-sector-overviews/facial-recognition-in-banking-current-applications/.

Michelson, J., Ortiz, J., 2006. Auto-tagging the facebook .

Moore, A.D., 1998. Intangible property: privacy, power, and information control. American Philosophical Quarterly 35.

Moore, A.D., 2000. Employee monitoring and computer technology: Evaluative surveillance v. privacy. Business Ethics Quarterly 10, 697–709.

Moore, A.D., 2003. Privacy: Its meaning and value. American Philosophical Quarterly 40, 215–227.

Moore, A.D., 2010. Privacy rights: Moral and legal foundations. Penn State Press.

Moore, A.D., 2015. Privacy, security and accountability: ethics, law and policy. Rowman & Littlefield International Ltd, London, United Kingdom.

Mortensen, K., Hughes, T., 2018. Comparing amazon's mechanical turk platform to conventional data collection methods in the health and medical research literature. Journal of General Internal Medicine 33. doi:10.1007/s11606-017-4246-0.

Mozur, P., 2019. In Hong Kong protests, faces become weapons. The New York Times URL: https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N., 2017. Privacy expectations and preferences in an iot world, in: Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS '17), pp. 399–412.

Nandakumar, K., Jain, A.K., 2015. Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine 32, 88–100.

NIST, 2017. Face recognition technology (feret) URL: https://www.nist.gov/programs-projects/face-recognition-technology-feret.

Normalini, M., Ramayah, T., et al., 2017. Trust in internet banking in malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security. Journal of Management Sciences 4, 3–26.

Oliver, D., 2019. Facial recognition scanners are already at some US airports. Here's what to know. USA TODAY URL: https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/.

Oppenheimer, D.M., Meyvis, T., Davidenko, N., 2009. Instructional manipulation checks: Detecting satisficing to increase statistical power. Journal of Experimental Social Psychology 45, 867–872.

Paolacci, G., Chandler, J., Ipeirotis, P.G., 2010. Running experiments on amazon mechanical turk. Judgment and Decision making 5, 411–419.

Pearson, B., 2018. 3 ways retailers can use facial recognition to create better experiences. Forbes URL: https://www.forbes.com/sites/bryanpearson/2018/03/15/3-ways-retailers-can-use-facial-recognition-to-express-better-experiences/.

Peer, E., Vosgerau, J., Acquisti, A., 2014. Reputation as a sufficient condition for data quality on amazon mechanical turk. Behavior Research Methods 46, 1023–1031.

Peter, K.J., Glory, G.G.S., Arguman, S., Nagarajan, G., Devi, V.V.S., Kannan, K.S., 2011. Improving atm security via face recognition, in: The

Proceedings of the Third International Conference on Electronics Computer Technology (ICECT '11), pp. 373–376. doi:10.1109/ICECTECH.2011.5942118.

Petroff, A., 2016. MasterCard launching selfie payments. CNNMoney URL: https://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/index.html.

Phillips, P.J., Yates, A.N., Hu, Y., Hahn, C.A., Noyes, E., Jackson, K., Cavazos, J.G., Jeckeln, G., Ranjan, R., Sankaranarayanan, S., Chen, J.C., Castillo, C.D., Chellappa, R., White, D., O'Toole, A.J., 2018. Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. Proceedings of the National Academy of Sciences 115, 6171–6176. URL: https://www.pnas.org/content/115/24/6171, doi:10.1073/pnas.1721355115, arXiv:https://www.pnas.org/content/115/24/6171.full.pdf.

Posner, R.A., 1981. The economics of privacy. The American Economic Review 71, 405–409. URL: http://www.jstor.org/stable/1815754.

Prabhakar, S., Pankanti, S., Jain, A.K., 2003. Biometric recognition: Security and privacy concerns. IEEE Symposium on Security and Privacy (S&P 2019) 1, 33–42. URL: https://doi.org/10.1109/MSECP.2003.1193209.

Rachels, J., 2017. Why privacy is important. Privacy , 11–21.

Rainie, L., 2016. The state of privacy in post-snowden america. Pew Research Center URL: http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

Rao, A., Schaub, F., Sadeh, N., Acquisti, A., Kang, R., 2016. Expecting the unexpected: Understanding mismatched privacy expectations online, in: Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS '16), pp. 77–96.

Redmiles, E.M., Kross, S., Mazurek, M.L., 2016. How i learned to be secure: A census-representative survey of security advice sources and behavior, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '16), ACM, New York, NY, USA. pp. 666–677. URL: http://doi.acm.org/10.1145/2976749.2978307, doi:10.1145/2976749.2978307.

Redmiles, E.M., Kross, S., Mazurek, M.L., 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples, in: IEEE Symposium on Security and Privacy (S&P '19), pp. 227–244.

Rogers, K., 2016. That time the super bowl secretly used facial recognition software on fans URL: https://www.vice.com/en_us/article/kb78de/that-time-the-super-bowl-secretly-used-facial-recognition-software-on-fans.

Romero, M., 2019. Portland gas station using facial recognition technology to curb crime. KGW URL: https://www.kgw.com/article/news/local/portland-gas-station-using-facial-recognition-technology-to-curb-crime/283-8ce9f30a-2ac8-4c07-9ea9-11518a75e40a.

Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F., 2015. A design space for effective privacy notices, in: Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15), pp. 1–17.

Seng, S., Kocabas, H., Al-Ameen, M.N., Wright, M., 2019. Poster: Understanding user's decision to interact with potential phishing posts on facebook using a vignette study, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '19), ACM. pp. 2617–2619.

Shapiro, D., Chandler, J., Mueller, P.A., 2013. Using mechanical turk to study clinical populations. Clinical Psychological Science , 213–220.

Singer, N., 2019. Amazon faces investor pressure over facial recognition. The New York Times URL: https://www.nytimes.com/2019/05/20/technology/amazon-facial-recognition.html.

Smith, A., 2019. More than falf of U.S. adults trust law enforcement to use facial recognition responsibly. Pew Research Center: Internet, Science & Tech URL: https://www.pewinternet.org/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

Stone, Z., Zickler, T., Darrell, T., 2008. Autotagging facebook: Social network context improves photo annotation, in: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, IEEE. pp. 1–8.

Tan, J., Bauer, L., Christin, N., Cranor, L.F., 2020. Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements, in: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 1407–1426.

Tengyuen, N., 2017. 3 webcam face recognition security software and bio-metrics password manager. GeckoandFly URL: https://www.geckoandfly.com/4068/webcam-face-recognition-security-software-and-password-manager-program/.

Thomson, J.J., 1975. The right to privacy. Philosophy & Public Affairs , 295–314.

Toor, A., 2017. This French school is using facial recognition to find out when students aren't paying attention. The Verge URL: https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france.

Turk, M., Pentland, A., 1991a. Eigenfaces for recognition. Journal of cognitive neuroscience 3, 71–86.

Turk, M.A., Pentland, A.P., 1991b. Face recognition using eigenfaces, in: Proceedings of the Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '91), IEEE. pp. 586–591.

Union, A.C.L., 2001. Use of facial recognition at Super Bowl and in Tampa. American Civil Liberties Union URL: https://www.aclu.org/other/use-facial-recognition-super-bowl-and-tampa.

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., 2016. Do users' perceptions of password security match reality?, in: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 3748–3760.

Venkatraman, S., Delpachitra, I., 2008. Biometrics in banking security: a case study. Information Management & Computer Security 16, 415–430. URL: https://doi.org/10.1108/09685220810908813.

Wallace, G., 2018. Instead of the boarding pass, bring your smile to the airport. CNN Travel URL: https://www.cnn.com/travel/article/cbp-facial-recognition/index.html.

Wang, J., 2018. You can now check in with a facial scan at Marriott in China. Forbes URL: https://www.forbes.com/sites/jennawang/2018/07/24/you-can-now-check-in-with-a-facial-scan-at-marriott/.

Wolfe-Robinson, M., 2019. Manchester City warned against using facial recognition on fans. The Guardian URL: https://www.theguardian.com/technology/2019/aug/18/manchester-city-face-calls-to-reconsider-facial-recognition-tech.

Wollerton, M., 2019. Elecpro's smart lock scans faces to let people in. CNET URL: `https://www.cnet.com/news/elecpros-smart-lock-scans-faces-to-let-people-in-ces-2019/`.

Zhang, Y., Chen, Z., Xue, H., Wei, T., 2015. Fingerprints on mobile devices: Abusing and leaking, in: Black Hat Conference.

Zimmermann, V., Gerber, N., 2017. ”if it wasn't secure, they would not use it in the movies” – security perceptions and user acceptance of authentication technologies, in: Tryfonas, T. (Ed.), Human Aspects of Information Security, Privacy and Trust, Springer International Publishing, Cham. pp. 265–283.

Appendix

See next page.

Privacy Concepts and Tools	Median	Mean	Standard Deviation
Privacy settings	5.00	4.44	0.6863
Incognito mode/private browsing mode in browsers	4.00	4.35	0.6425
Browser Cookie	4.00	4.33	0.7868
IP address	4.00	4.31	0.8816
Encryption	4.00	3.78	1.0071
Virtual Private Network (VPN)	4.00	3.74	1.2537
Proxy server	4.00	3.60	1.4216
Secure Sockets Layer (SSL)	3.00	3.00	1.0591
Tor	3.00	2.74	0.6227

Table 4
Users' Response [1: Strongly Disagree; 5: Strongly Agree] to Likert-scale Questions about Familiarity with Privacy Concepts and Tools Kang et al. (2015); Rao et al. (2016)

Privacy Statement	Median	Mean	Standard Deviation
Companies seeking information online should disclose the way the data are collected, processed, and used.	7.00	6.57	1.0572
A good consumer online privacy policy should have a clear and conspicuous disclosure.	7.00	6.56	1.0649
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	6.00	6.18	1.2276
Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	6.00	6.06	0.9201
Consumer control of personal information lies at the heart of consumer privacy.	6.00	6.06	0.8487
I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	6.00	6.03	0.9888
When online companies ask me for personal information, I sometimes think twice before providing it.	6.00	5.97	1.3727
I'm concerned that online companies are collecting too much personal information about me.	6.00	5.78	1.0840
It bothers me to give personal information to so many online companies.	6.00	5.72	1.3170
It usually bothers me when online companies ask me for personal information.	6.00	5.45	1.3237

Table 5
Users' Response [1: Strongly Disagree; 7: Strongly Agree] to IUIPC Online Privacy Concern Scale Malhotra et al. (2004)

Context	Setting	Scenario	Percentage of Participants
Unlocking Personal Devices	Laptop	A	23.08%
		B	27.59%
	Smartphone	A	28.85%
		B	36.36%
Unlocking a Physical Space	Smart Lock	A	14.29%
		B	10.91%
Financial Transaction	ATM	A	17.50%
		B	18.18%
		C	25.00%
	Cash Register	A	18.52%
		B	10.34%
	Online	A	36.54%
		B	35.59%
Identification at Customer Service	Finance	A	25.00%
		B	20.34%
	Non-Finance	A	21.25%
		B	16.67%
	In-store Pickup	A	12.07%
		B	16.36%
Personalized Service and Ads	Retail Checkout	A	10.53%
		B	20.00%
	Restaurant	A	6.67%
		B	16.36%
	Library	A	20.69%
		B	8.77%
	Gas Station	A	30.36%
		B	23.53%
Tracking People	Retail	A	14.71%
		B	29.63%
		C	30.56%
	Public	A	29.63%
		B	50.00%
Boarding	Flight	A	22.22%
		B	20.97%
Recording Attendance	Classroom	-	8.93%

Table 6
Real-Life Experience of Encountering a Scenario Presented in the Vignette. [For each vignette, the percentage of participants is calculated through dividing the number of participants who reported to encounter that scenario in real life by the number of participants who were presented with that vignette in the study]

Context	Setting	Scenario	Comfort Level (Did not Encounter)	Comfort Level (Encountered)	Usefulness (Did not Encounter)	Usefulness (Encountered)
Unlocking Personal Devices	Laptop	A	4.8	4.5	5.3	5.5
		B	4.2	5.8	4.0	5.7
	Smartphone	A	4.3	6.5	5.3	6.6
		B	4.4	5.5	4.1	5.7
Unlocking a Physical Space	Smart Lock	A	4.0	4.6	4.8	5.4
		B	4.2	3.7	4.8	3.8
Financial Transaction	ATM	A	4.0	5.4	4.3	5.6
		B	4.4	4.7	5.3	4.8
		C	4.1	5.6	4.9	5.8
	Cash Register	A	2.8	5.0	4.2	6.0
		B	3.4	4.8	3.9	4.7
	Online	A	3.3	4.8	4.2	5.6
		B	3.3	5.6	3.9	6.3
Identification at Customer Service	Finance	A	3.9	5.6	4.9	5.8
		B	4.3	5.3	4.3	5.7
	Non-Finance	A	3.3	3.9	3.7	4.3
		B	4.0	4.4	3.7	4.2
	In-store Pickup	A	3.2	4.1	4.1	5.0
		B	3.5	4.1	3.6	4.0
Personalized Service and Ads	Retail Checkout	A	2.7	4.7	3.4	5.3
		B	2.5	3.6	3.0	3.8
	Restaurant	A	3.2	4.7	3.5	5.0
		B	3.5	4.0	3.3	4.2
	Library	A	3.3	4.4	2.8	3.6
		B	3.3	5.6	2.9	6.4
	Gas Station	A	2.6	3.4	1.8	2.6
		B	2.3	3.3	2.1	3.2
Tracking People	Retail	A	1.7	3.3	3.2	3.6
		B	2.2	4.8	3.1	4.4
		C	3.0	4.0	4.1	4.9
	Public	A	2.4	3.4	3.5	4.1
		B	3.2	3.9	4.0	5.0
Boarding	Flight	A	4.4	4.9	4.9	4.8
		B	4.3	5.2	4.7	5.7
Recording Attendance	Classroom	-	3.9	4.2	4.1	4.3

Table 7
Average Comfort Level and Perceived Usefulness of Participants Based on Whether They *Encountered* or *Did not Encounter* a Scenario (Presented in the Vignette) in Real Life

Context	Setting	Scenario	Description
Unlocking Personal Devices	Laptop	A	Only FR is used for authentication.
		B	FR, in conjunction with traditional password, is used for authentication.
	Smartphone	A	Only FR is used for authentication
		B	You FR, in conjunction with traditional PIN/pattern lock, is used for authentication.
Unlocking a Physical Space	Smart Lock	A	Only FR is used.
		B	You live in a home, which has a smart lock system at the entrance. In addition to using a traditional physical key, the lock system also needs to successfully recognize your face in order to let you enter the house. With the permission of a master user (e.g., head of the house), the lock-system can include additional authorized users (e.g., family members) and let them enter the house after successfully recognizing their face, and having them use the physical key.
Financial Transaction	ATM	A	You are at a self-service ATM machine to make financial transaction. After you insert your debit card, the ATM uses facial recognition (linked to your account) to authenticate you instead of requiring you to enter a 4-digit PIN.
		B	You are at a self-service ATM to make financial transaction. Instead of requiring you to insert a debit card, the ATM uses facial recognition (linked to your account) to authenticate you. In addition to facial recognition, you need to enter your 4-digit PIN to make a transaction.
		C	You are at a self-service ATM to make financial transaction. After you insert your debit card, the ATM uses facial recognition (linked to your account) to authenticate you. In addition to facial recognition, you need to enter your 4-digit PIN to make a transaction.
	Cash Register	A	Facial recognition is linked to your credit/debit card account. While you make an in-person payment at a retail store, the in-store facial recognition system (with camera) recognizes you, and lets you make the payment without requiring to present/swipe your debit/credit card.
		B	Facial recognition is linked to your debit/credit card account. At a retail store, you need to be recognized by the in-store facial recognition system (with camera) while you make an in-person payment by swiping your debit/credit card.
	Online	A	You have an application on your smartphone for making online payments linked to your debit/credit card account. Facial recognition is linked to this application. You can log into this application and make an online payment by scanning your face with smartphone camera, where you do not need to enter any password.
		B	You have an application on your smartphone for making online payments linked to your debit/credit card account. Facial recognition is linked to this application. You can log into this application and make an online payment by scanning your face with smartphone camera and entering your password.
Identification at Customer Service	Finance	A	You are at a customer service desk of a financial organization (e.g., a bank), where facial recognition is linked to your account. You will be successfully identified after the facial recognition camera recognizes you at the service desk, where you do not need to present any identification card (e.g., driver's license).
		B	You are at a customer service of a financial organization (e.g., a bank), where facial recognition is linked to your account. You will be successfully identified after the facial recognition camera recognizes you, and you present a valid identification card (e.g., driver's license) at the service desk.
	Non-Finance	A	You are at a customer service desk of an organization that is not financial (e.g. a utility company, retailer, a university registrar, an airline), where facial recognition is linked to your account with them. You will be successfully identified after the facial recognition camera recognizes you at the service desk, where you do not need to present any identification card (e.g., driver's license).
		B	You are at a customer service of an organization that is not financial (e.g. a utility company, retailer, university registrar, travel agent, etc.), where facial recognition is linked to your account with them. You will be successfully identified after the facial recognition camera recognizes you, and you present a valid identification card (e.g., driver's license) at the service desk.
	In-store Pickup	A	You have ordered goods online and would pickup those at a retail store. When you arrive at the store, you do not need to show any identification card (e.g., driver's license). Rather, facial recognition is linked to your account with that retailer, where you receive the items (purchased online) after the in-store facial-recognition camera recognizes you.
		B	You have ordered goods online and would pickup those at a retail store. Facial recognition is linked to your account with that retailer. When you arrive at the store, you present an identification card (e.g., driver's license), and the facial recognition system identifies you, before you receive the items (purchased online).
Personalized Service and Ads	Retail Checkout	A	Your account with a retail store is linked to facial recognition. While you check out at the store, the in-store facial recognition system (with camera) recognizes you and activates your account, which in turn keep records of the items you have purchased.
		B	Your account with a retail store is linked to facial recognition. While you check out at the store, the in-store facial recognition system (with camera) recognizes you and activates your account, which in turn keep records of the items you have purchased. This information helps the retailer to let you know (e.g., through email, mobile app, online account etc.) about future deals on the items you generally buy.
	Restaurant	A	You are a loyalty member of a restaurant, where facial recognition is linked to its loyalty program. The ordering kiosks use facial recognition to recognize you as a loyalty member as you approach, activates your loyalty account and, based on previous purchases, displays your favorite meals and any special deals.
		B	You are a loyalty member of a restaurant, where facial recognition is linked to its loyalty program. The ordering kiosks use facial recognition to recognize you as a loyalty member as you approach and then require you to enter your password associated with the loyalty account. Upon successful authentication, the system activates your loyalty account and, based on previous purchases, displays your favorite meals and special deals.
	Library	A	When you walk into a library, the facial recognition system (with camera) identifies your demographic information (e.g., age, gender, etc.) by scanning your face, where it does not link that to any personally identifiable information (e.g., name, date of birth, address, etc.), but links your demographic information to your book selection.
		B	When you walk into a library, the facial recognition system (with camera) identifies your demographic information (e.g., age, gender, etc.) by scanning your face, where it does not link that to any personally identifiable information (e.g., name, date of birth, address, etc.). The system links your demographic information to the type of books you read, enabling the library to make a catalog of books preferred by users with different demographic traits and use that information to recommend books to a new user.
	Gas Station	A	When you stop by a gas station to refuel your vehicle, the facial recognition system (with camera) identifies your demographic information (e.g., age, gender) by scanning your face, where it does not link that to any of your personally identifiable information (e.g., name, date of birth, address, etc.).
		B	When you stop by a gas station to refuel your vehicle, the facial recognition system (with camera) identifies your demographic information (e.g., age, gender) by scanning your face, where it does not link that to any of your personally identifiable information (e.g., name, date of birth, address, etc.). Here, the system uses your demographic information to show you tailored advertisements on the small TV screen while you refuel your vehicle.
Tracking People	Retail	A	FR, linked to user's online account with the retailer, Your account with a retail store is linked to facial recognition. While you enter the store, the in-store facial recognition system (with camera) recognizes you and activates your account. It then tracks you during shopping and keeps records of the items you purchase and those you showed interest in but did not purchase.
		B	Your account with a retail store is linked to facial recognition. While you enter the store, the in-store facial recognition system (with camera) recognizes you and activates your account. It then tracks you during shopping and keeps records of the items you purchase and those you showed interest in but did not purchase. This information helps the retailer to let you know (e.g., through email, mobile app, online account etc.) about future deals on the items you generally buy and those you show interest in.
		C	FR is used for tracking (participants are informed of the reason: to prevent shoplifting and in-store violence).
	Public	A	FR is used for tracking (participants are not informed of the reason).
		B	FR is used for tracking (participants are informed of the reason: public safety and law enforcement).
Boarding	Flight	A	FR is used instead of requiring to show a boarding pass.
		B	You FR is used, in conjunction with requiring to show a boarding pass.
Recording Attendance	Classroom	-	FR is used for automated attendance tracking in a classroom.

Table 8
Full Description of Vignettes