A Look into User Privacy and Third-party Applications in Facebook

Sovantharith Seng
Computing and Information Sciences
Rochester Institute of Technology
Rochester, New York, USA
sovantharith.seng@mail.rit.edu

Mahdi Nasrullah Al-Ameen
Computer Science
Utah State University
Logan, Utah, USA
mahdi.al-ameen@usu.edu

Matthew Wright
Computing Security
Rochester Institute of Technology
Rochester, New York, USA
matthew.wright@rit.edu

***Abstract*—A huge amount of personal and sensitive data is shared on Facebook, which makes it a prime target for attackers. Adversaries can exploit third-party applications connected to a user's Facebook profile (i.e., Facebook apps) to gain access to this personal information. Users' lack of knowledge and the varying privacy policies of these apps make them further vulnerable to information leakage. However, little has been done to identify mismatches between users' perceptions and the privacy policies of Facebook apps. We address this challenge in our work. We conducted a lab study with 31 participants, where we received data on how they share information in Facebook, their Facebook-related security and privacy practices, and their perceptions on the privacy aspects of 65 frequently-used Facebook apps in terms of data collection, sharing, and deletion. We then compared participants' perceptions with the privacy policy of each reported app. Participants also reported their expectations about the types of information that should not be collected or shared by any Facebook app. Our analysis reveals significant mismatches between users' privacy perceptions and reality (i.e., privacy policies of Facebook apps), where we identified over-optimism not only in users' perceptions of information collection, but also on their self-efficacy in protecting their information in Facebook despite experiencing negative incidents in the past. To the best of our knowledge, this is the first study on the gap between users' privacy perceptions around Facebook apps and the reality. The findings from this study offer directions for future research to address that gap through designing usable, effective, and personalized privacy notices to help users to make informed decisions about using Facebook apps.**

***Index Terms*—Privacy; Perceptions; Facebook; Third-party Applications; User Study**

I. Introduction

Social networks like Facebook have become an integral part of everyday life for many people, as they are used to maintain social ties, build professional connections, share news and interests, and promote business. Also, a wide variety of third-party applications use Facebook's *social login* feature that allows users to log into those applications from their Facebook profile (we call these *Facebook apps* or just *apps* in this paper). People share a plethora of information through their Facebook profile, which makes it a prime target for attackers to gain access to users' sensitive and personal information [27, 44, 55]. Adversaries may also exploit Facebook apps to collect users' information from their Facebook account. The Cambridge Analytica scandal [7, 25]in particular exposed the vulnerability of users' personal information to these third parties.

A. Motivation

After the Cambridge Analytica incident [7, 25], the privacy risks of third-party apps connected to users' Facebook accounts have drawn widespread attention. However, users lack knowledge of how to keep the security and privacy of their social network profile [3, 27, 49]. This challenge can be exacerbated by the varying privacy policies of Facebook apps in terms of data collection and sharing. Prior work has shed light on users' understanding of general privacy settings on the Facebook website [26, 38, 54, 56]. However, users' perceptions and expectations about data collection, sharing, and deletion through Facebook apps are still understudied. Prior work on mismatches between privacy policies and user expectations in platforms other than Facebook [4, 13, 43], while partially helpful in this regard, also illustrates that these policies vary across platforms.

With the ubiquitous use of social login to third-party apps, it is important to understand users' information sharing, their security and privacy practices, and the mismatch between users' perceptions and the privacy policies of Facebook apps in order to effectively devise usable solutions to help users make more informed privacy decisions for third-party apps.

We address these challenges in this paper. In particular, we conducted a lab study, where participants reported their information sharing through Facebook, security and privacy practices in Facebook to protect their information, frequently used Facebook apps, and their perceptions of each of those apps' privacy policies in terms of data collection, sharing, and deletion (i.e., the right to be forgotten), and their expectations of information that should not be collected or shared by any Facebook app.

B. Contributions

In this study, we received data on a total of 113 apps (65 unique apps) from 31 participants. We then investigated the

Information and Computer Security Journal
Accepted: 12 October 2020
DOI: https://doi.org/10.1108/ICS-08-2019-0108

privacy policy of each reported app and compared it with the privacy perceptions of the participants. Our analysis reveals significant mismatches between users' privacy perceptions and reality (i.e., the actual privacy policies of the apps). Overall, we identified a 40% mismatch between perceptions and policies on information collection, where 80% of these mismatches are overly optimistic: participants believe that the information is not collected by an app, even though it actually is collected according to the app's privacy policy.

We identified similar over-optimism in participants' responses on their ability (*self-efficacy*) to protect their information in Facebook. Despite experiencing negative incidents in the past, including account compromise and leakage of personal information, users do not take adequate security and privacy protection steps in Facebook. Our results also indicate how users' information sharing behavior in Facebook could pose risks for their overall online security and privacy.

As participants reported their expectations for privacy from Facebook apps, we found that they expect apps to share less information than they collect. Based on our findings, we recommend providing users with tools and information that they need to make informed decisions in using Facebook apps. We provide directions for apps to better address users' privacy expectations, where our findings provide important insights to design usable and effective privacy notices by highlighting unexpected data practices. Our study also shows the importance of taking users' demographic traits into account in the design of personalized privacy notices, where we identified differences in mismatched privacy perceptions across gender and age.

II. Background

In this section, we discuss recent incidents of information leakage in Facebook, users' understanding of Facebook privacy settings, and mismatches between users' expectations and online privacy policies, including Facebook. We then briefly discuss *social login*, which is used by the third-party apps connected to users' Facebook accounts.

A. Information Leakage through Facebook

With the progress of technology and the development of new business models, the security and privacy issues become more complex, creating major concerns for users [37].

The privacy issues with Facebook stem from the abundance of data that its users share through the platform [16]. A bug in the Facebook interface exposed the private information of around six million users in 2013 [14]. In 2014, Facebook conducted an experiment regarding mood manipulation via the newsfeed of randomly selected users [35], which raised unrest among users about how Facebook was handling their data. Then in 2015, Facebook had to shut down an API that allowed applications to access users' private information, especially the information about users' friends [8]. As the Cambridge Analytica scandal broke in 2018 [24], the news came to light that the personal information of about 87 million Facebook users were harvested and used through the third-party app without the users' consent. While this news sparked a worldwide discussion about users' data privacy in Facebook, all these noted incidents in recent years kept raising the question of how much control the users have on their personal and sensitive information shared through social networking sites and Facebook in particular.

B. Privacy Policy and Settings

Privacy notices often fail to help users with making an informed privacy decision due to their excessive length, complicated language, or poor visualization [28, 41]. As a result, users pay little attention to the privacy policy, and give consent to use the application, website, or an IoT (Internet-of-Things) device without a proper understanding of its data collection and sharing practices [13, 39, 48].

As recommended in prior studies [41, 48], a privacy notice should aim for simplicity, brevity, and clarity in design for being understandable to general users. Knijnenburg and Cherry [34] proposed a comic-based approach to make privacy policies more understandable and fun to read. The studies of Kelly et al. [30, 31]evaluated the usability and efficacy of a privacy "nutrition label," where the authors designed a tabular format to enhance user's understanding of privacy practices, increase the speed of finding privacy related information, and facilitate comparison between the privacy policies of different websites and applications.

Sathyendra et al. [47] examined the problem of automatic identification of privacy choices in a privacy policy. They focused on opt-out choices offered in a privacy policy, and leveraged machine-learning techniques to automatically extract relevant information from the privacy policy of a website [47]. Sadeh et al. [46] employed crowdsourcing on top of machine-learning and natural language processing to develop a scalable infrastructure that semi-automatically provides answers to the privacy related questions that a user may have. Anton et al. [4] leveraged the privacy policy of different healthcare providers to present a taxonomy for classifying privacy goals, where they also described the use of goal-mining to examine the privacy policy for system requirements.

In our work, we focused on the third-party applications that are connected to users' Facebook accounts. Within this domain,

Torres et al. [54] found that over 25% of participants in their study were unsure of their Facebook privacy settings, and about 20% of participants did not change their privacy settings at all, indicating that it did not seem necessary. In contrast, Jabee et al. [26] found that users resorted to the default Facebook privacy settings due to not understanding how to find and change them. Tuunainen et al. [56] reported that over half of the participants in their study were unaware of how the information from their Facebook profile was shared with other entities, despite stating that they went through the general Facebook privacy settings. Boyd et al. [6] focused on the privacy practices of young adults in Facebook, where they found a general interest among participants to adjust the

privacy settings of their account. In a separate study [38], 85% of participants stated that Facebook's privacy settings should be improved.

These studies only consider the general Facebook privacy settings and did not shed light on the privacy features of third-party apps connected to users' Facebook accounts.

C. Mismatches in Privacy Expectations

Rao et al. [43] examined mismatches between users' expectations and the privacy policies of general websites, like the financial and health sites. The study [43] revealed that the mismatch between users' privacy expectations and the actual privacy policy of a website could be over 50% for certain types of information. Liu et. at [38] examined the disparity between users' expectations and their Facebook privacy settings. In this study, authors found that the privacy expectations of users did not match with their privacy setting in 37% of cases. Neither of these studies, however, focused on the mismatch between users' perceptions and the privacy policies of third-party apps connected to their Facebook account.

D. Social Login

Social login [45] is a mechanism that uses existing information to identity a user on a social networking platform to register or log into a third-party app or website. The convenience in account creation and authentication via social login has elevated its popularity among users [52]. However, social login may provide third-party websites and apps with permissions to obtain users' personal information from their social network profile. Accordingly, Egelman [12] found that 15% of participants chose not to use the social login service due to privacy concerns, where 88% of participants reported understanding the access privileges they allow to a website through social login.

In this paper, we focus on the third-party apps connected to users' Facebook accounts through social login. In particular, we study users' perceptions on the type of information collected and shared by these apps and users' ability to have their collected information deleted. We then identify the mismatch between users' perceptions and the privacy policies of these apps.

III. Methodology

We conducted the study in a lab environment, between August 2018 and January 2019, where participants completed the survey hosted on the Qualtrics platform after they had read and agreed to informed consent document. We preferred a lab setting for this study to make sure participants go through their Facebook account in order to carefully review the apps connected to their account before they report them in the study. Participants were given the option to use either their own laptop or the lab computer to log into their Facebook account and complete the survey. When participants used the lab computer, we ensured that they used an incognito browser tab and logged out of their Facebook account by the end of study session. The sessions lasted for around 35 minutes on average. Student participants each received a $10 Amazon gift card for taking part in the study, though we could not compensate the university staff members due to university rules. The study was approved by the university's Institutional Review Board.

For each reported app, we asked participants about their privacy perceptions in terms of information collected and shared by that app, and the deletion options it offers to users. Later, we conducted a detailed review of the privacy policy of each app reported by the participants and compared that with their privacy perceptions. Here, we analyzed the privacy policies that were in effect as of April 2019, which was after the Cambridge Analytica incident [7, 25] and the publishing of new privacy policy by Facebook in May, 2018 [50]. Our analysis revealed the mismatches in the privacy perceptions of users and their choices of apps.

A. Data Collection

For each reported app, participants were asked about their perceptions of its privacy policy in terms of: information collected from users, information shared with other entities to provide users with intended services or for other purposes, and the options offered to users to delete the information collected from them. After participants reported their privacy perceptions for each of the reported apps, they were asked about their overall privacy expectations, such as the types of information they believe should not be collected and shared by any app connected to their Facebook account.

In addition to the questions on privacy perceptions and expectations, we asked participants about their demographics (e.g., gender, birth year, race), education and current occupation, training in fields related to computer science, general Facebook usage (e.g., how long they have been using Facebook, how many friends they have, how many groups they are member of, and how often they access Facebook), type of information they share through their Facebook profile, steps they take for security and privacy-preserving use of Facebook, their self-efficacy in protecting the security and privacy of their Facebook account, and any negative experiences they had faced in the past with regard to using Facebook and performing online activities.

B. Facebook Applications

Participants were asked to report all of their apps up to a maximum of five, where participants with more than five apps were asked to report the five apps used most frequently. We categorize the reported apps (see below) based on the guidelines from prior research [20, 21].

- **Financial.** This category includes apps that involve financial transactions. We divide these apps into two subcategories: i) *Primary financial app*, where making financial transactions is the primary purpose of the app, as in online banking, and ii) *Secondary financial app*, where financial transactions are not the primary purpose of the app but are certainly required, as in e-commerce.

- **Identity.** An app that needs users to provide their identity, health, or other personal information to use its primary services is included to Identity category. We divide these apps into four subcategories: i) *Communication*: apps that facilitate conversation through chat, voice, or video call, ii) *Fitness*: apps that assist in fitness and health tracking, iii) *Q&A*: apps that allow the users to get answers on certain topics from other users, and iv) *Social Networking*: apps that create a platform for users to socialize in an online setting.
- **Content.** The apps in this category provide users with content related to *entertainment*, *news*, and different types of *listing* (e.g., jobs, apartments, etc). Users do not need to make any financial transactions or provide their personal information to use these apps.
- **Other.** Apps in the *game* and *utility* subcategories comprise most of the Other category.

IV. Results

In this section, we present the findings from our user study and report the results of our statistical tests where we found a significant difference (p-value is less than 0.05).

A. Participants

A total of 31 participants took part in our study (Female: 15; Male: 15; Did not disclose gender: one participant). Twenty of our participants were students, and the remaining 11 participants were university staff members. The average age of our participants was 29 (minimum: 19; maximum: 63), where the average age of the participants in the staff and student pools were 40 and 23, respectively. Seventeen of our participants identified as White, followed by 12 Asian/Pacific Islanders, one Black/African American, and one multiracial. All of our participants had at least a Bachelor's degree or were currently working toward it. Fourteen participants are pursuing or have completed a degree in computer science or a related field.

B. Facebook Usage

All of the participants are regular users of social networking sites like Facebook. On average, they have been using Facebook for around nine years (students: eight years, staff: eleven years), currently have around 500 friends, and are members of about 25 groups. Each participant had on average 10 apps connected to their Facebook account. Participants in the staff pool reported visiting their Facebook account more often as compared to the student population.

1) Sharing Personal Information.: Over two-thirds of the participants reported that they do not share their mobile number, email ID, or current physical address through their Facebook profile, neither publicly nor with their friend list, where over one-third of participants do not share information about their current relationship status, religious views, or political views. On the other hand, at least half of the participants share their full name and gender publicly through their profile, and at least one-third of our participants publicly share the information about their educational institutions (e.g., high school, college), current workplace, and current city. This means that anyone could gain access to this information by crawling their Facebook profile. We found instances where participants do not share their physical address with their friend list but do share the more general information publicly, like the city they currently live in (see Table IX in the Appendix for further details).

In response to the question on sharing their current location in Facebook (e.g., through 'check-in' posts), 21 participants (67.7%) reported that they never share their current location publicly, i.e., with someone who is not in their friend list, while 14 participants (45%) do not share their current location even with their Facebook friends.

2) Security and Privacy Protection: We asked participants about the steps they take for secure browsing, checking their Facebook security and privacy settings, and confirming the identity of unknown persons before adding them to their friend list. Participants also reported their self-efficacy in maintaining the security and privacy of their Facebook account.

a) Secure Browsing.: Checking for a secure connection before visiting a website and checking the destination

Category	Sub-Category	App Count	Total Mentions
Financial	Primary	2	6
	Secondary	12	15
Identity/Personal	Communication	2	5
	Fitness	4	4
	Q&A	1	6
	Social Networking	8	16
Content	Entertainment	10	23
	Listing	8	15
	News	3	3
Other	Game	9	11
	Utility	6	9

TABLE I: Number of Unique Facebook Apps and Total Number of Mentions Reported by the Participants

Category	Sub-Category	Concerns				
		Waste of Time	Improper Content	Privacy	None	Other
Financial	Primary	0	0	4	2	0
	Secondary	1	0	1	11	3
Identity/Personal	Communication	1	1	1	3	0
	Fitness	0	0	0	3	1
	Q&A	0	2	3	2	1
	Social Networking	7	5	2	6	2
Content	Entertainment	9	6	2	14	0
	Listing	1	0	7	7	1
	News	2	0	0	1	0
Other	Game	5	1	0	5	1
	Utility	2	0	1	6	0

TABLE II: Users' Concerns about Facebook Apps

Category	Sub-Category	Types of Information											
		Work & Education	Places I Have Lived	Contact & Basic Info	Family & Relationship	Details about Me	Photos & Videos	Current Location	Friend's Info	Posts on Newsfeed	Online Presence	Inbox	Other
Financial	Primary	3	1	4	1	3	0	1	4	0	1	0	0
	Secondary	6	5	10	1	10	1	5	1	1	5	0	1
	SUBTOTAL	9	6	14	2	13	1	6	5	1	6	0	1
	%	**42.9%**	**28.6%**	**66.7%**	**9.5%**	**61.9%**	**4.8%**	**28.6%**	**23.8%**	**4.8%**	**28.6%**	**0.0%**	**4.8%**
Identity/Personal	Communication	0	0	3	0	2	2	1	0	1	2	1	0
	Health	0	2	4	2	3	0	0	1	0	0	0	1
	Q/A	4	2	4	0	2	0	1	1	2	3	1	0
	Social Networking	7	7	13	4	14	8	8	5	4	4	1	0
	SUBTOTAL	11	11	24	6	21	10	10	7	7	9	3	1
	%	**35.5%**	**35.5%**	**77.4%**	**19.4%**	**67.7%**	**32.3%**	**32.3%**	**22.6%**	**22.6%**	**29.0%**	**9.7%**	**3.2%**
Content	Entertainment	2	5	11	5	14	4	6	8	3	7	1	4
	Listing	4	4	14	1	12	2	7	1	2	5	1	1
	News	3	3	3	1	3	0	2	0	0	1	0	0
	SUBTOTAL	9	12	28	7	29	6	15	9	5	13	2	5
	%	**22.0%**	**29.3%**	**68.3%**	**17.1%**	**70.7%**	**14.6%**	**36.6%**	**22.0%**	**12.2%**	**31.7%**	**4.9%**	**12.2%**
Other	Game	1	1	9	0	5	3	0	3	2	4	0	1
	Utility	1	0	7	2	5	2	5	2	1	0	0	1
	SUBTOTAL	2	1	16	2	10	5	5	5	3	4	0	2
	%	**10.0%**	**5.0%**	**80.0%**	**10.0%**	**50.0%**	**25.0%**	**25.0%**	**25.0%**	**15.0%**	**20.0%**	**0.0%**	**10.0%**
	TOTAL	31	30	82	17	73	22	36	26	16	32	5	9
	%	**27.4%**	**26.5%**	**72.6%**	**15.0%**	**64.6%**	**19.5%**	**31.9%**	**23.0%**	**14.2%**	**28.3%**	**4.4%**	**8.0%**

TABLE III: Users' Perceptions of Information Collected by Facebook Apps

while clicking on a link are recommended security practices to protect against cyber attacks, including phishing and malware [3, 10, 36]. In our study, about one-fifth of the participants reported that they always check for a secure connection (e.g., 'https', padlock icon in URL bar) when visiting Facebook. About one-fourth of our participants noted that they always hover over a Facebook link before clicking on it to be sure of the destination site.

b) Checking Security and Privacy Settings.: All of our participants except two reported checking the security and privacy settings of their Facebook account, where 14 participants (45.2%; students: seven out of 20, staff: seven out of 11) check that setting whenever they find out about a security or privacy breach in someone else's account, either through news or personal communication. Fifteen of our participants (48.4%; students: 11 out of 20, staff: four out of 11) check their security and privacy settings when they are informed of any new changes in Facebook's security and privacy features. Students (55%) are more likely than the staff participants (36%) to check their security and privacy settings when they come to know about any new changes in Facebook's security and privacy features. On the other hand, as compared to the student population (35%), staff members (64%) are more likely to check their security and privacy setting when they get to know about a security or privacy incident.

c) Adding Unknown Friends.: When accepting a friend request from an unknown person in Facebook, 14 of 21 students (70%) and seven of 11 staff members (63.6%) reported that they do not usually take any steps to verify the identity of that person, which could create risks of compromise by adversaries posing as friends.

d) Self Efficacy.: The participants reported above-average self-efficacy (higher than 3.5 on a 7-point Likert scale) on all aspects related to maintaining the security and privacy of their Facebook account. Overall, students reported higher self-efficacy than the staff participants in all aspects except for having no fake people in their Facebook friend list (see Table X in Appendix).

3) Negative Experiences: Six of our student participants reported that their Facebook account had been hacked by adversaries in the past, where 27 participants (87.1%) had heard of at least one incident in which the Facebook account of their friend or family member was compromised. Upon hearing about such incidents, 18 (58.1%) of our participants changed their Facebook password, 10 (32.3%) participants turned on two-factor authentication for their Facebook account, and five participants (16%) reviewed their friend list to identify any fake or suspicious entities. Several participants reported taking more than one of the above steps to protect their account from unauthorized access, but four participants (12.9%) reported not taking any step at all.

In addition to Facebook account compromise, participants reported having faced other negative experiences through social networking sites and online activities, including stalking and harassment (students: 5, staff: 4), damage of reputation (students: 5), difficulties in personal relationships due to

Category	Sub-Category	Types of Information											
		Work & Education	Places I Have Lived	Contact & Basic Info	Family & Relationship	Details about Me	Photos & Videos	Current Location	Friend's Info	Posts on Newsfeed	Online Presence	Inbox	Other
Financial	Primary	0	0	5	0	0	0	2	3	0	0	0	0
	Secondary	0	1	7	0	2	1	3	2	0	2	0	0
	SUBTOTAL	0	1	12	0	2	1	5	5	0	2	0	0
	%	**0.0%**	**4.8%**	**57.1%**	**0.0%**	**9.5%**	**4.8%**	**23.8%**	**23.8%**	**0.0%**	**9.5%**	**0.0%**	**0.0%**
Identity/Personal	Communication	0	0	4	0	2	2	0	0	0	0	0	0
	Health	1	0	2	0	2	0	1	0	0	1	0	0
	Q/A	2	1	3	0	3	0	1	0	1	1	0	0
	Social Networking	2	1	10	0	9	4	5	1	1	1	0	1
	SUBTOTAL	5	2	19	0	16	6	7	1	2	3	0	1
	%	**16.1%**	**6.5%**	**61.3%**	**0.0%**	**51.6%**	**19.4%**	**22.6%**	**3.2%**	**6.5%**	**9.7%**	**0.0%**	**3.2%**
Content	Entertainment	0	4	9	2	9	1	9	2	1	8	0	3
	Listing	2	2	8	0	8	1	7	1	1	4	0	0
	News	0	0	0	0	0	0	0	0	0	1	0	0
	SUBTOTAL	2	6	17	2	17	2	16	3	2	13	0	3
	%	**4.9%**	**14.6%**	**41.5%**	**4.9%**	**41.5%**	**4.9%**	**39.0%**	**7.3%**	**4.9%**	**31.7%**	**0.0%**	**7.3%**
Other	Game	1	0	4	1	2	1	0	1	1	2	0	0
	Utility	0	0	5	1	4	1	3	1	0	0	0	0
	SUBTOTAL	1	0	9	2	6	2	3	2	1	2	0	0
	%	**5.0%**	**0.0%**	**45.0%**	**10.0%**	**30.0%**	**10.0%**	**15.0%**	**10.0%**	**5.0%**	**10.0%**	**0.0%**	**0.0%**
	TOTAL	8	9	57	4	41	11	31	11	5	20	0	4
	%	**7.1%**	**8.0%**	**50.4%**	**3.5%**	**36.3%**	**9.7%**	**27.4%**	**9.7%**	**4.4%**	**17.7%**	**0.0%**	**3.5%**

TABLE IV: Users' Perceptions of Information Shared by Facebook Apps with Other Entities (to Provide Service)

social networking posts (students: 10, staff: 3), leakage of personal information to unwanted entities (students: 3, staff: 7), and being a victim of online scams incurring monetary loss (students: 4, staff: 1). Among students, it was common to face difficulties in personal relationships due to social networking posts, where half of them reported having this experience. For staff, leakage of personal information by unwanted entities was a notable concern, where two-third of them reported being a victim of such an incident.

C. Facebook apps

As we asked participants to report the apps connected to their Facebook account, we received a total of 113 entries as listed in Table I. After removing the duplicate apps, we got 65 unique apps. Participants reported to learn about most of the apps from their friends, either through online invitations or offline conversations. They also learn about Facebook apps through ads. The majority of reported apps are used by our participants at least once a week, and about one-third of the apps are used daily.

a) Users' Concerns and Past Removal of apps.: The participants reported "Waste of Time" and "Privacy" to be their primary concerns about the apps connected to their Facebook account (see Table II). They mentioned removing **a total of 23 apps** in the past, where most of them were games or entertainment apps. They removed those apps as they were no longer needed, or they were too time consuming. They did not mention about removing any app due to privacy concerns.

D. Privacy Perceptions of Users

In this section, we present our findings on the perceptions of users about the types of information collected and shared by their third-party Facebook apps, and their ability to have their collected information deleted.

1) Information Collection.: As perceived by our participants, identity apps collect the most information from users, followed by content, financial, and finally other apps (e.g., game, utility). According to them, the contact and basic information of users are collected by 73% of all apps, followed by users' details like name and favorites (65%), their current location (32%), and information about users' work and education (27%). Below, we discuss our findings on users' perceptions of information collection across different app categories (see Table III for further details).

a) Financial.: According to our participants, around two-thirds of financial apps to collect users' details (e.g., name, favorites), contact and basic information, and over one-third of financial apps collect information about users' work and education. In contrast, no financial app is believed to collect users' inbox messages, while posts on their newsfeed, and users' photos and videos are collected by fewer than 5% of financial apps in their view.

b) Identity.: Our participants believe that over three-fourths of identity apps collect users' contact and basic information, two-thirds collect their details (e.g., name, favorites), and around one-third collect users' photos and videos, information about their work and education, places they have lived,

Category	Sub-Category	Types of Information											
		Work & Education	Places I Have Lived	Contact & Basic Info	Family & Relationship	Details about Me	Photos & Videos	Current Location	Friend's Info	Posts on Newsfeed	Online Presence	Inbox	Other
Financial	Primary	4	3	0	4	5	4	2	1	3	4	3	0
	Secondary	5	5	3	6	3	6	5	4	5	6	4	0
	SUBTOTAL	9	8	3	10	8	10	7	5	8	10	7	0
	%	**42.9%**	**38.1%**	**14.3%**	**47.6%**	**38.1%**	**47.6%**	**33.3%**	**23.8%**	**38.1%**	**47.6%**	**33.3%**	**0.0%**
Identity/Personal	Communication	1	2	0	1	3	0	2	1	2	3	1	0
	Health	1	2	2	2	4	1	0	1	2	1	1	0
	Q/A (Quora)	3	3	1	1	3	1	2	1	1	1	0	0
	Social Networking	6	6	5	7	5	4	6	5	6	9	8	0
	SUBTOTAL	11	13	8	11	15	6	10	8	11	14	10	0
	%	**35.5%**	**41.9%**	**25.8%**	**35.5%**	**48.4%**	**19.4%**	**32.3%**	**25.8%**	**35.5%**	**45.2%**	**32.3%**	**0.0%**
Content	Entertainment	9	6	8	8	9	6	5	7	5	6	7	0
	Listing	6	5	7	6	8	6	4	4	7	5	4	0
	News	2	2	2	2	3	1	1	1	2	1	1	0
	SUBTOTAL	17	13	17	16	20	13	10	12	14	12	12	0
	%	**41.5%**	**31.7%**	**41.5%**	**39.0%**	**48.8%**	**31.7%**	**24.4%**	**29.3%**	**34.1%**	**29.3%**	**29.3%**	**0.0%**
Other	Game	2	3	4	4	4	5	2	3	3	5	1	0
	Utility	3	3	1	3	1	1	1	3	2	4	3	1
	SUBTOTAL	5	6	5	7	5	6	3	6	5	9	4	1
	%	**25.0%**	**30.0%**	**25.0%**	**35.0%**	**25.0%**	**30.0%**	**15.0%**	**30.0%**	**25.0%**	**45.0%**	**20.0%**	**5.0%**
	TOTAL	42	40	33	44	48	35	30	31	38	45	33	1
	%	**37.2%**	**35.4%**	**29.2%**	**38.9%**	**42.5%**	**31.0%**	**26.5%**	**27.4%**	**33.6%**	**39.8%**	**29.2%**	**0.9%**

TABLE V: Users' Perceptions of Information Shared by Facebook Apps with Other Entities (Not Required to Provide Service)

and current location. About 10% of identity apps are believed to view users' inbox messages.

c) Content.: More than two-thirds of content apps are believed to collect users' details (e.g., name, favorites), contact and basic information, while around one-third collect current location and online presence. Fewer than 5% of content apps collect users' inbox messages.

d) Other.: Over three-fourths of apps in the 'other' category (e.g., game, utility) are believed to collect users' contact and basic information, and half of the apps collect users' details (e.g., name, favorites). On the other hand, none of the apps in 'other' category collect users' inbox messages, and fewer than 10% of 'other' apps collect information about the places users have lived in our participants' view.

2) Information Sharing.: As we asked participants about their perceptions on the information that apps share with other entities as necessary to provide them with intended service, and they reported that 50.4% of apps (financial: 57.1%, identity: 61.3%, content: 41.5%, and other: 45.0%) share their contact and basic information with other entities. According to the participants' perceptions, their details (e.g., name, favorites) and information about their current location are shared by 36.9%, and 27.4% of apps, respectively (see Table IV).

The participants also reported their perceptions on the information that they think the apps share with other entities although such sharing is not needed to provide them with intended service (see Table V. In this regard, participants think that above one-third of apps share at least one of the following information with other entities: users' details (name, favorites), information about their family and relationship, online presence, their work and education, places they have lived, and posts on their Facebook newsfeed. As perceived by the participants, 31% of apps share their photos and videos with other entities, although they do not need to share such personal information to provide the intended service.

3) Information Deletion.: For 77% of apps, users think that they would be allowed to delete the information that is collected by these apps (see Table VI). In particular, they reported expecting that all six apps in the 'financial: primary' category would allow them to delete the collected information.

E. Mismatched Privacy Perceptions

For each app, we compared participants' privacy perceptions with the app's privacy policy. We could not compare users' perceptions of information sharing with the privacy policy, since sufficient details about information sharing are not stated in the apps' privacy policies.

1) Information Collection.: There are four cases resulting from our comparison between users' perceptions and an app's privacy policy in terms of data collection by the apps:

- *'YY' match*: the user believes that the information is collected by an app and the privacy policy states that it is indeed collected;

Category	Sub-Category	Deletion Preference	
		Allowed to Delete	Not Allowed
Financial	Primary	6	0
	Secondary	10	5
	SUBTOTAL	**16**	**5**
	%	**76.2%**	**23.8%**
Identity/Personal	Communication	4	1
	Health	3	1
	Q&A	4	1
	Social Networking	12	3
	SUBTOTAL	**23**	**6**
	%	**79.3%**	**20.7%**
Content	Entertainment	16	7
	Listing	11	4
	News	3	0
	SUBTOTAL	**30**	**11**
	%	**73.2%**	**26.8%**
Other	Game	8	2
	Utility	7	2
	SUBTOTAL	**15**	**4**
	%	**78.9%**	**21.1%**
	TOTAL	**84**	**26**
	%	**76.4%**	**23.6%**

TABLE VI: Users' Perceptions of Deletion Preference Offered by Facebook Apps

- *'NN' match*: the user believes that the information is not collected by an app and the privacy policy of that app does not indicate such data is collected;
- *'YN' mismatch*: the user thinks that the information is collected by an app, but that information is not collected according to the app's privacy policy; and
- *'NY' mismatch*: the user thinks that the information is not collected by an app, but that information is collected according to the app's privacy policy.

Overall, we found an approximately 40% mismatch rate between users' perceptions and reality, as we compared participants' perceptions of information collection with the privacy policy of each reported app. Here, we found most mismatches for Communication apps (51.7%), followed by Q&A (44.4%) and Entertainment (41.7%) apps (see Table VII). We found a significantly higher rate of 'NY' mismatches (79.3%) as compared to 'YN' mismatches (20.7%), $\mathcal{X}^2 = 7.49$, $p < 0.05$. There was little difference in both the overall mismatch rate and proportion of 'NY' versus 'YN' mismatches among the four categories of apps.

Our analysis reveals the mismatch between users' perceptions and apps' privacy policy for different types of information, where we found most mismatches for the following types of information: online presence of users (61.1%), places where users have lived (58.4%), users' family and relationship (50.4%), information about users' friends in Facebook (51.3%), and the current location of users (44.2%). Among these types of mismatches, we identified a 'NY' mismatch in 89.6% cases (see Table XI- XIV in the Appendix).

While there was not a notable difference between male and female participants in the overall rate of mismatches, we identified a significantly higher 'NY' mismatch for female participants (84.6%) as compared to male participants (74.4%), $\mathcal{X}^2 = 9.2526$, $p < 0.05$.

2) Information Deletion.: As with, information collection, there are four cases for information deletion:

- *'YY' match*: the user believes that she can have her information deleted, and the app's privacy policy states that it can indeed be deleted;
- *'NN' match*: the user believes that the app will not delete her information, and the app's privacy policy indeed does not indicate that her information can be deleted;
- *'YN' mismatch*: the user thinks that she can have the app delete her information, but the app's privacy policy does not indicate that it will heed her request; and
- *'NY' mismatch*: the user believes that the app will not delete her information, but the app's privacy policy actually indicates that it will delete the information on request.

We identified 41.7% mismatches between users' perceptions and apps' privacy policies in terms of information deletion. We

Category	Sub-Category	MATCH			MISMATCH		
		YY	NN	%	YN	NY	%
Financial	Primary	14	32	63.9%	4	22	36.1%
	Secondary	32	77	60.6%	15	56	39.4%
	SUBTOTAL	**46**	**109**	**61.5%**	**19**	**78**	**38.5%**
Identity/Personal	Communication	10	19	48.3%	1	30	51.7%
	Fitness	8	21	60.4%	5	14	39.6%
	Q&A	12	28	55.6%	14	18	44.4%
	Social Networking	61	64	65.1%	11	56	34.9%
	SUBTOTAL	**91**	**132**	**59.9%**	**31**	**118**	**40.1%**
Content	Entertainment	47	114	58.3%	18	97	41.7%
	Listing	44	64	60.0%	10	62	40.0%
	News	8	15	63.9%	8	5	36.1%
	SUBTOTAL	**99**	**193**	**59.3%**	**36**	**164**	**40.7%**
Other	Game	20	63	62.9%	11	38	37.1%
	Utility	18	53	65.7%	13	24	34.3%
	SUBTOTAL	**38**	**116**	**64.2%**	**24**	**62**	**35.8%**
	TOTAL	**274**	**550**	**60.8%**	**110**	**422**	**39.2%**

TABLE VII: Information Collected by Facebook Apps: Users' Perceptions Compared to Privacy Policy

Category	Sub-Category	MATCH			MISMATCH		
		YY	NN	%	YN	NY	%
Financial	Primary	0	0	0.0%	6	0	100.0%
	Secondary	7	1	53.3%	3	4	46.7%
	SUBTOTAL	**7**	**1**	**38.1%**	**9**	**4**	**61.9%**
Identity/Personal	Communication	4	0	80.0%	0	1	20.0%
	Fitness	2	0	50.0%	1	1	50.0%
	Q&A	5	0	83.3%	0	1	16.7%
	Social Networking	10	1	68.8%	3	2	31.3%
	SUBTOTAL	**21**	**1**	**71.0%**	**4**	**5**	**29.0%**
Content	Entertainment	16	0	69.6%	0	7	30.4%
	Listing	4	4	53.3%	7	0	46.7%
	News	2	0	66.7%	1	0	33.3%
	SUBTOTAL	**22**	**4**	**63.4%**	**8**	**7**	**36.6%**
Other	Game	8	0	72.7%	1	2	27.3%
	Utility	6	0	66.7%	1	2	33.3%
	SUBTOTAL	**14**	**0**	**70.0%**	**2**	**4**	**30.0%**
	TOTAL	**64**	**6**	**68.0%**	**23**	**20**	**41.7%**

TABLE VIII: Deletion Preference Offered by Facebook Apps: Users' Perceptions Compared to Privacy Policy

found the most mismatches for the financial apps (61.9%), followed by the apps in other (41.7%), content (36.6%), and identity categories (29.0%). Overall, we found 53.5% 'YN' mismatch, with 100% 'YN' mismatches for the apps in 'financial: primary' category (see Table VIII).

We found a 40.4% mismatch rate for male participants and 35.7% mismatch rate for female participants, where our analysis reveals 52.2% and 55% 'YN' mismatch for the male and female participants, respectively. However, these analysis are not significant.

We conducted significance tests to identify if the mismatched privacy perceptions of users in terms of information collection and deletion vary across application categories or type of information. We did not find any significant differences in these cases.

F. Expectations: Never Collect or Share

In this section, we present our findings on the expectations of users about the types of information that should not be collected or shared by any app, where we compare those expectations between the users from two different groups: students (mean age: 23) and university staff (mean age: 40).

1) Collection.: Figure 1a presents the information that participants expect not to be collected by any app, where students are found to be more lenient than the professional staff members. Most students (85%) do not expect inbox messages to be collected by an app, and half of the student participants believe that no app should collect their photos and videos, information about their family and relationships, places they have lived, and their Facebook friends. The majority of participants from the staff pool do not expect any information except the contact and basic information of users should be collected by an app. In this regard, 91% of the staff participants do not expect inbox message to be collected by any app, and about three-fourths of the participants from the staff pool believe that no app should collect their photos and videos or information about their Facebook friends.

2) Sharing.: Figure 1b presents the information that participants expect not to be shared by an app with other entities. Around three-fourths of student participants expect that their inbox messages and photos and videos would not be shared with other entities. The professional staff members reported a more strict expectation in terms of information sharing; more than 80% of them believe that none of the information should be shared by an app with other entities, except for contact and basic information, where still two-thirds of staff members expect the information to not be shared.

3) Collection vs. Sharing.: Overall, the participants in both groups (students and staff) expect that apps will collect more information than they share with other entities. Among students, for example, 84% expect that apps will collect contact and basic information and the information about their work and education, but just 60% expect that this information might be shared. Similarly, 64% of staff members do not think their contact and basic information should be shared by any app, in contrast to 9% of staff who do not expect this information to be collected by any app. Also, 40% of students and 55% of staff expect the information about their current location not to be collected by any app, while 65% of students and 81% of staff do not expect their current location to be shared with other entities by any app.

V. Discussion

We now discuss the implications of our findings, the limitations of our work, and possible directions for future research.

A. Information Sharing through Facebook

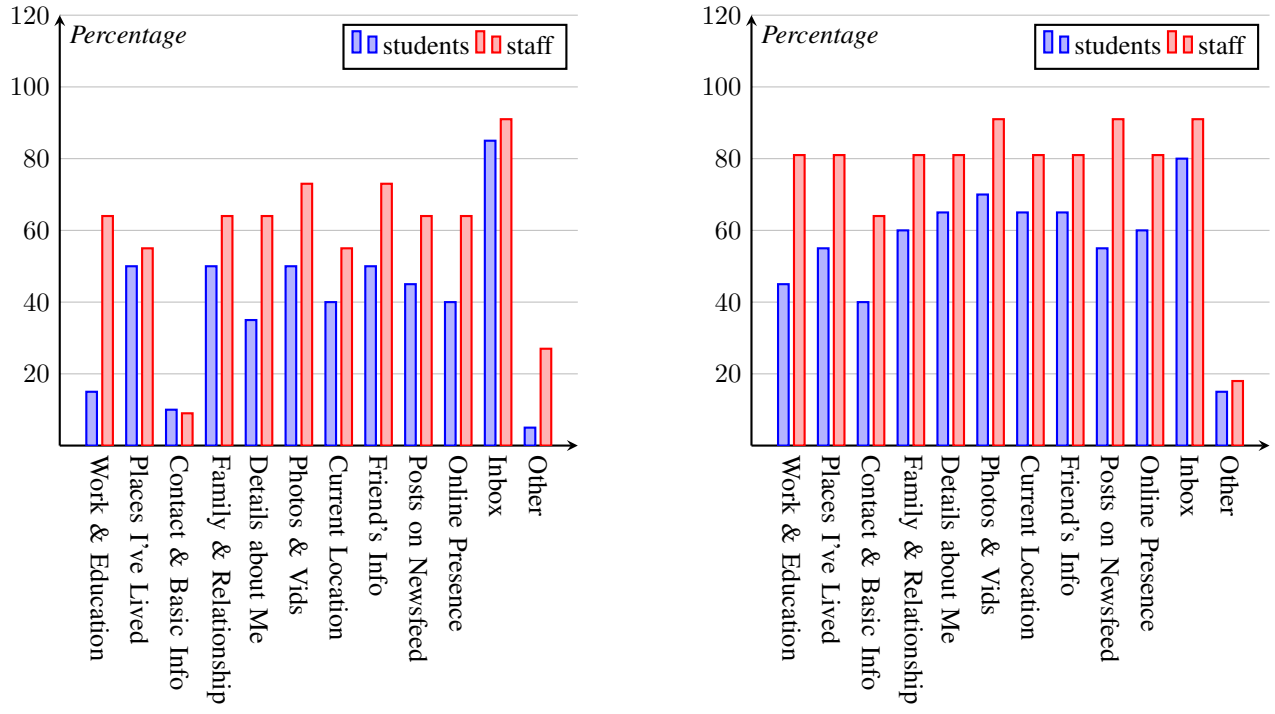
Participants are more conservative in sharing their contact information (e.g., mobile number, email ID) and physical address through their Facebook profile as compared with their personal information, like name, gender, relationship status, and political and religious views. Users may prioritize the information to make their sharing decision based on its immediate effect on possible privacy risks, where prior study identified users' tendency to care less about "distant" harms [11]. A majority of participants do not share their current location publicly in Facebook, which could be related to their privacy concerns [32], and declining popularity of location-sharing in social networking sites [42].

Users often create passwords based on their personal information [57, 58]. Personal information are also used to answer security questions, a widely-used method for fallback authentication [19, 29]. Our study reveals that at least one-third of participants publicly share their information about educational institutions, workplace, and current city; which could pose security risks to their online accounts, further elevated due to password reuse [20, 51], if those information are used for password creation.

Participants seem to weigh the sensitivity of information based on its level of details, and make their sharing decision accordingly, like many of them share their current city as a public information in Facebook profile, but do not share current physical address even with friends in Facebook. It is not clear though how the users set thresholds between varying level of details in personal information while making a sharing decision over online social network. Future investigations should shed light into this issue, and identify the privacy implications of users' mental model of information sharing with varying level of details in social networking sites.

B. Security and Privacy Practices in Facebook

Around one-sixth of our participants were victim of online scam incurring monetary loss, where one-third of participants reported leakage of their personal information to unwanted entities through social networking site and online activities. Social engineering attacks including phishing and online scams are on rise in recent years, especially through exploiting users' insecure online behavior including in Facebook [3, 18, 27, 33]. Our results support this argument, where the majority of participants do not check for a secure connection (e.g., https, padlock icon in URL bar) while visiting Facebook, nor hover



(a) Should Not Be Collected

(b) Should Not Be Shared

Fig. 1: **User Expectations**: Information that Should Not Be (a) *Collected* or (b) *Shared* by Any Facebook App

over a link (to be assured of the destination site) before clicking on it in their Facebook newsfeed.

We found interesting differences between student and staff population in what triggers them to check the security and privacy setting of their Facebook account. Our results suggest that students are more enthusiastic than staff population to learn about the latest changes in the security and privacy setting of Facebook when they receive an online notification of such changes. On the other hand, staffs are more likely than the students to check their security and privacy setting in Facebook when they come to know about a security or privacy breach at someone else's account. These findings have important implications on considering the demographic traits of users to design effective security and privacy notifications. For example, including a link to the relevant news of privacy breach with the notification could better motivate staff population to review the latest changes in Facebook's privacy setting. In other words, informing users about the vulnerabilities that motivated a change in the security or privacy setting could intrigue them to take full advantage of those new features in Facebook.

The majority of participants add unknown people to their friend list without verifying their identity. However, most of the participants do not review their friend list to identify fake or suspicious entity when their Facebook account is compromised, or they hear of similar incidents from friends or family members. It is not clear though if it is due to users' trust on their Facebook friends, or their ignorance in reviewing friend list to identify suspicious entity. In this regard, the rate of adding unknown friend is higher among student population as compared to staff members, where staff population reported higher confidence than the students that they do not have any fake people in their Facebook friend list.

Privacy is one of the noted concerns of the participants about the apps connected to their Facebook account. However, they did not remove any app yet due to privacy concern. So, it is possible that despite being worried about the data collection by their Facebook apps, they do not see it as an immediate threat to their online privacy. Or, users might perceive that if they stop using an app it also puts an end to the data collection, and further removal of that app is not needed to preserve their digital privacy. We could not conclude which of the above statements holds true for the participants, since we did not explicitly ask them about it. A further investigation in future research would give us clear insights into this issue.

C. Facebook Apps: Perceptions, Expectations, and Privacy Policy

In more than one-third of cases, participants' perceptions of information collection do not match with reality (i.e., apps' privacy policy). A closer look into those mismatches reveals that in most cases participants perceive that the information is not collected by an app, although that information is actually collected according to the app's privacy policy. For the mismatched perceptions of information deletion, participants mistakenly perceive in majority of cases that they would be allowed to delete their information collected by the apps. As

it appears, users have lack in understanding about the information collection and deletion policy of the apps connected to their Facebook account. In other words, they use these apps without fully realizing their privacy compromise.

The mismatched privacy perceptions of users implies that the privacy notice of Facebook apps need to attain higher efficacy and usability in informing them about the information collection, sharing, and deletion policy. Prior studies [9, 17, 31, 34, 53]proposed several techniques, including the use of icons, nutrition label, and comics to enhance the effectiveness and usability of privacy notices. On top of these techniques, our results suggest to highlight the aspects in privacy policy where we found a relatively higher mismatch between users' perceptions and apps' privacy policy. We also identified differences in mismatched privacy perceptions across gender, where female participants had a significantly higher 'NY' mismatch in terms of information collection, indicating the importance of designing personalized privacy notice by taking users' demographic traits into account.

The completeness in privacy policy is crucial to help users with making informed decision. Both the student and staff population reported strict expectations in terms of information sharing with other entities by the apps. They are more conservative in their expectations for information sharing, in comparison to information collection by the apps. Using those apps first-hand may make them comfortable with information collection, while they are concerned when their information is shared with unknown entities by the apps. So, the apps should clearly state their policy of information sharing in their privacy notice. However, our analysis of the privacy policy of 65 apps (reported by the participants) reveal that those apps fail to provide sufficient details or ignore mentioning about information sharing. Thus, users do not have a clear way to learn how their information is shared with other entities, despite their expectations that their information would not be shared by the Facebook apps.

D. Limitations and Future Work

Although our sample size is relatively small, we collected data on a total of 113 apps, including 65 unique apps across multiple categories, e.g., financial, identity, content. This study is based in an urban university, where most of the participants are educated. We note that users' privacy perceptions might be different in areas with a less-educated population. Since users' security and privacy perceptions are positively influenced by their knowledge and technical efficacy [23, 40, 49], we speculate that the privacy perceptions of users reported in this paper represent an upper bound. That means, the mismatches between users' privacy perceptions and the privacy policy of apps might be higher for the less-educated population than the results reported in this paper. Thus, the findings from this study might not be generalizable to the entire population, and might not directly contribute to the development of privacy theory. Rather, the implications of this study are more focused towards the design of usable and effective privacy notices through understanding users' privacy perceptions and expectations.

We conducted the study in a lab setting, which offers a controlled environment with minimal distraction for participants [5, 15]. Like prior lab-based studies conducted in a university environment (e.g., [1, 2, 22]), we recruited participants from the university's student and employee populations, where our participants have diverse demographic characteristics (see §IV-A for details).

Now that our results provide interesting insights into the mismatch between reality (i.e., app's privacy policy) and users' privacy perceptions of Facebook apps, in future work, we would conduct a large-scale online study using Amazon Mechanical Turk to get participants from diverse backgrounds.

In this study, if a participant had more than five apps connected to their Facebook account, we asked them to report five apps that they use most frequently. Facebook does not provide a feature to sort the apps based on a user's frequency of use or any metric. So, the participants had to rely on their memorability and self-judgment to select most frequently-used apps, where we could not verify if the reported apps are used most frequently by the participants. In addition, we had to omit a few apps from analysis due to spelling errors making the app names unrecognizable. Despite these issues, we compared users' perceptions with the privacy policy of 65 different Facebook apps.

In this paper, keeping consistent with the methodology suggested in prior work [43], we consider the privacy policy of a website or app to be representative of its data collection practices. Going further to identify the discrepancies between an app's privacy policy and its actual data collection practices is thus beyond the scope of this work. Future research to investigate such discrepancies would be valuable.

VI. Conclusion

The widespread use of social login to access third-party apps via a user's Facebook profile creates significant risks to user privacy. In this work, we studied Facebook users' information sharing practices and the security and privacy practices they use to protect their information. The varying privacy policies of Facebook apps could make it difficult for users to have a clear understanding about how individual apps are collecting and sharing data, as well as whether they enable users to delete any collected data. In this regard, we compared users' perceptions with the privacy policies of 65 different Facebook apps that are frequently used by our participants. Our analysis reveals the gaps between users' perceptions and these privacy policies, providing important directions for future research: (i) to gain a more in-depth understanding on this issue through a large-scale study with diverse groups of populations, and (ii) helping users to make informed decisions by designing usable and effective privacy notice and choice.

VII. Acknowledgement

We would like to thank RIT students and staff members for participating in this study. We would also like to thanks the reviewers for their valuable feedback.This material is based

upon work supported by the National Science Foundation under Awards No. 1949694 and 1949699.

REFERENCES

[1] M. N. Al-Ameen, K. Fatema, M. Wright, and S. Scielzo. The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pages 185–196, 2015.

[2] M. N. Al-Ameen, M. Wright, and S. Scielzo. Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2315–2324, 2015.

[3] M. Alsharnouby, F. Alaca, and S. Chiasson. Why phishing still works. *Int. J. Hum.-Comput. Stud.*, 82 (C):69–82, Oct. 2015. ISSN 1071-5819. doi: 10.1016/j.ijhcs.2015.05.005. URL http://dx.doi.org.ezproxy.rit.edu/10.1016/j.ijhcs.2015.05.005.

[4] A. I. Antón, J. B. Earp, and A. Reese. Analyzing website privacy requirements using a privacy goal taxonomy. In *Proceedings IEEE Joint International Conference on Requirements Engineering*, pages 23–31. IEEE, 2002.

[5] R. Biddle, S. Chiasson, and P. C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):1–41, 2012.

[6] D. Boyd and E. Hargittai. Facebook privacy settings: Who cares? *First Monday*, 15(8), July 2010. ISSN 13960466. doi: 10.5210/fm.v15i8.3086. URL https://journals.uic.edu/ojs/index.php/fm/article/view/3086.

[7] C. Cadwalladr and E. Graham-Harrison. Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach. *The Guardian*, 17:2018, Mar. 2018.

[8] J. Constine. Facebook Is Shutting Down Its API For Giving Your Friends Data To Apps, Apr. 2015. URL http://social.techcrunch.com/2015/04/28/facebook-api-shut-down/.

[9] L. F. Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, 10:273, 2012.

[10] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 581–590, New York, NY, USA, 2006. ACM. ISBN 1-59593-372-7. doi: 10.1145/1124772.1124861. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/1124772.1124861.

[11] P. Dolan, M. Hallsworth, D. Halpern, D. King, and I. Vlaev. Mindspace: influencing behaviour through public policy [internet]. london: Institute for government; c2010, Accessed: March 31, 2012.

[12] S. Egelman. My Profile is My Password, Verify Me!: The Privacy/Convenience Tradeoff of Facebook Connect. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 2369–2378, New York, NY, USA, Apr. 2013. ACM. ISBN 978-1-4503-1899-0. doi: 10.1145/2470654.2481328. URL http://doi.acm.org/10.1145/2470654.2481328.

[13] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 534. ACM, 2019.

[14] Facebook. Important Message from Facebook's White Hat Program, June 2013. URL https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766.

[15] S. Fahl, M. Harbach, Y. Acar, and M. Smith. On the ecological validity of a password study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–13, 2013.

[16] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen. Security Issues in Online Social Networks. *IEEE Internet Computing*, 15(4):56–63, July 2011. ISSN 1089-7801. doi: 10.1109/MIC.2011.50.

[17] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 321–340, Denver, CO, June 2016. USENIX Association. ISBN 978-1-931971-31-7. URL https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck.

[18] T. Halevi, J. Lewis, and N. Memon. Phishing, personality traits and facebook. *arXiv preprint arXiv:1301.7643*, 2013.

[19] A. Hang, A. De Luca, and H. Hussmann. I know what you did last week! do you?: Dynamic security questions for fallback authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1383–1392, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3145-6. doi: 10.1145/2702123.2702131. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/2702123.2702131.

[20] S. T. Haque, M. Wright, and S. Scielzo. A study of user password strategy for multiple accounts. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, CODASPY '13, pages 173–176, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-1890-7. doi: 10.1145/2435349.2435373. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/2435349.2435373.

[21] S. T. Haque, M. Wright, and S. Scielzo. Hierarchy of users web passwords: Perceptions, practices and susceptibilities. *International Journal of Human-Computer Studies*, 72(12):860–874, 2014.

[22] S. T. Haque, M. N. Al-Ameen, M. Wright, and S. Scielzo. Learning system-assigned passwords (up to 56 bits) in a single registration session with the methods of cognitive psychology. *Proc. USEC. The Internet Society*, 2017.

[23] I. Ion, R. Reeder, and S. Consolvo. ... no one can hack my mind: Comparing expert and non-expert security

practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[24] J. Isaak and M. J. Hanna. User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, 51(8):56–59, Aug. 2018. ISSN 0018-9162. doi: 10.1109/MC.2018.3191268.

[25] J. Isaak and M. J. Hanna. User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, 51(8):56–59, Aug. 2018. ISSN 0018-9162. doi: 10.1109/MC.2018.3191268.

[26] R. Jabee and M. A. Alam. Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). volume 144, pages 36–40, June . doi: 10.5120/ijca2016910174.

[27] T. N. Jagatic, N. A. Johnson, M. Jakobsson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, Oct. 2007. ISSN 0001-0782. doi: 10.1145/1290958.1290968. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/1290958.1290968.

[28] C. Jensen and C. Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 471–478. ACM, 2004.

[29] M. Just and D. Aspinall. Personal choice and challenge questions: A security and usability assessment. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 8:1–8:11, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-736-3. doi: 10.1145/1572532.1572543. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/1572532.1572543.

[30] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[31] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, pages 1573–1582, 2010.

[32] H.-S. Kim. What drives you to check in on facebook? motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior*, 54:397–406, Jan. 2016.

[33] G. H. Kirwan, C. Fullwood, and B. Rooney. Risk factors for social networking site scam victimization among malaysian students. *Cyberpsychology, Behavior, and Social Networking*, 21(2):123–128, Feb. 2018.

[34] B. Knijnenburg and D. Cherry. Comics as a medium for privacy notices. In *Twelfth Symposium on Usable Privacy and Security*, 2016.

[35] A. D. I. Kramer, J. E. Guillory, and J. T. Hancock. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111(24):8788–8790, June 2014. ISSN 0027-8424, 1091-6490. doi: 10.1073/pnas.1320040111. URL https://www.pnas.org/content/111/24/8788.

[36] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching johnny not to fall for phish. *ACM Trans. Internet Technol.*, 10(2):7:1–7:31, June 2010. ISSN 1533-5399. doi: 10.1145/1754393.1754396. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/1754393.1754396.

[37] L. Liu, E. Yu, and J. Mylopoulos. Security and privacy requirements analysis within a social setting. In *Proceedings. 11th IEEE International Requirements Engineering Conference, 2003.*, pages 151–161. IEEE, 2003.

[38] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: User expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, pages 61–70, New York, NY, USA, Nov. 2011. ACM. ISBN 978-1-4503-1013-0. doi: 10.1145/2068816.2068823. URL http://doi.acm.org/10.1145/2068816.2068823.

[39] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4):250–271, 2019.

[40] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 173–186. ACM, 2013.

[41] A. M. Mcdonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor. A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies*, pages 37–55. Springer, 2009.

[42] N. Miller. After Years of Challenges, Foursquare Has Found its Purpose – and Profits, Mar. 2017. URL https://www.entrepreneur.com/article/290543.

[43] A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang. Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online. pages 77–96, June 2016. ISBN 978-1-931971-31-7. URL https://www.usenix.org/conference/soups2016/technical-sessions/presentation/rao.

[44] E. M. Redmiles, N. Chachra, and B. Waismeyer. Examining the demand for spam: Who clicks? In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 212:1–212:10, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-5620-6. doi: 10.1145/3173574.3173786. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/3173574.3173786.

[45] M. Rouse. What Is Social Login?, Dec. 2014. URL https://whatis.techtarget.com/definition/social-login.

[46] N. Sadeh, A. Acquisti, T. D. Breaux, L. F. Cranor, A. M. McDonald, J. R. Reidenberg, N. A. Smith, F. Liu, N. C. Russell, F. Schaub, et al. The usable privacy policy project. In *Technical report, Technical Report, CMU-*

ISR-13-119. Carnegie Mellon University, 2013.

[47] K. M. Sathyendra, S. Wilson, F. Schaub, S. Zimmeck, and N. Sadeh. Identifying the provision of choices in privacy policy text. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, pages 2774–2779, 2017.

[48] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security*, pages 1–17, 2015.

[49] S. Seng, M. N. Al-Ameen, and M. Wright. Understanding users' decision of clicking on posts in facebook with implications for phishing. In *Workshop on Technology and Consumer Protection (ConPro 18)*, May 2018.

[50] E. Stewart. What you need to know about Facebooks new privacy settings. https://www.vox.com/technology/2018/4/18/17251480/facebook-privacy-scandal-changes-europe-gdpr, 2018.

[51] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 243–255, Menlo Park, CA, July 2014. USENIX Association. ISBN 978-1-931971-13-3. URL https://www.usenix.org/conference/soups2014/proceedings/presentation/stobert.

[52] N. Stokes. Should You Use Facebook or Google to Log In to Other Sites?, May 2017. URL https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/.

[53] M. Tabassum, A. Alqhatani, M. Aldossari, and H. Richter Lipford. Increasing user attention with a comic-based policy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 200:1–200:6, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-5620-6. doi: 10.1145/3173574.3173774. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/3173574.3173774.

[54] A. M. Torres and D. O'Brien. Social networking and online privacy: Facebook users' perceptions. In *Irish Journal of Management*, volume 31, pages 63–87, Feb. 2012. URL https://aran.library.nuigalway.ie/handle/10379/4059.

[55] M. Tsikerdekis and S. Zeadally. Online deception in social media. *Commun. ACM*, 57(9):72–80, Sept. 2014. ISSN 0001-0782. doi: 10.1145/2629612. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/2629612.

[56] V. K. Tuunainen, O. Pitkanen, and M. Hovi. Users' Awareness of Privacy on Online Social Networking Sites - Case Facebook. page 17, Jan. 2009.

[57] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. "i added '!' at the end to make it secure": Observing password creation in the lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 123–140, Ottawa, July 2015. USENIX Association. ISBN 978-1-931971-249. URL https://www.usenix.org/conference/soups2015/proceedings/presentation/ur.

[58] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 3748–3760, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-3362-7. doi: 10.1145/2858036.2858546. URL http://doi.acm.org.ezproxy.rit.edu/10.1145/2858036.2858546.

APPENDIX

	Do Not Share	**Friends**	**Public**
Full Name	3	6	22
Current Workplace	6	13	12
Previous Workplaces	7	14	10
College	3	13	15
High School	5	14	12
Professional Skills	14	11	6
Current City	6	14	11
Hometown	7	15	9
Other Places You've Lived	12	14	5
Mobile Number	25	6	0
Email Address	21	9	1
Other Phone Number	27	4	0
Current Physical Address	27	4	0
Public Key	28	3	0
Personal Website	20	8	3
Other SNS	19	11	1
Birthday	8	19	4
Birthyear	12	15	4
Gender	4	13	14
Languages	16	9	6
Religious Views	17	9	5
Political Views	17	10	4
Who You're Interested In	18	9	4
Current Relationship Status	13	14	4
Spouse	12	17	2
Parents	9	20	2
Siblings	8	19	4
Others	11	16	4
About You	10	15	6
Name Pronunciation	17	8	6
Other Names	18	7	6
Favorite Quotes	15	12	4

TABLE IX: Users' Information Sharing Settings

Security and Privacy Scenario	Student	Staff
Creating a secure password for my Facebook account	5.9	5.5
Having no fake people in my friend list	5.4	6.4
Taking necessary precautions to protect my Facebook account from being compromised/hacked	5.6	5.4
Understanding the latest security and privacy settings/features in Facebook	5.2	4.3
Protecting my personal information in Facebook from unauthorized access by third-party applications	5.6	5.1
Not clicking on malicious posts, links, or videos	6.4	5.8
Sharing information about others in Facebook that will NOT harm their privacy	6.1	6.0
Protecting my device from malware (e.g. a computer virus) spreading through Facebook	6.4	4.7
Taking necessary actions to regain my account if it is compromised/hacked	5.7	5.1
Protecting my personal information, photos, or videos in Facebook from the people whom I don't want to share them with	6.2	5.4

TABLE X: Users' Self-Efficacy in Maintaining the Security and Privacy of their Facebook Account (7-Point Likert Scale)

		Work & Education							Places I Have Lived							Contact & Basic Info					
			MATCH			MISMATCH			MATCH			MISMATCH				MATCH			MISMATCH		
Main Category	Subcategory	Total	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%
Finance	Primary	6	0	3	50.0%	3	0	50.0%	1	5	100.0%	0	0	0.0%	4	0	66.7%	0	2	33.3%
	Secondary	15	0	10	66.7%	5	0	33.3%	5	1	40.0%	1	8	60.0%	10	0	66.7%	0	5	33.3%
	SUBTOTAL	**21**	**0**	**13**	**61.9%**	**8**	**0**	**38.1%**	**6**	**6**	**57.1%**	**1**	**8**	**42.9%**	**14**	**0**	**66.7%**	**0**	**7**	**33.3%**
Identity/Personal	Communication	5	0	5	100.0%	0	0	0.0%	0	0	0.0%	0	5	100.0%	5	0	100.0%	0	0	0.0%
	Fitness	4	0	2	50.0%	0	2	50.0%	1	0	25.0%	1	2	75.0%	4	0	100.0%	0	0	0.0%
	Q&A	6	0	1	16.7%	5	0	83.3%	0	3	50.0%	3	0	50.0%	5	0	83.3%	0	1	16.7%
	Social Networking	16	1	11	75.0%	4	0	25.0%	6	7	81.3%	1	2	18.8%	14	0	87.5%	0	2	12.5%
	SUBTOTAL	**31**	**1**	**19**	**64.5%**	**9**	**2**	**35.5%**	**7**	**10**	**54.8%**	**5**	**9**	**45.2%**	**28**	**0**	**90.3%**	**0**	**3**	**9.7%**
Content	Entertainment	23	0	18	78.3%	2	3	21.7%	4	0	17.4%	0	19	82.6%	10	0	43.5%	0	13	56.5%
	Listing	15	0	10	66.7%	4	1	33.3%	4	0	26.7%	0	11	73.3%	14	0	93.3%	0	1	6.7%
	News	3	0	0	0.0%	3	0	100.0%	2	0	66.7%	1	0	33.3%	3	0	100.0%	0	0	0.0%
	SUBTOTAL	**41**	**0**	**28**	**68.3%**	**9**	**4**	**31.7%**	**10**	**0**	**24.4%**	**1**	**30**	**75.6%**	**27**	**0**	**65.9%**	**0**	**14**	**34.1%**
Other	Game	11	0	9	81.8%	2	0	18.2%	0	6	54.5%	0	5	45.5%	9	0	81.8%	0	2	18.2%
	Utility	9	1	6	77.8%	1	1	22.2%	1	1	22.2%	0	7	77.8%	7	0	77.8%	0	2	22.2%
	SUBTOTAL	**20**	**1**	**15**	**80.0%**	**3**	**1**	**20.0%**	**1**	**7**	**40.0%**	**0**	**12**	**60.0%**	**16**	**0**	**80.0%**	**0**	**4**	**20.0%**
	TOTAL	**113**	**2**	**75**	**68.1%**	**29**	**7**	**31.9%**	**24**	**23**	**41.6%**	**7**	**59**	**58.4%**	**85**	**0**	**75.2%**	**0**	**28**	**24.8%**

TABLE XI: Information Collected by Facebook Apps: Users' Perceptions Compared to Privacy Policy - Part 1

		Family & Relationship							Details about Me							Photos & Vids					
			MATCH			MISMATCH			MATCH			MISMATCH				MATCH			MISMATCH		
Main Category	Subcategory	Total	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%
Finance	Primary	6	1	1	33.3%	0	4	66.7%	3	0	50.0%	0	3	50.0%	0	6	100.0%	0	0	0.0%
	Secondary	15	0	13	86.7%	1	1	13.3%	6	1	46.7%	5	3	53.3%	0	14	93.3%	1	0	6.7%
	SUBTOTAL	**21**	**1**	**14**	**71.4%**	**1**	**5**	**28.6%**	**9**	**1**	**47.6%**	**5**	**6**	**52.4%**	**0**	**20**	**95.2%**	**1**	**0**	**4.8%**
Identity/Personal	Communication	5	0	0	0.0%	0	5	100.0%	2	0	40.0%	0	3	60.0%	2	0	40.0%	0	3	60.0%
	Fitness	4	0	2	50.0%	2	0	50.0%	1	0	25.0%	2	1	75.0%	0	4	100.0%	0	0	0.0%
	Q&A	6	0	0	0.0%	0	6	100.0%	3	0	50.0%	0	3	50.0%	0	0	0.0%	0	6	100.0%
	Social Networking	16	4	4	50.0%	0	8	50.0%	13	0	81.3%	1	2	18.8%	10	2	75.0%	1	3	25.0%
	SUBTOTAL	**31**	**4**	**6**	**32.3%**	**2**	**19**	**67.7%**	**19**	**0**	**61.3%**	**3**	**9**	**38.7%**	**12**	**6**	**58.1%**	**1**	**12**	**41.9%**
Content	Entertainment	23	2	8	43.5%	1	12	56.5%	13	2	65.2%	2	6	34.8%	0	19	82.6%	1	3	17.4%
	Listing	15	1	4	33.3%	0	10	66.7%	11	2	86.7%	1	1	13.3%	0	12	80.0%	2	1	20.0%
	News	3	0	2	66.7%	1	0	33.3%	1	0	33.3%	2	0	66.7%	0	3	100.0%	0	0	0.0%
	SUBTOTAL	**41**	**3**	**14**	**41.5%**	**2**	**22**	**58.5%**	**25**	**4**	**70.7%**	**5**	**7**	**29.3%**	**0**	**34**	**82.9%**	**3**	**4**	**17.1%**
Other	Game	11	0	9	81.8%	1	1	18.2%	3	5	72.7%	1	2	27.3%	0	8	72.7%	3	0	27.3%
	Utility	9	1	4	55.6%	1	3	44.4%	3	4	77.8%	2	0	22.2%	0	7	77.8%	2	0	22.2%
	SUBTOTAL	**20**	**1**	**13**	**70.0%**	**2**	**4**	**30.0%**	**6**	**9**	**75.0%**	**3**	**2**	**25.0%**	**0**	**15**	**75.0%**	**5**	**0**	**25.0%**
	TOTAL	**113**	**9**	**47**	**49.6%**	**7**	**50**	**50.4%**	**59**	**14**	**64.6%**	**16**	**24**	**35.4%**	**12**	**75**	**77.0%**	**10**	**16**	**23.0%**

TABLE XII: Information Collected by Facebook Apps: Users' Perceptions Compared to Privacy Policy - Part 2

		Current Location							Friends' Info							Posts on Newsfeed					
			MATCH			MISMATCH			MATCH			MISMATCH				MATCH			MISMATCH		
Main Category	Subcategory	Total	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%
Finance	Primary	6	0	4	66.7%	1	1	33.3%	4	1	83.3%	0	1	16.7%	0	6	100.0%	0	0	0.0%
	Secondary	15	5	0	33.3%	1	9	66.7%	0	9	60.0%	0	6	40.0%	0	14	93.3%	1	0	6.7%
	SUBTOTAL	**21**	**5**	**4**	**42.9%**	**2**	**10**	**57.1%**	**4**	**10**	**66.7%**	**0**	**7**	**33.3%**	**0**	**20**	**95.2%**	**1**	**0**	**4.8%**
Identity/Personal	Communication	5	0	0	0.0%	0	5	100.0%	1	0	20.0%	0	4	80.0%	0	5	100.0%	0	0	0.0%
	Fitness	4	0	2	50.0%	0	2	50.0%	1	2	75.0%	0	1	25.0%	0	4	100.0%	0	0	0.0%
	Q&A	6	0	5	83.3%	1	0	16.7%	0	5	83.3%	1	0	16.7%	0	4	66.7%	2	0	33.3%
	Social Networking	16	7	2	56.3%	0	7	43.8%	3	3	37.5%	1	9	62.5%	1	13	87.5%	2	0	12.5%
	SUBTOTAL	**31**	**7**	**9**	**51.6%**	**1**	**14**	**48.4%**	**5**	**10**	**48.4%**	**2**	**14**	**51.6%**	**1**	**26**	**87.1%**	**4**	**0**	**12.9%**
Content	Entertainment	23	3	11	60.9%	1	8	39.1%	8	3	47.8%	1	11	52.2%	0	17	73.9%	3	3	26.1%
	Listing	15	7	2	60.0%	0	6	40.0%	1	3	26.7%	0	11	73.3%	0	12	80.0%	2	1	20.0%
	News	3	1	1	66.7%	1	0	33.3%	0	3	100.0%	0	0	0.0%	0	3	100.0%	0	0	0.0%
	SUBTOTAL	**41**	**11**	**14**	**61.0%**	**2**	**14**	**39.0%**	**9**	**9**	**43.9%**	**1**	**22**	**56.1%**	**0**	**32**	**78.0%**	**5**	**4**	**22.0%**
Other	Game	11	1	6	63.6%	1	3	36.4%	2	0	18.2%	1	8	81.8%	0	9	81.8%	2	0	18.2%
	Utility	9	5	1	66.7%	1	2	33.3%	0	6	66.7%	2	1	33.3%	0	7	77.8%	2	0	22.2%
	SUBTOTAL	**20**	**6**	**7**	**65.0%**	**2**	**5**	**35.0%**	**2**	**6**	**40.0%**	**3**	**9**	**60.0%**	**0**	**16**	**80.0%**	**4**	**0**	**20.0%**
	TOTAL	**113**	**29**	**34**	**55.8%**	**7**	**43**	**44.2%**	**20**	**35**	**48.7%**	**6**	**52**	**51.3%**	**1**	**94**	**84.1%**	**14**	**4**	**15.9%**

TABLE XIII: Information Collected by Facebook Apps: Users' Perceptions Compared to Privacy Policy - Part 3

		Online Presence							Inbox							Other					
			MATCH			MISMATCH			MATCH			MISMATCH				MATCH			MISMATCH		
Main Category	Subcategory	Total	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%	YY	NN	%	YN	NY	%
Finance	Primary	6	1	0	16.7%	0	5	83.3%	0	6	100.0%	0	0	0.0%	0	0	0.0%	0	6	100.0%
	Secondary	15	5	0	33.3%	0	10	66.7%	0	15	100.0%	0	0	0.0%	1	0	6.7%	0	14	93.3%
	SUBTOTAL	**21**	**6**	**0**	**28.6%**	**0**	**15**	**71.4%**	**0**	**21**	**100.0%**	**0**	**0**	**0.0%**	**1**	**0**	**4.8%**	**0**	**20**	**95.2%**
Identity/Personal	Communication	5	0	0	0.0%	0	5	100.0%	0	4	80.0%	1	0	20.0%	0	5	100.0%	0	0	0.0%
	Fitness	4	0	1	25.0%	0	3	75.0%	0	4	100.0%	0	0	0.0%	1	0	25.0%	0	3	75.0%
	Q&A	6	4	0	66.7%	0	2	33.3%	0	4	66.7%	2	0	33.3%	0	6	100.0%	0	0	0.0%
	Social Networking	16	2	3	31.3%	0	11	68.8%	0	15	93.8%	1	0	6.3%	0	4	25.0%	0	12	75.0%
	SUBTOTAL	**31**	**6**	**4**	**32.3%**	**0**	**21**	**67.7%**	**0**	**27**	**87.1%**	**4**	**0**	**12.9%**	**1**	**15**	**51.6%**	**0**	**15**	**48.4%**
Content	Entertainment	23	5	7	52.2%	3	8	47.8%	0	22	95.7%	1	0	4.3%	2	7	39.1%	3	11	60.9%
	Listing	15	5	0	33.3%	0	10	66.7%	0	14	93.3%	1	0	6.7%	1	5	40.0%	0	9	60.0%
	News	3	1	0	33.3%	0	2	66.7%	0	3	100.0%	0	0	0.0%	0	0	0.0%	0	3	100.0%
	SUBTOTAL	**41**	**11**	**7**	**43.9%**	**3**	**20**	**56.1%**	**0**	**39**	**95.1%**	**2**	**0**	**4.9%**	**3**	**12**	**36.6%**	**3**	**23**	**63.4%**
Other	Game	11	5	0	45.5%	0	6	54.5%	0	11	100.0%	0	0	0.0%	0	0	0.0%	0	11	100.0%
	Utility	9	0	5	55.6%	1	3	44.4%	0	9	100.0%	0	0	0.0%	0	3	33.3%	1	5	66.7%
	SUBTOTAL	**20**	**5**	**5**	**50.0%**	**1**	**9**	**50.0%**	**0**	**20**	**100.0%**	**0**	**0**	**0.0%**	**0**	**3**	**15.0%**	**1**	**16**	**85.0%**
	TOTAL	**113**	**28**	**16**	**38.9%**	**4**	**65**	**61.1%**	**0**	**107**	**94.7%**	**6**	**0**	**5.3%**	**5**	**30**	**31.0%**	**4**	**74**	**69.0%**

TABLE XIV: Information Collected by Facebook Apps: Users' Perceptions Compared to Privacy Policy - Part 4