Exploring privacy concerns and violations for smartphone notifications

ANONYMOUS AUTHOR(S)*

Notifications are one of the most important features of mobile devices. Multitudes of notifications are delivered to users everyday. These notifications often carry sensitive content like financial information, private messages, business information etc. To understand privacy concerns and violations related to notification content and delivery, we conducted a study in which participants (n = 213) described their preferences and practices regarding smartphone notifications. Majority of the participants (63%) reported at least one negative experience connected to notifications. We report on various privacy violations arising due to notifications, such as unwanted information disclosures, information leaks when sharing devices, and inopportune intrusion. Our work contributes to a better understanding of privacy risks presented by mobile device notifications and points to various design suggestions for notification delivery mechanisms that are more sensitive to privacy concerns.

CCS Concepts: • **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: smartphone notifications, user privacy, information disclosures, device sharing, intrusion

ACM Reference Format:

Anonymous Author(s). 2018. Exploring privacy concerns and violations for smartphone notifications. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Notifications are an important method of information delivery on mobile devices. The device operating system as well as third party apps generate notification to alert users about a number of matters such as incoming content, reminders for upcoming events and tasks, availability of software updates, warnings regarding data access, and so on. On average, smartphone users receive more than 50 notifications per day [36, 37], making notifications more pervasive and common than phone calls.

While the information contained in the notifications is useful, it can also be privacy sensitive. For instance, notifications may contain personally identifiable information or confidential discussions that users do not wish to divulge to other parties. Since notifications are typically triggered by the actions of other parties, users cannot predict when a notification pops up. If notifications containing private information are displayed when a user is in a situation in which the mobile device is shared with someone else or the device screen is easily viewable by other parties, users experience privacy violations owing to undesirable information disclosure. Moreover, notifications that interrupt the user at inopportune moments can violate privacy by intruding upon solitude, a facet of privacy [40].

Although information disclosures and privacy concerns have been investigated in the specific context of email notifications [22], there has not yet been a systematic and comprehensive investigation of privacy aspects of mobile-device notifications in general. We aim to fill this gap by investigating user preferences and practices regarding

Manuscript submitted to ACM

notifications received via mobile devices from a privacy point of view. Specifically, we addressed the following research questions:

- **RQ1:** What are the privacy considerations associated with notifications received via mobile devices?
- **RQ2:** How do device mechanisms to control notifications (e.g., silent mode, notification delivery preferences, etc.) pertain to privacy aspects related to notifications?

We sought to answer the above questions using an online questionnaire administered via the Amazon Mechanical Turk (AMT) platform. The questionnaire covered device settings, device-sharing behavior, notification content, and contextual aspects related to notification delivery and reception. Based on questionnaire responses of 213 participants, we found that notifications on mobile devices do indeed impact the privacy of the recipients and potentially of those whose information might be included in the notification. We further uncovered that privacy threats of notifications are particularly high in situations that involve device sharing. The contribution of our work lies in complementing prior research on notifications and extending it to the context of mobile devices. Our findings contribute to an improved understanding of privacy concerns connected to mobile device notifications, and the insight can be applied to enhance notification delivery to avoid privacy violations.

In the following sections, we describe notification delivery mechanisms typical of current smartphones, provide an overview of notification customization functionality, and explain the method we used to conduct our study. We then present our empirical findings and apply them to propose privacy-enhancing improvements to the delivery of notifications on mobile devices.

2 RELATED WORK

Our study broadly lies at the intersection of individual privacy concerns, privacy issues specific to mobile devices, and privacy aspects connected to notifications. We cover the salient work in each space in turn.

2.1 Individual Privacy Concerns

Lacking a universal definition due to its highly contextual and nuanced nature, privacy has been conceptualized in a number of ways. Altman [4] states different aspects of Individual privacy concerns are connected to the "interplay of people, their social world, the physical environment, and the temporal nature of social phenomena" [4]. As a result of such contextual and nuanced nature privacy lacks a universal definition and has been conceptualized in a number of ways. For instance, Westin's [48] influential characterization describes privacy as being connected to four states: Solitude, Intimacy, Anonymity, and Reserve. As summarized by Margulis [25], Solitude is being free from observation by others; Intimacy refers to small group seclusion to achieve a close, relaxed, frank relationship among group members; Anonymity provides freedom from identification and from surveillance in public places and for public acts; and Reserve is based on the desire to limit disclosures to others. Solove [40] has described how everyday activities are connected conceptual characterizations of privacy such as 'intrusion' of solitude: "intrusion involves invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy" (p. 549). Digital intrusions, such as spam, telemarketing, unwanted or inopportune notifications, etc., violate privacy by disrupting solitude, interrupting ongoing activities, and creating discomfort much the same as intrusions experienced in physical spaces [40]. Our study examines how notification content and delivery are connected to these various facets of privacy.

To measure individual privacy concerns in the digital context, researchers have developed standardized instruments pertaining to information privacy, such as the Concern for Information Privacy (CFIP) [39] scale later refined to the Internet Users' Information Privacy Concerns (IUIPC) scale [24]. Specifically in the realm of technology-mediated interpersonal interactions, researchers have been studying digital privacy preferences and practices through the lenses of information disclosure (e.g., [31]) and self presentation (e.g., kramer2011online), covering a variety of applications, such as workplace collaboration (e.g., [32]), messaging platforms (e.g., [23]), location sharing systems (e.g., [33]), social media (e.g., [49]), etc. The findings of these investigations provide empirical confirmation of the contextual variation in privacy preferences and practices and reveal that privacy violations are often a result of violations of contextual needs and expectations [30]. Therefore, our study examines how privacy aspects connected to notifications might be influenced by contextual factors, such as time and place of delivery, type of app, etc.

2.2 Privacy in Mobile Devices

As the introduction of the smartphone has led to mobile devices becoming an integral part of everyday life, Human Computer Interaction (HCI) researchers have focused specifically on understanding privacy considerations pertaining to mobile devices. For instance, to help researchers measure individual privacy concerns specifically for the context of smartphone apps, Xu et al. [50] developed the Mobile Users' Information Privacy Concerns (MUIPC) scale containing the constructs of 'perceived surveillance,' 'perceived intrusion' experienced because of the use of mobile devices and apps. In addition, researchers have proposed a number of enhancements to support user privacy needs and expectations when using mobile devices and applications. For instance, researchers have developed techniques to raise user awareness regarding privacy-affecting operations of devices and apps (e.g., [8]) and proposed "soft paternalistic" [7] approaches that nudge users to make privacy-protecting decisions [3, 6, 28].

In a complimentary vein to improve privacy protection, researchers have explored more effective mechanisms for device locking, such as context-sensitive screen locks [29] and progressive authentication [38]. Further, tools such as ColorSnakes [16] and XSide [13] protect authentication entry against the threat of shoulder surfing in real-world use [14]. Relatedly, Von Zezschwitz et al. [42] designed a photo obfuscation technique to prevent privacy leaks when jointly browsing photo albums on a smartphone with others in order to locate and show them specific photos, and Ali et al. [2] developed the iAlert tool to alert users to the presence of bystanders who might be able to view the screen of the user's device.

However, none of these efforts have explicitly focused on notification features of mobile devices. Moreover, the various tools and techniques do not taken into account device access by others besides bystanders as is the case when sharing the device, a common practice [26] that has been identified to impinge upon privacy [17, 21], especially in less individualistic societies [1]. Our study aims to shed light on privacy concerns with notifications received when sharing the device with others.

2.3 Privacy Aspects of Notifications

Notification mechanisms have been a feature operating systems and applications for several decades. While researchers have paid particular attention to the interruptions caused by notifications, these investigations have been primarily concerned with measuring and avoiding the negative impact of these interruptions on productivity and affect by attempting to identify opportune moments when a user might be interruptible and receptive to the notification (e.g., [10, 15, 27, 34, 51]). However, research on the privacy aspects of notifications apart from the disruption of interruptions is still relatively scant. Vardhan et al. [41] designed a classifier to determine whether a notification is likely

to be private based on the title, content, and the name of the application that generated the notification. The classifier can be adjusted based on user feedback regarding whether a notification should be treated as private. However, the classifier does not take into account how privacy judgments and classifications might be affected by contextual factors, such as time, place, delivery mode, etc. A recent study by Kim et al. [22] found that the context in which notifications are received on a mobile device does impact the likelihood and severity of privacy risk of undesirable information disclosure. However, Kim et al. [22]'s study was narrowly scoped to include a sample from a single organization and considered only email notifications in the context of in-person workplace meetings. Our study builds on the works of Vardhan et al. [41] and Kim et al. [22] by broadening the scope to cover multiple facets of privacy aspects connected to all types of notifications received in a diverse variety of contexts. Moreover, our study includes consideration for the privacy of other parties whose information is present in the notification.

3 METHOD

We designed a questionnaire to address the research questions outlined in Section 1. All study materials and procedures (see Supplementary Material) were approved by our institution's Institutional Review Board (IRB).The following subsections describe the design and deployment of the study, provide an overview of our sample, and specify our data analysis approach.

3.1 Questionnaire Design

We designed a questionnaire that asked smartphone users about their preferences and practices related to notifications received on their devices. Apart from inquiring about device characteristics and preferences settings related to notifications, we included questions regarding the context in which notifications were received and read and practices related to sharing the device with others. For delving deeper into these aspects via tighter coupling between general preferences and practices and specifics of particular notifications, we asked questions related to the latest notification, such as delivery mode, context, privacy concern, etc. Since privacy violations are negative experiences, we next asked participants to elaborate on their most negative experience connected to smartphone notifications. Such an approach allowed us to capture a broad set of negative experiences without explicitly priming and constraining people by using the term 'privacy.' We then asked for the level of concern for someone else reading notification content for a variety of common app types (i.e., Social media, Calendar, E-mail, Banking and payments, Health and fitness, and Dating).

Following the above core questions related to our research questions, we used standard scales from the literature as measures of baseline privacy concern when using mobile devices [50] and general technical expertise [5]). The questionnaire concluded with by collecting standard demographic information. Wherever applicable, we provided the option to enter open-ended explanations.

We tested and iteratively refined the questionnaire via multiple small-scale pilots involving other student and postdoctoral researchers at our institution as well as personal contacts of the authors. The pilots served to ensure that the questions were easily comprehensible and the questionnaire operation was error-free.

3.2 Study Deployment

We deployed the study as a Human Intelligence Task (HIT) available on the AMT crowd work platform between November 12, 2020 and December 1, 2020. Since privacy is known to vary by culture, we limited participation to those from the United States to limit the impact of the answers being affected by cultural variation. We further restricted

participation to those with a task approval rating of 95% of higher with at least 50 completed tasks to maximize the chances of receiving high-quality responses.

Upon accepting the HIT, participants were provided a link to the online questionnaire implemented via the Qualtrics platform. Upon reading the initial study information and consenting to participate, participants proceeded to complete the questionnaire that began with a question to gauge the commitment to providing thoughtful answers. No questions were mandatory; participants could choose to skip any question they did not wish to answer. Upon completing the questionnaire, participants received a randomly-generated unique code to be entered on AMT as proof of completion. All those who answered the questionnaire attentively and entered a valid code were compensated US $1.80 for their participation. Based on an mean study completion time of 19 minutes, the compensation translates to roughly $6/hour which is typical of AMT based studies and in line with the minimum wage for our state.

3.3 Sample Characteristics

We obtained responses from individuals covering a broad age range from 18 to 70 with a median age of 35 and mean of 36. Most (87%; $n = 187$) reported living the United States for more than 10 years. Participants were split 61% ($n = 130$) and 38% ($n = 81$) between men and women respectively with two participants choosing not to report gender. While nearly three quarters of the participants were White Caucausians (74%; $n = 158$), the remainder of the sample included individuals from a variety of ethnic backgrounds: American Indian or Native American ($n = 3$), Asian($n = 14$), Black or African American($n = 24$), Hispanic($n = 7$), Native Hawaiian or Pacific Islander ($n = 3$). One participant reported being multi-ethnic, and two chose not to report ethnicity. Participants reported a wide variety of professional backgrounds, such as construction, management, Information Technology, media production, art, pharmaceutical, etc. Nearly all participants (93%; $n = 198$) reported completed at least some college education, with 80% ($n = 171$) having completed a Bachelor's degree or higher. A majority of the participants were married (63%, $n = 134$), while roughly 1/3rd were (31%; $n = 66$) single and the remaining 6% were separated, divorced, widowed. Most participants (72%; $n = 153$) lived in households of three or more people, with the remaining either living alone (15%; $n = 33$) or with one other person (13%; $n = 27$).

3.4 Data Analysis

We first examined the data to flag and filter invalid responses. Of the 275 total responses, we excluded 60 for failing any of the attention checks embedded within the questionnaire and/or not committing to providing thoughtful answers. We filtered out two additional responses because they originated from IP addresses outside the United States. After filtering, we were left with 213 complete and valid responses that we analyzed to derive our findings.

Given the exploratory nature of our study, we used relevant descriptive statistics for examining the quantitative variables captured by the questionnaire. Where applicable, we used appropriate inferential statistics to examine the statistical significance of claims connected to numeric variables. Since the data was not normally distributed, we used non-parametric statistical tests, such as Kruskall-Wallis test and Mann-Whitney U test.

We analyzed qualitative data collected via open-ended questions by employing three independent coders, one of whom was the first author of the paper. The first author generated an initial list of codes based on a detailed examination of the responses and consultation with the second author. The three coders then independently used thematic analysis techniques [9] to code all open-ended responses according to the initial list of codes. During the independent coding process, coders were free to suggest refinements to the existing codes and add codes to the initial list. After initial independent coding, we consolidated the three sets of codes, flagged disagreements, and held a discussion among the

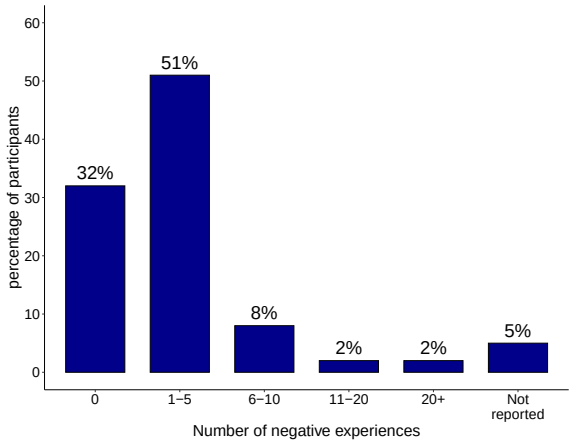


Fig. 1. Percentage of participants reporting the number of negative experiences due to smartphone notifications.

three coders to resolve the discrepancies. The discussion resulted in renaming some of the initial codes and adding a few new ones, culminating in full agreement among the three coders. We then clustered similar codes into higher-level themes connected to concepts taken from the literature [40, 48] (see Section 2.1).

4 FINDINGS

In this section, we elaborate upon user privacy violations and concerns due to smartphone notifications. We examined how these concerns vary based on content from different types of app categories and relate to contexts in which others parties can view the device screen (RQ1). We then highlight the interplay between privacy concerns and violations with device-control features and technical expertise (RQ2).

4.1 Privacy Concerns and Violations due to Smartphone Notifications

We studied privacy breaches and concerns due to smartphone notifications as part of negative experiences with notification. A majority of the participants (63%; $n = 134$) reported facing at least one negative experience due to smartphone notifications (see Figure 1). A little more than half of the participants (51%; $n = 109$) faced 1-5 instances of negative experiences. To understand how these negative experiences relate to privacy breaches, we analyzed the 95 open-ended responses in which participants elaborated on the most negative experience. Table 1 presents the themes that emerged from the responses.

It can be seen that the four broad privacy violations connected to smartphone notifications (RQ1) are:

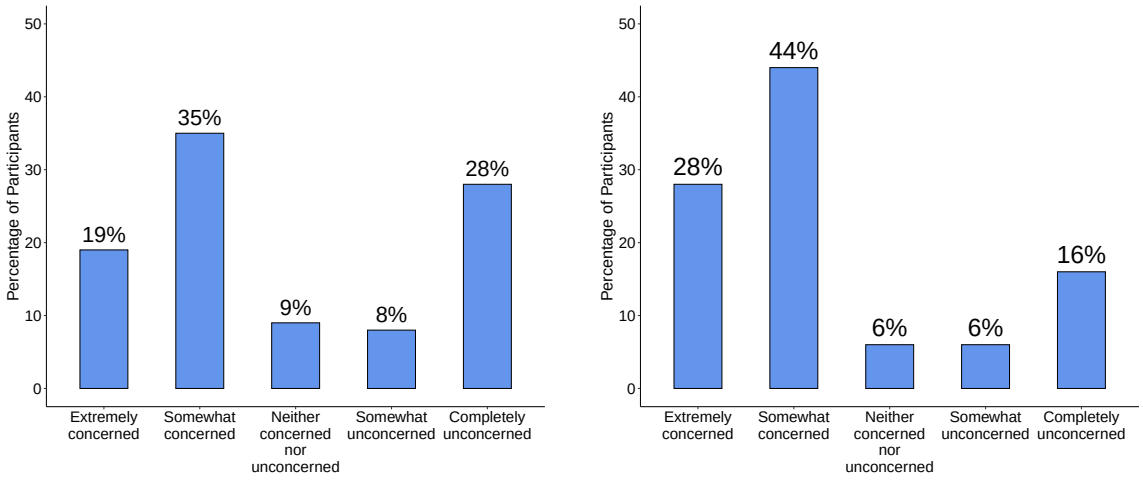
(1) unintended information disclosures;
(2) privacy breaches during device sharing or screen cast / projection;
(3) intrusions in task, personal solitude, and digital space; and
(4) invasions of social intimacy.

To understand if the instances of negative experiences due to notifications are associated with the type of smartphone operating system, we performed a Mann-Whitney U Test with number of negative experiences as dependent variable

Table 1. Categorization of privacy violations due to smartphone notifications.

Theme	Code	Count	Example Comments
Information disclosure	Private content disclosed	21	"My girlfriend saw a message from one of my friends that was too private for her concern." (P 96)
	Inappropriate content disclosed	9	"Someone sent me inappropriate photos without permission and my spouse seen them. She thought I was cheating." (P 109)
	Content about third person was disclosed	2	"One of my friends read a message that was about her, and it made her upset." (P 47)
Privacy breach during shared device use	Device was with someone else	7	"When my phone was with my sibling my partner sent me a romantic message. My sister saw that message, which was a negative experience." (P 143)
	Device screen was cast/projected	2	"When I was working on something for work where i had to cast my device screen for others to see. The notification was highly personal.," (P 45)
Intrusion	Digital intrusion (with undesired content, malware)	25	"One time i clicked the link on the notification received without studying in details resulted phone affected with virus." (P 42), "I have little experience that i receive fake notifications from unwanted websites" (P 154)
	Intrusion in personal solitude	4	"The most negative experience was being woken up by notifications in the middle of the night and not being able to fall back asleep even though I had work in the morning." (P 92)
	Felt uncomfortable and uneasy due to notification	9	"I kept on getting advertisement notifications – repeatedly one after another – from a shopping app I had, that were really not related to the app itself, and would not stop unless I would open the app right away – so wound up deleting the app altogether." (P 142)
	Caused distraction in work/ task flow	5	"Group chats are always annoying and they send a lot of notifications. It is distracting and irritating especially when you're busy. Also, some of the apps frequently send notifications and it's frustrating that I can not customize them." (P 81)
	High frequency of interruptions	14	"Just sometimes my friend likes to blow up iMessage and I get irritated or annoyed." (P 152)
Intimacy breach	Interruption in a social setting	6	"I received a email from a colleague that popped up in my notifications when I had my sound on and was attending a formal dinner party and it went off during a speech." (P 89)
	Caused misunderstanding with someone else	4	"I had an ex get jealous because he saw a text from an unknown number. He accused me of cheating when it was not the case." (P 18)
	Caused conflict with someone else	5	"Someone saw a personal text for me and got mad at me" (P 129)

and type of operating system as independent variable. We found no statistically significant differences in the number of negative experiences between Android and iOS users ($p = 0.7449$).



(a) Concern for self.

(b) Concern of other parties.

Fig. 2. (a)Participants' level of concern if someone else viewed the latest notification they received. (b) Participants' perception about concern of other parties if information about that party contained in the latest notification was seen by someone other than participant (i.e., the notification receiver).

4.1.1 Information Disclosures due to Notifications. We found that smartphone notifications deliver and disclose private content ($n = 22$), information about other parties ($n = 2$) and inappropriate content ($n = 7$). Inappropriate content refers to racy photos or videos, adult language, etc. These information disclosures often led to misunderstandings ($n = 4$) and conflicts ($n = 5$).

To identify the prevalence of the risks of private information disclosure, we analyzed the responses pertaining to the latest notification received by the participants. These notifications were generated by a wide variety of app categories such as social media, messaging, news, shopping, ridesharing, dating, and many others. A majority of the participants (54%; $n = 116$) reported that they were concerned (i.e., they selected somewhat concerned or extremely concerned on a 5-point scale) if someone else viewed the content of the latest notification on their smartphone (Figure 2a).

We then sought to identify the prevalence of risks of information disclosures for other parties. Out of total 213 participants, 87 participants mentioned that the last notification contained information pertaining to another party. Around 72% (62/87) of these participants reported that the other person would be concerned (i.e., somewhat concerned or extreme concerned on a 5-point scale) if someone other than the receiver saw the notification content (see Figure 2b). Hence, there was a risk for information disclosure of someone else for about one-third of the participants.

Some of the instances of unintended information disclosures from smartphone notifications reported by participants are as follows:

- "I was texting something personal with my hubby, suddenly when i was with my colleague it popped up and the person read out, it was a negative experience." (P 72)
- "Someone sent me inappropriate photos without permission and my spouse seen them. She thought I was cheating." (P 108)
- "I received a text from someone who I wasn't supposed to be messaging and my friend who was with me a that point saw the text and who it was from pop up on my phone." (P 39)

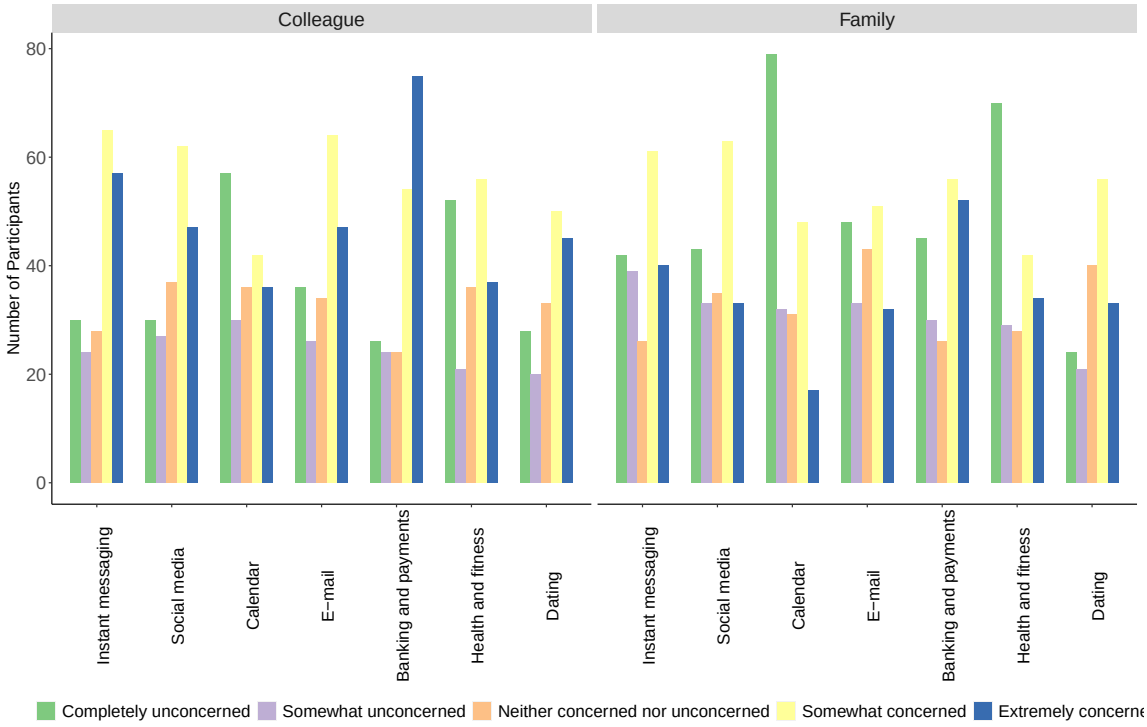


Fig. 3. Participants' concern if content from different app categories is read by either a colleague or a family member.

Table 2. Participants' mean score (standard deviation) for concern if notification content from different app categories is read by a family member or colleague.

App Categories	Mean (sd) Family	Mean (sd) Colleague
Instant messaging	3.09 (1.44)	3.47 (1.39)
Social media	3.05 (1.39)	3.34 (1.36)
Calendar	2.48 (1.41)	2.85 (1.48)
E-mail	2.93 (1.4)	3.29 (1.4)
Banking and payments	3.19 (1.5)	3.63 (1.41)
Health and fitness	2.71 (1.53)	3.02 (1.47)
Dating	3.30 (1.29)	3.36 (1.39)

We then evaluated participants' privacy concerns for content from different app categories. We found that content from different apps cause different level of concerns when seen by a family member or a colleague (see Figure 3 and Table 2). A Mann Whitney U test (with Bonferroni correction) confirmed that the differences between the groups (family member and colleague) are statistically significant ($p < 0.05$) for Instant Messaging, E-mail, Banking and payments categories.

Hence, we found that:

(1) Notifications delivered in the presence of colleagues are more sensitive than notifications received in presence of family members for all types of apps categories.
(2) Content from Calendar apps is seen as the least sensitive.
(3) Around family members, content from Banking & payments apps is seen as sensitive (i.e., participants responded with somewhat concerned or extremely concerned on 5-point scale) by most respondents (n = 108), followed by Instant Messaging apps (n = 101).
(4) Around colleagues, content from Banking & payments app category is seen as sensitive (i.e., participants responded with somewhat concerned or extremely concerned on 5-point scale) by most respondents (n = 129), followed by Instant Messaging apps (n = 120).

4.1.2 Privacy Invasion due to Notifications. Participant responses clearly indicate that smartphone notifications are connected to the facet of privacy linked to intrusion [40] as they cause distractions in task/ activity (n = 5), interrupt frequently (n = 7), disturb personal solitude (n = 6), and invade digital space (n = 14). Notifications further interrupt the privacy facet connected to the intimacy of social settings (n = 6) [48].

We describe 'invasion of digital space' as notifications that ping with unwanted content like scam links, fraudulent messages, viruses and spam; e.g., participants reported "some unwanted video notifications irritate me a lot time" (P 66); and "I kept on getting advertisement notifications – repeatedly one after another – from a shopping app I had, that were really not related to the app itself, and would not stop unless I would open the app right away – so wound up deleting the app altogether. in order to use the app, I had to have notifications. however repeated notifications happened – one after the other – untill I opened the app, so had to delete the app" (P 142). In addition, participants reported unwanted interruptions in social settings due to notifications such as, "It was a Facebook notification. I was in a work meeting that was very important and I had forgotten to silence my notifications. It was very embarrassing" (P 171) and "notification ring in office meeting" (P 213). Further, participants reported that notifications caused conflict and misunderstanding, thus breaching the 'intimacy' facet of privacy.

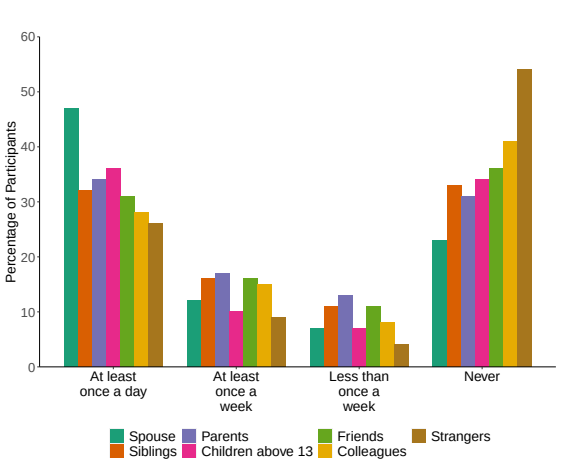
Table 3 shows the mean scores of 'Perceived Intrusion' and 'Perceived Surveillance' subscales from the MUIPC scale for participants grouped by reported 'Instances of Negative Experiences' due to smartphone notifications. We found these two variables to be statistically significantly correlated (Spearman correlation coefficient = 0.19; p = 0.007). Kruskal-Wallis rank sum test showed that there are statistically significant differences between the groups of 'Perceived Intrusion' ($p < 0.01$) and 'Perceived Surveillance' ($p < 0.05$) on instances of negative experiences. This implies that smartphone users who report a higher concern for their information privacy are associated with facing more privacy concerns due to their smartphone notifications.

4.1.3 Privacy Considerations due to Device Sharing. Close to half of the participants (47%; n = 100) reported that they shared their smartphone with their spouse at least once a day (see Figure 4a). Nearly a third of the participants shared with their smartphone at least once a day with their siblings (32%; n = 69) or friends (31%; n = 66). A bit more than a third did so with their parents (35%; n = 74) and children above 13 years of age (36%; n = 77), and a bit more than a quarter with colleagues (28%; n = 59) or even strangers (27%; n = 574) with strangers.

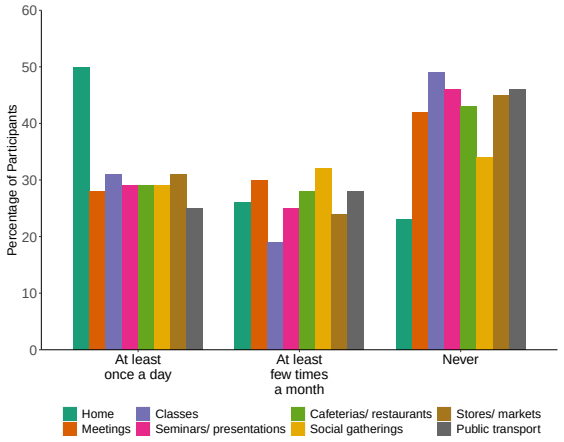
Apart from device sharing, half of the participants (50%; n = 107) reported that someone else can view the contents of their smartphone notifications at least once a day in a variety of contexts, such as meetings (28%; n = 60), classes (31%; n = 66), seminars and presentations (29%; n = 61); cafeterias and restaurants (29%; n = 62), social gatherings (29% (n = 62), stores and markets (31%; n = 66), and public transportation (25.7%; n = 65) (see Figure 4b).

Table 3. Mean scores of Perceived Intrusion and Perceived Surveillance constructs from the MUIPC scale grouped by Instances of Negative Experiences and mean use of different features (in hours) grouped by Instances of Negative Experiences.

Instances of Negative Experiences	Perceived Intrusion	Perceived Surveillance	DND Mode	Silent Mode	Turn Off Device	Airplane Mode	Notification Management Apps
0	14.62	14.91	1.64	6.11	1.05	1.08	2.18
1-2	15.38	15.49	2.81	5.47	1.49	1.43	4.85
3-5	15.96	16.11	2.98	6.18	2.91	2.82	5.86
6-10	16.50	16.81	7.75	10.25	7.81	9.50	11.81
11-20	18.33	17.00	6.50	5.75	5.25	5.75	4.25
More than 20	18.00	17.60	2.2	4.20	0.40	0.20	2.00



(a) Frequency of device sharing with various parties.



(b) Frequency for someone else viewing notification contents at various places.

Fig. 4. Device sharing and undesired exposure of other people's information.

Privacy concerns and risks are exacerbated by the prevalence of various shared viewing contexts such as lending the device to someone else, viewing information on a device jointly with other parties, screencasting, presence of bystanders in social and professional settings. Indeed, participants reported several privacy concerns arising from device sharing or visibility of the device screen to someone other than the owner:

- "When I was working on something for work where i had to cast my device screen for others to see. The notification was highly personal." (P 45)
- "I was watching a video with a younger cousin and the notification popped up. It was adult language that a child (cousin) was able to read." (P 77)
- "While giving my mobile to my sibling I forget to turn off the notification from my personal chat." (P 162)

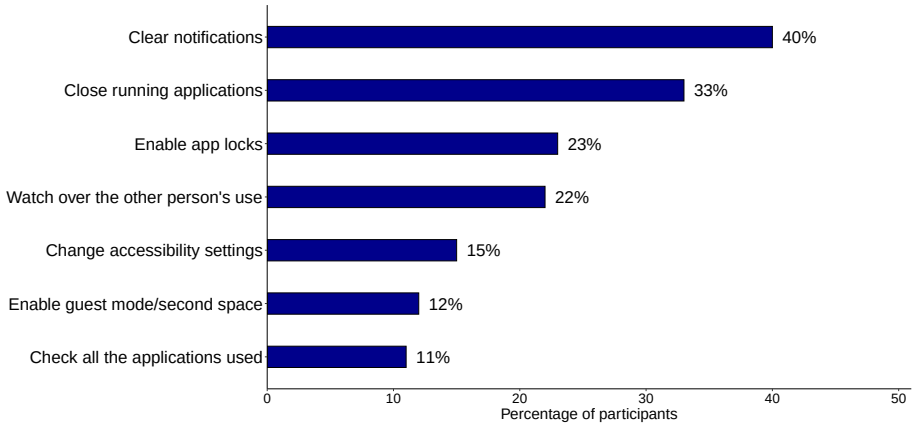


Fig. 5. Actions taken prior to handing over the device to someone else.

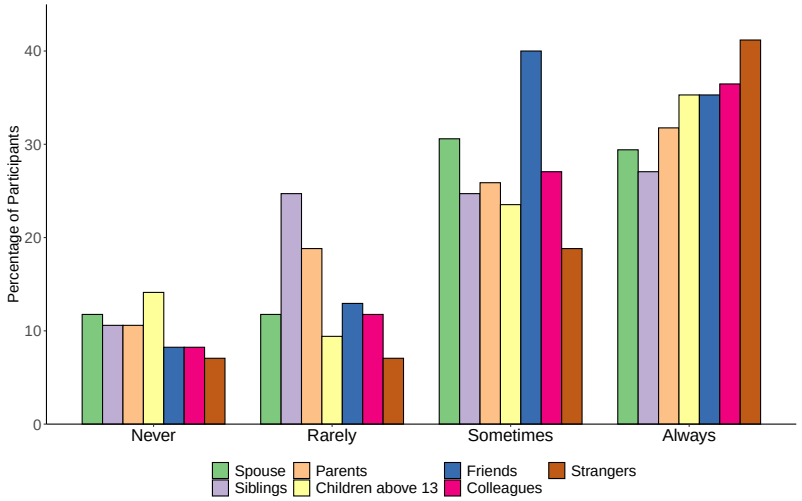


Fig. 6. Frequency of clearing notifications prior to handing over the device to various parties.

We investigated practices and preferences when sharing the smartphones with someone else (see Figure 5). Prior to sharing the device, users have the ability to take a few privacy-protective actions, such as clearing notifications or closing applications. We found that few of our participants showed the inclination to use these mechanisms; only 40% (n = 85) preferred to clear notifications before handing device over to someone else, only a third (33%; n = 71) reported closing any active applications, and only 12% (n = 25) mentioned that they used 'guest mode.' We further analyzed the preferences of participants who reported that they cleared notifications before handing over their device to others (see Figure 6). Notably, 59% (n = 40), out of the 85 participants did not always clear notifications before handing over their device to a stranger.

Table 4. Mean use of features to control the smartphone state (in hours) and correlation of use of smartphone features with the occurrences of negative experiences due to notifications, along with the adjusted p-values.

Smartphone Feature	Mean Use	Correlation with Neg. Experiences	p-values
Use **Do Not Disturb (DND)** Mode	2.85	0.29 0.26	0.014
Use **Silent** Mode	6.61	0.033 0.13	1.00
Turn off the device	2.19	0.27 0.297	0.028
Use **Airplane** mode	2.28	0.28 0.295	0.024
Use **notification management apps**	4.63	0.26 0.32	0.036

4.2 Control over Smartphone State

Participants reported controlling notifications by making routine use of various smartphone features to control the device state: Do Not Disturb (DND) mode (56%; $n = 97$), silent mode (80%; $n = 138$), turning off the device (45%; $n = 77$), airplane mode (43%; $n = 74$) and notification management preferences and apps (62%; $n = 107$). Table 4 provides the mean and median usage (in hours) of these smartphone features in a typical day. We found that users prefer to use the silent mode and notification management apps over other alternatives to control their smartphone device and manage their notifications, based on usage per day. A total of 53 participants elaborated on their reasons for controlling device state through the mentioned smartphone features (see Table 5). Other reasons for using smartphone modes that participants reported were saving battery, restarting the phone, driving, eating, or special circumstances.

We then tried to understand how the use of various device-control features is associated with the instances of negative experiences due to smartphone notifications. To this end, we grouped the responses based on number of negative occurrences and calculated the group-wise mean usage (in hours) in a typical day (see Table 3). Kruskal-Wallis rank sum test shows statistically significant differences in the use of Do Not Disturb mode ($p < 0.01$), silent mode ($p < 0.05$), turning off the device ($p < 0.05$), airplane mode($p < 0.005$), and notification management apps ($p < 0.001$) on instances of negative experiences. In particular, we noted that the use of device-control mechanisms increases until 10 instances of negative experiences, but decreases thereafter.

We calculated the correlation of the hourly use of each smartphone mechanism with the instances of negative experience (see Table 4), adjusting the p values using Bonferroni correction. We found that the number of instances of negative experiences is weakly correlated with the use of the Do Not Disturb mode, turning the device off, airplane mode, and notification management apps ($p < 0.05$).

4.2.1 Digital difficulties. We measured technical expertise using the digital difficulties scale [5]. Table 6 provides the mean scores of the participants on the digital difficulties scale grouped by the number of instances of negative experiences. Higher scores indicate greater digital difficulties, i.e., lower technical proficiency. Interestingly, we found that those who indicated higher technical proficiency reported no negative experiences with notifications at all or a large number (more than 10) of negative experiences. Compared to these two groups of participants, those who reported 1–10 negative instances of notification-related negative experiences were less technically proficient.

5 DISCUSSION

As our report Section 4 indicates, our findings show that privacy concerns related to smartphone notifications are influenced by information content and additional audience beyond the receiver, thus echoing privacy-related findings

Table 5. User preferences for controlling the device state.

Theme	Code	Count	Example Comments
Prefer to control device state	to avoid ring of phone from notifications/ calls	6	"I do not like alerts or noises. So I keep my phone in silent mode at all times. I find this works best for me and limits distractions." (P 48)
	to limit interruptions and check device at own accord	4	"I turn it off overnight, and not on until I pick it up to leave the house for work. At work, and for the rest of the day I have it silent, I'll look at it when I feel the need." (P 16)
	during sleep	17	"Some mid night calls are coming so i am off the airplane mode." (P 121)
	during work or for specific tasks	17	"I make sure I can't be disturbed at all when I'm working. It's just easier to turn on DND than fiddle with individual apps." (P 152)
	when around someone else (meetings/ social gathering, etc.)	6	"I generally have my phone on silent for the 8 hours I sleep at night and then for at least about 4 hours in the evening when spending time with the family." (P 10)
	customize notification settings	4	"I just set custom individual notification settings for most of my apps. If they're atrociously annoying I uninstall them" (P 52), "…I do use a notification manager from samsung to group notifications." (P 64)
	other reasons	5	"…While in office hours I use Do Not Disturb mode. Device is off while eating lunch." (P 162)
Do not control device state	to be available in case of an emergency	2	"I keep it on just in case there's an emergency and someone is trying to get a hold of me." (P 110)
	to stay alert to notifications	4	"I prefer to get all alerts and notifications when the arrive, regardless of the time of day." (P 107)
	other reasons	7	"I never use any of the services mentioned, because I do not see the need for them." (P 174), "Since I live alone and I usually do not get late calls I leave cell on. I also leave on in case someone has an emergency." (P 58)

Table 6. Digital difficulties score grouped by instances of negative experiences due to smartphone notifications.

Instances of Negative Experiences	Mean	Median	Standard Deviation
0	10.61	8	6.49
1-2	15.70	18	6.51
3-5	15.75	18	6.26
6-10	18.19	19	4.65
11-20	14.75	15.5	9.11
More than 20	11.80	8	8.11

from other domains covered in the literature (see Section 2). At the same time, our findings extend the literature by adding notification-specific nuance and surface additional privacy-affecting aspects connected to notifications. For instance, we found that privacy concerns for notifications vary based on the type of app in question. In future work, it would be interesting to investigate if users further differentiate privacy sensitivity of notifications from a single app that delivers different types of notifications for different features within the app (e.g., messaging apps typically permit users to set different types of notification settings for different types of events within the apps).

Apart from the content of the notification, we note that the disruption caused by notification alerting mechanisms (such as sounds) impinge upon the Solitude facet of privacy [48]. Participants reported deleting apps that send notifications too frequently. The content of the notifications can further impact the Intimacy and Reserve facets of privacy [48] by causing misunderstanding, unease, and conflict that can have a negative impact on interpersonal relationships. Yet, current mechanisms for controlling notification delivery do not provide any consideration for the user's social context at the time of notification delivery. Notification content that contains undesirable or malicious content, such as spam, advertisements, malicious links, etc., can raise the additional privacy issue of digital intrusion. While infrastructure and end-point solutions exists for detecting and filtering email spam, there are no analogous mechanisms for notification content.

As reported by past studies on device sharing, the practices of our participants confirm that users do share the device with others, even strangers, or engage in joint use of device, such as watching a video together. While current smartphones offer the privacy-protecting option of using a 'guest' mode when sharing a device, such all-or-none binary access control is neither adequate nor well-suited to handle the variety of situations under which device sharing occurs [21]. It should be no surprise then that we found little use of these features with many participants opting for quick-but-crude solutions such as clearing notifications or closing apps and many not taking any precautions at all! Apart from poor usability and user experience, additional factors behind the low use of such privacy-protective features might be to avoid the social awkwardness of signalling distrust by overt and obvious use of the features, needing access to specific functionality or data that is not available in the restricted guest mode, or avoiding the loss of important notifications. As a participant reported "sometimes I cleared the important notifications. Then I forget to answer" (P 208). Further research is needed to develop mechanisms that can facilitate a seamless and socially workable solution for transition to a mode that protects notification privacy in contexts of shared use.

Although more sophisticate options for controlling delivery are available within smartphone operating systems and apps, we found that people mostly rely on crude-but-quick mechanisms such as silent or DND modes. The use of these modes does mean that the user can miss out on important calls or urgent messages. Interestingly, slightly more participants reported the use of notification management apps (62%) than the use of the DND mode (56%). It would be interested to understand the advantages these third party apps offer over available operating system features such that a large percentage of smartphone users to use them to control notifications.

Although the latest versions of smartphone operating systems include greater control over notifications, these features do not cover all of the privacy issues surfaced by our findings. For instance, iOS allows users to customize lock-screen notification previews by app [11], however these options cannot be tailored based on social or temporal context. Moreover, when an unlocked device is shared with someone else, notifications can leak information via pop up alerts and/or the notification center. Although the DND mode in Android versions 9 and above can be helpful for limiting interruptions from notifications [20], Android users in our sample did not report using the feature, and it is unclear if the feature can limit the risks of undesired information disclosure. The recent feature for snoozing notifications introduced in Android versions 8 and above [19] might not be helpful in preventing information disclosures

either as they might be exposed when they are redelivered later. Additionally, the latest version of Android includes 'digital well-being' features [18] such as 'Focus Mode' and allows users to flip the phone down to turn off interruptions. While these recent features can be helpful in reducing distractions and interruptions from notifications, it does not address the various other privacy issues related to notifications surfaced by the findings of our study. For instance, none of the features in current smartphones permit users to disable notifications while device sharing or screencasting.

While we found that those who experience a few negative experiences seem to increase the use of device-control options, the tendency appears to dissipate after a handful of such experiences, with those reporting large numbers of negative experiences also reporting lower usage of device-control options, despite being technically proficient. Further research is needed to investigate whether these findings are driven by a lack of effective ways to scale the control mechanisms to handle a large volume of potentially privacy-affecting notifications or user acceptance of negative experiences with notifications as routine part of everyday device use.

6 IMPLICATIONS

Our findings suggest a number of design recommendations for helping users avoid experiencing privacy violations due to mobile device notifications:

6.1 Personalize Notification Content and Delivery Frequency

As a participant reported, "Group chats are always annoying and they send a lot of notifications. It is distracting and irritating especially when you're busy. Also, some of the apps frequently send notifications and it's frustrating that I can not customize them." We recommend that app developers allow users to opt in for notifications for only the most preferred content from the app. In this regard, the recent versions of the Android operating system (Android 8.0 and above) provide greater control over app notifications through the mechanism of 'channels,' which are content categories that can individually turned on and off. For example, a social media app could create separate 'notification channels' for different content such as group messages, direct messages, mentions, likes, follows, etc. [12].

Weber et al. [43] recently investigated the reasons and the role of manual deferring of notifications. We recommend studies to understand if deferral of notifications is helpful in reducing privacy risks or avoiding privacy breaches. While previous studies (e.g., [15, 35]) to predict opportune moments of notification delivery have shown that delaying notification can partially reduce interruptibility (intrusion facet of privacy), it would be of interest to see if deferral of notification can mitigate additional privacy risks and breaches. Additionally, mechanisms for opportune delivery can be extended for considerations beyond interruptiblity to include considerations of privacy-affecting contextual factors, such as the presence of others who can view the screen, use of the device by someone other than the owner, etc. For example, the 'Hide sensitive content' option for lock screen notifications in Android be set to location-dependent.

6.2 Ease User Privacy Concerns for Device Sharing

Our study reveals that notifications cause unintended information disclosures when the device is shared with others. Therefore, we recommend automatically turning off notifications when it is detected that the device is handed over to someone else, device screen is cast to a publicly viewable display, or multiple people are watching the device screen. The detection of such 'public' contexts can be based on explicit user action and/or relevant heuristics and/or machine learning techniques. For instance, machine learning algorithms could be trained for automatic detection of contexts of shared use and additional audiences beyond the device owner based on features such as the characteristics of the person handling the device, temporal factors (e.g., business hours vs. sleep time), sensor readings of environmental context [29]

etc. For additional protection, users can be allowed to assign password protection for accessing the notification collection (i.e., notification drawer or notification center) [45] such that users do not need to lose important notifications by clearing them prior to sharing the phone with someone else because password protection will prevent the other party from accessing notifications from the collection.

Further, natural language processing algorithms could be employed to the notification content to prevent risks of information disclosure for someone else's information by obfuscating other people's names when displaying notifications in a shared context. As a past study by Weber et al. [47] showed, users preserved the privacy of their contacts by censoring names before logging notifications, thus underscoring the utility of automating such obfuscation.

6.3 Limit the Number of Notifications

Various participants reported feeling uneasy and uncomfortable due to the intrusion caused by notifications. High frequency of notifications caused participants to experience negative emotions, such as annoyance and irritation. Hence, limiting the number of notifications can decrease digital intrusions from unwanted content, reduce intrusions of personal solitude, and increase the overall user experience of notifications. Moreover, reducing notification frequency reduces the number of occasions for potential privacy violations, thus reducing privacy risk. We recommend some of the following ways to limit the number of notifications:

(1) Allow users to control notification delivery based on specified keywords, such as *urgent, OTP, update, important.*
(2) Bundle notifications and display only upon reaching a threshold or at set time intervals, such as every hour, or at fixed times of the day, say noon.
(3) Permit users to set per-app limits on the number of notifications in a given time interval.

7 LIMITATIONS AND FUTURE WORK

Our findings are impacted by the limitations of self-selection and self-reporting. Future work should compare these results with real-world analytics of behavioral data and metadata that captures notification content and user interactions with notifications via tools such as Clear All [46] or Notification Log [44]. Further, tools like Annotif [47] can enable the collection of corresponding retrospective user reflection that adds context to the captured logs and facilitates more nuanced interpretation based on a combination of analytics and user responses.

Our sample consists of individuals from the United States. Since privacy is known to be influenced by cultural factors, generalizability to other cultures requires verification and is an important direction for future work. Apart from privacy concerns, device sharing practices in particular, are likely to differ substantially in developing nations because of various sociocultural differences.

Our investigation focused on mobile devices (smartphones, in particular). It would be interesting to compare these results with privacy aspects of notifications from other smart devices such as those embedded in a user's physical environment (i.e., Internet of Things (IoT) devices).

8 CONCLUSION

Users of mobile devices receive dozens of notifications every day. Inopportune notifications can result in undesirable information disclosures and disruptions, thus violating privacy. The portable nature of mobile device exacerbates these aspects because the device is often used in situations when other people are around and can be easily shared with other people by simply handing it over. However, preference settings to control mobile-device notifications currently lack

any consideration of these usage context with high potential for privacy violation. The findings of our study highlight the need for greater attention ensuring that notification delivery avoid privacy violations for the user as well as the other parties whose information is contained in the notification content.

REFERENCES

[1] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 17 (Dec. 2017), 20 pages. https://doi.org/10.1145/3134652

[2] Mohammed Eunus Ali, Anika Anwar, Ishrat Ahmed, Tanzima Hashem, Lars Kulik, and Egemen Tanin. 2014. Protecting Mobile Users from Visual Privacy Attacks. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (Seattle, Washington) *(UbiComp '14 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/2638728.2638788

[3] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 787–796.

[4] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975).

[5] Sarah Anrijs, Koen Ponnet, and Lieven De Marez. 2020. Development and psychometric properties of the Digital Difficulties Scale (DDS): An instrument to measure who is disadvantaged to fulfill basic needs by experiencing difficulties in using a smartphone or computer. *Plos one* 15, 5 (2020), e0233891.

[6] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[7] Rebecca Balebako, Pedro G Leon, Hazim Almuhimedi, Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Cranor, and Norman Sadeh-Koniecpol. 2011. Nudging users towards privacy on mobile devices. (2011).

[8] Antoine Boutet and Sébastien Gambs. 2019. Inspect What Your Location History Reveals About You: Raising User Awareness on Privacy Threats Associated with Disclosing His Location Data. In *Proceedings of the 28th ACM International Conference on Information and Knowledge Management* (Beijing, China) *(CIKM '19)*. Association for Computing Machinery, New York, NY, USA, 2861–2864. https://doi.org/10.1145/3357384.3357837

[9] V. Braun and V. Clarke. 2012. Thematic analysis. In *H*, P. M. Camic Cooper, D. L. Long, A. T. Panter, D. Rindskopf, and K. J. Sher (Eds.). Quantitative, qualitative, neuropsychological, and biological (p.. American Psychological Association, APA handbooks in psychology®. APA handbook of research methods in psychology, Vol. 2. Research designs, 57–71. https://doi.org/10.1037/13620-004

[10] Hyunsung Cho, Jinyoung Oh, Juho Kim, and Sung-Ju Lee. 2020. I Share, You Care: Private Status Sharing and Sender-Controlled Notifications in Mobile Instant Messaging. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW1, Article 034 (May 2020), 25 pages. https://doi.org/10.1145/3392839

[11] Jason Cross. 2018. iOS 11: How to hide sensitive info in notification previews. https://www.macworld.com/article/231076/ios-11-how-to-hide-sensitive-info-in-notification-previews.html [Online; posted 6-March-2018].

[12] Corbin Davenport. 2017. Android O feature spotlight: Notification Channels give more controls over notifications to users. https://www.androidpolice.com/2017/03/28/android-o-feature-spotlight-notification-channels-simplify-managing-notifications/ [Online; posted 28-March-2017].

[13] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097

[14] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. *Understanding Shoulder Surfing in the Wild: Stories from Users and Observers*. Association for Computing Machinery, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[15] Joel E. Fischer, Chris Greenhalgh, and Steve Benford. 2011. Investigating Episodes of Mobile Phone Activity as Indicators of Opportune Moments to Deliver Notifications. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (Stockholm, Sweden) *(MobileHCI '11)*. Association for Computing Machinery, New York, NY, USA, 181–190. https://doi.org/10.1145/2037373.2037402

[16] Jan Gugenheimer, Alexander De Luca, Hayato Hess, Stefan Karg, Dennis Wolf, and Enrico Rukzio. 2015. ColorSnakes: Using Colored Decoys to Secure Authentication in Sensitive Contexts. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 274–283. https://doi.org/10.1145/2785830.2785834

[17] Alina Hang, Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2012. Too Much Information! User Attitudes towards Smartphone Sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design* (Copenhagen, Denmark) *(NordiCHI '12)*. Association for Computing Machinery, New York, NY, USA, 284–287. https://doi.org/10.1145/2399016.2399061

[18] Android Help. [n.d.]. Digital Wellbeing. https://www.android.com/digital-wellbeing/#productivity-get-stuff-done

[19] Android Help. 2018. Control notifications on Android. https://support.google.com/android/answer/9079661

[20] Android Help. 2018. Limit interruptions with Do Not Disturb on Android. https://support.google.com/android/answer/9069335

[21] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. Association for Computing Machinery, New York, NY, USA, 1647–1650. https://doi.org/10.1145/1518701.1518953

[22] Yongsung Kim, Adam Fourney, and Ece Kamar. 2019. Studying Preferences and Concerns about Information Disclosure in Email Notifications. In *The World Wide Web Conference* (San Francisco, CA, USA) *(WWW '19)*. Association for Computing Machinery, New York, NY, USA, 874–885. https://doi.org/10.1145/3308558.3313451

[23] Alfred Kobsa, Sameer Patil, and Bertolt Meyer. 2012. Privacy in instant messaging: An impression management model. *Behaviour & Information Technology* 31, 4 (2012), 355–370.

[24] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15, 4 (Dec. 2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[25] Stephen T Margulis. 2011. Three theories of privacy: An overview. *Privacy online* (2011), 9–17.

[26] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll Just Grab Any Device That's Closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5921–5932. https://doi.org/10.1145/2858036.2858051

[27] Abhinav Mehrotra, Mirco Musolesi, Robert Hendley, and Veljko Pejovic. 2015. Designing Content-Driven Intelligent Notification Mechanisms for Mobile Applications. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Osaka, Japan) *(UbiComp '15)*. Association for Computing Machinery, New York, NY, USA, 813–824. https://doi.org/10.1145/2750858.2807544

[28] Nicholas Micallef, Mike Just, Lynne Baillie, and Maher Alharby. 2017. Stop Annoying Me! An Empirical Investigation of the Usability of App Privacy Notifications. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction* (Brisbane, Queensland, Australia) *(OZCHI '17)*. Association for Computing Machinery, New York, NY, USA, 371–375. https://doi.org/10.1145/3152771.3156139

[29] Nicholas Micallef, Mike Just, Lynne Baillie, Martin Halvey, and Hilmi Güneş Kayacik. 2015. Why Aren't Users Using Protection? Investigating the Usability of Smartphone Locking. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 284–294. https://doi.org/10.1145/2785830.2785835

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

[31] Judith S. Olson, Jonathan Grudin, and Eric Horvitz. 2005. A Study of Preferences for Sharing and Privacy. In *CHI '05 Extended Abstracts on Human Factors in Computing Systems* (Portland, OR, USA) *(CHI EA '05)*. Association for Computing Machinery, New York, NY, USA, 1985–1988. https://doi.org/10.1145/1056808.1057073

[32] Sameer Patil and Jennifer Lai. 2005. Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Portland, Oregon, USA) *(CHI '05)*. Association for Computing Machinery, New York, NY, USA, 101–110. https://doi.org/10.1145/1054972.1054987

[33] Sameer Patil, Greg Norcie, Apu Kapadia, and Adam J. Lee. 2012. Reasons, Rewards, Regrets: Privacy Considerations in Location Sharing as an Interactive Practice. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 5, 15 pages. https://doi.org/10.1145/2335356.2335363

[34] Veljko Pejovic and Mirco Musolesi. 2014. InterruptMe: Designing Intelligent Prompting Mechanisms for Pervasive Applications. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 897–908. https://doi.org/10.1145/2632048.2632062

[35] Martin Pielot, Bruno Cardoso, Kleomenis Katevas, Joan Serrà, Aleksandar Matic, and Nuria Oliver. 2017. Beyond Interruptibility: Predicting Opportune Moments to Engage Mobile Phone Users. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 91 (Sept. 2017), 25 pages. https://doi.org/10.1145/3130956

[36] Martin Pielot, Karen Church, and Rodrigo de Oliveira. 2014. An In-Situ Study of Mobile Phone Notifications. In *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services* (Toronto, ON, Canada) *(MobileHCI '14)*. Association for Computing Machinery, New York, NY, USA, 233–242. https://doi.org/10.1145/2628363.2628364

[37] Martin Pielot, Amalia Vradi, and Souneil Park. 2018. Dismissed! A Detailed Exploration of How Mobile Phone Users Handle Push Notifications. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Barcelona, Spain) *(MobileHCI '18)*. Association for Computing Machinery, New York, NY, USA, Article 3, 11 pages. https://doi.org/10.1145/3229434.3229445

[38] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive authentication: deciding when to authenticate on mobile phones. In *21st {USENIX} Security Symposium ({USENIX} Security 12)*. 301–316.

[39] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly* (1996), 167–196.

[40] Daniel J Solove. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (2006), 477.

[41] Raj Vardhan, Ameya Sanzgiri, Dattatraya Kulkarni, Piyush Joshi, and Srikanth Nalluri. 2017. Notify Assist: Balancing Privacy and Convenience in Delivery of Notifications on Android Smartphones. In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society* (Dallas, Texas, USA) *(WPES '17)*. Association for Computing Machinery, New York, NY, USA, 17–20. https://doi.org/10.1145/3139550.3139561

[42] Emanuel von Zezschwitz, Sigrid Ebbinghaus, Heinrich Hussmann, and Alexander De Luca. 2016. You Can't Watch This! Privacy-Respectful Photo Browsing on Smartphones. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 4320–4324.

[43] Dominik Weber, Alexandra Voit, Jonas Auda, Stefan Schneegass, and Niels Henze. 2018. Snooze! Investigating the User-Defined Deferral of Mobile Notifications. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Barcelona, Spain) *(MobileHCI '18)*. Association for Computing Machinery, New York, NY, USA, Article 2, 13 pages. https://doi.org/10.1145/3229434.3229436

[44] Dominik Weber, Alexandra Voit, and Niels Henze. 2018. Notification Log: An Open-Source Framework for Notification Research on Mobile Devices. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (Singapore, Singapore) *(UbiComp '18)*. Association for Computing Machinery, New York, NY, USA, 1271–1278. https://doi.org/10.1145/3267305.3274118

[45] Dominik Weber, Alexandra Voit, and Niels Henze. 2019. Clear All: A Large-Scale Observational Study on Mobile Notification Drawers. In *Proceedings of Mensch Und Computer 2019* (Hamburg, Germany) *(MuC'19)*. Association for Computing Machinery, New York, NY, USA, 361–372. https://doi.org/10.1145/3340764.3340765

[46] Dominik Weber, Alexandra Voit, and Niels Henze. 2019. Clear All: A Large-Scale Observational Study on Mobile Notification Drawers. In *Proceedings of Mensch Und Computer 2019* (Hamburg, Germany) *(MuC '19)*. Association for Computing Machinery, New York, NY, USA, 361–372. https://doi.org/10.1145/3340764.3340765

[47] Dominik Weber, Alexandra Voit, Gisela Kollotzek, and Niels Henze. 2019. Annotif: A System for Annotating Mobile Notifcations in User Studies. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (Pisa, Italy) *(MUM '19)*. Association for Computing Machinery, New York, NY, USA, Article 24, 12 pages. https://doi.org/10.1145/3365610.3365611

[48] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[49] Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give Social Network Users the Privacy They Want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1427–1441. https://doi.org/10.1145/2675133.2675256

[50] Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John M Carroll. 2012. Measuring mobile users' concerns for information privacy. (2012).

[51] Fengpeng Yuan, Xianyi Gao, and Janne Lindqvist. 2017. *How Busy Are You? Predicting the Interruptibility Intensity of Mobile Users*. Association for Computing Machinery, New York, NY, USA, 5346–5360. https://doi.org/10.1145/3025453.3025946