Exploring privacy concerns and violations for smartphone notifications

ANONYMOUS AUTHOR(S)*

Notifications form one of the most important, pervasive features of mobile devices. Multitudes of notifications are delivered to users everyday. The notifications often carry sensitive content like financial information, private messages, business information etc. To understand privacy concerns regarding notification content and delivery, we conducted a study in which participants (n = 235) described their preferences and practices related to smartphone notifications. Majority of the participants (60%) reported 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 the device, and intrusion in various contexts. 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 user 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, 30 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Notifications form an important method of information delivery on mobile devices. On average smartphone users receive 63.5 notifications per day [39]. Third party applications or system services often generate notifications to inform users about updates, warnings, reminders and various events like new messages, appointments, etc. Mobile notifications are more pervasive and common than phone calls.

Notifications can contain sensitive content like personal details, financial information, private messages, valuable business information etc., that is stored on smartphones these days, which may be visible to onlookers. Uncomfortable situations could arise if a notification pops up when a personal device is shared with or viewable by others or its screen is cast on another device. This makes notifications an avenue for unintended and undesired disclosure of private information. Notifications can also intrude upon solitude if they interrupt the user at an inappropriate time; e.g., notification rings if a user is sleeping. Intrusions can interrupt activities or routines, disrupt solitude, and often make the user feel uncomfortable and uneasy [43].

Woodstock '18, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

Previous studies have shown that ill-timed notifications can have negative effects on productivity such as distractions, interruptions, and increased stress [31, 39]. Although information disclosures and privacy concerns have been investigated in the specific context of email notification [25], 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.

As Farrell [18] wrote:

> "By making smart devices ubiquitous, we've exposed ourselves to computer-assisted embarrassment…User-experience design must also be concerned with social user experience: the situated experiences with technologies in the context of groups of people. We need to understand how the behaviors of what we design fit or do not fit with families, work environments, school cultures, and play."

Hence, in an attempt to reduce privacy risks associated with notifications and suggest improved smartphone notifications delivery, we study user preferences and concerns regarding privacy aspects of mobile device notifications. We complement and extend prior research by tackling the following research questions:

- **RQ1:** What are the various privacy considerations associated with smartphone notifications?
- **RQ2:** How do smartphone mechanisms to control interruptions (e.g., silent mode, notification delivery preferences, etc.) relate to privacy risks of notifications?

We sought answer to the above questions via an online questionnaire administered via the Amazon Mechanical Turk (AMT) platform. The study included questions regarding device settings, device sharing behavior, notification content, and contextual aspects related to notification delivery and reception.

We found that notifications on mobile devices do indeed impact privacy of the recipients and potentially of those whose information might be included in the notification. We uncovered that an increase in negative experiences with notifications is associated with greater use of device control mechanisms, but the relationship seems to reverse if the negative experiences continue to grow beyond a threshold. We further found that the privacy threats of notifications are particularly higher in situations that involve device sharing. Yet, most participants reported not taking preventive actions prior to sharing the device with others. These findings contribute to an improved understanding of privacy concerns connected to mobile device notifications in general.

In the following sections, we describe current notification delivery mechanisms, provide an overview of notification customization functionality, and explain our method. 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 and security issues specific to mobile devices, and notification mechanisms. We cover salient work in each space in turn.

2.1 Individual Privacy Concerns

The first step in understanding user privacy concerns for notifications, is to understand various definitions and dimensions of privacy. Pioneering work by Westin [47] categorised four states of privacy: Solitude, Intimacy, Anonymity and Reserve. These four states are summarised aptly by [28]- Solitude is being free from observation by others; Intimacy refers to small group seclusion for members to achieve a close, relaxed, frank relationship; Anonymity refers to freedom from identification and from surveillance in public places and for public acts; Reserve is based on a

desire to limit disclosures to others, it requires others to recognize and respect that desire. We focus on the dimensions of solitude, intimacy and reserve in our study. Likewise, Altman [9] states different aspects of privacy to include the 'interplay of people, their social world, the physical environment, and the temporal nature of social phenomena.' Solove [43] provides an understanding of privacy by focusing on different kinds of activities that impinge upon privacy such as 'intrusion.' He says, "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). Intrusion need not involve spatial incursions: spam, junk mail, junk faxes, and telemarketing are disruptive in a similar way, as they sap people's time and attention and interrupt their activities [43].

Researchers have also examined how the privacy preferences relate to type of information disclosures and context of audience witnessing it [2, 37]. For example, Olson et al. [37] found differences in people's preferences to share information based on different *classes* of recipients, like high variance for willingness to share various personal items with co-workers, including sharing one's age with a competitor, one's pregnancy status with other team members and one's marital status in a company newsletter. Hence, based on these results we examine the role of content from different types of apps categories and two varied contexts of hypothetical witness of information disclosure.

Additionally, various instruments have been developed to look at privacy quantitatively such as Concern for Information Privacy (CFIP) [42], Internet Users' Information Privacy Concerns (IUIPC) [27]. Xu et al. [49] developed a scale of mobile users' information privacy concerns (MUIPC) to measure the nature of privacy concerns among mobile users. They described 'perceived surveillance' construct of their scale as user concerns related to persistent data collections which 'induce the perception of intensive data logging' and 'impression of being constantly monitoring' through smartphones.' Apps can collect far more personally invasive data than was previously conceivable in conventional use of personal computers, e.g., identity, upcoming schedule, time spent on different apps, contact lists, real-time location, etc.. The 'perceived intrusion' dimension of their study has been connected to the concept of personal space [43]. It refers to physical as well as informational space, such as the problem of malware and malicious apps for smartphones.

2.2 Privacy and Security in Mobile Devices

Various studies have investigated authentication schemes to make smartphone locking mechanism more efficient and secure: analysis of (un)locking behavior and perceptions of smartphone users [22], design of context-sensitive screen locking application [33], prototype of progressive authentication by constantly collecting cues about the user [41]. Researchers have also studied the use of privacy nudges, which are notifications that use a "soft-paternalistic" method to nudge (instead of force) users to make more informed privacy decisions [7, 11, 32, 46]. Another theme that researchers have worked on is authentication systems that aim to mitigate shoulder surfing (e.g., [8, 16, 17, 20]). Von et al. [45] designed a system to obfuscate photos to check privacy leaks from smartphone photos. Ali et al. [6] developed an app to mitigate visual privacy attacks, i.e., unauthorized visual access of the mobile display by the bystanders.

Our study has been influenced by past studies on shared use of smartphones and the associated privacy and security concerns [1, 5, 21, 24]. Research by Hang et al.(2012) [21] found that push notifications are a source for privacy infringement. However, with addition of newer features to smartphones like screencast, privacy infringements may have changed, which our study takes into account.

2.3 Notifications

Most of the earlier work on smartphone notifications focuses on the disruptive effects of interruptions and seeks to find opportune moments, modes to deliver them with least interference. Various studies show the potential negative effects of interruptions on task performance [13, 14, 23], task resumption rate [36] and emotional state [4]. Recent work by Kushlev et al. [26] shows that interruptions due to phone notifications can cause inattention and hyperactivity in the general population. Though frequent interruptions due to notifications can increase engagement in smartphone based health interventions [34] yet too high frequency of notifications can be perceived as disturbing and users should therefore be given the opportunity to determine the frequency with which they receive notifications [48].

Attempts have been made in the past to predict opportune moments to deliver notifications to prevent to reduce disruptive effects of ill-timed interruptions e.g., content and context driven intelligent notification mechanisms for mobile applications [30], based on sensing mobile phone activity to find task transitions [19], based on real time user data like activity, emotions and engagement, time and location [38], prediction of predict users' interruptibility intensity based on user's context and interruption content [50]. To lower the pressure for an immediate reply and reduce unnecessary interruptions by untimely notifications, two design concepts for Mobile Instant Messaging were examined-private status sharing and sender-controlled notifications- that aimed to decrease the negative effects of ill-timed notifications in smartphones [12]. Our study differs from these previous studies as we consider privacy concerns associated with notifications, rather than productivity cost of notifications.

2.3.1 Privacy concerns due to Notifications. Vardhan et al. [44] designed a classification engine for Android Smartphones to classify a notification into private or non-private while taking into account in user feedback. However, the study takes into account only notification content, title and the name of the parent application sending it to determine classification of notification as private or not. It does not make use of temporal context, context of audience in person's surroundings etc. Most closely related to our work is by Kim et al. [25] on examining information disclosure risks arising from email notifications to recommend social-context aware notification strategies. However, the study has only been performed in an enterprise environment in the scenario of a person receiving an email notification on notification- capable devices while attending a meeting. Hence, the research results can not be generalized to different countries, organisational cultures. Their research does not examine information disclosure risks for senders of emails and other people whose information might be contained in the email. Neither of these two studies consider various dimensions of notification privacy, such as intrusion and interruption, which our study includes.

3 METHOD

In order to understand the disruptive effects of smartphone notifications, especially those pertaining to user privacy, we conducted a survey. All study materials and procedures were reviewed and approved by Institutional Review Board (IRB) of our university. (See Supplementary Material for the complete study instrument and questionnaire.) The recruitment materials provided some background information about this study and required that participants be 18 years of age or older to participate in the survey. We presented participants with a study information sheet. Only those who explicitly consented to participate could proceed to the study. We included several measures within the study to ensure collection of high quality responses. At the beginning, we included a screening question asking participants if they intended to provide high quality answers. Within the study, we included two attention check questions. We set a browser cookie to reduce chances of multiple submissions by the same person. To avoid priming, we did not use the term 'privacy'

Table 1. Components of the questionnaire.

Topic	No. of questions
Notifications & Smartphone Features	5
Device Sharing Behavior	5
Last Notification	9
Negative Experiences	3
Content sensitivity for apps	6
MUIPC	1
Technical Efficacy	1
Demographics	11

anywhere within the study description. The following subsections provide the details of the study procedures, recruitment, and characteristics of the sample.

3.1 Questionnaire

The survey began by asking various background questions about smartphone device such as its operating system, settings enabled for lock screen notifications (Android) or notification previews (iOS) password protection mechanisms and who else apart from the primary user of the device could unlock it. Table 1 provides an overview of the questionnaire structure.

Next, we asked related questions about frequency of smartphone sharing, screen visibility to someone else, and participants' behaviors regarding device sharing. After that, participants were required to answer questions pertaining to the latest notification on their smartphone device, such as mode of delivery of notification, user's response to it, level of concern if someone else viewed it and if applicable, concern of the person whose information was included in notification.

Following these questions, we asked participants to answer how many instances of negative experiences they had faced in their lifetime due to their smartphone notifications. We then asked participants to elaborate on the most negative experience and mention the cause for it. Then, we asked a series of questions to understand user concerns for content from different types of apps.

Next, we collected responses to standard scales on information privacy concerns and technical expertise. We used validated scales from literature: (i) an instrument to measure information privacy concerns among mobile users provided by Xu et al. [49] to measure perceived surveillance and perceived intrusion dimensions of information privacy; (ii) an instrument to capture general digital difficulties experienced by participants provided by Anrijs et al. [10] to gauge technical expertise. The questionnaire concluded with standard demographics questions. Wherever applicable, we provided participants the option to enter explanatory details via open-ended responses. No questions were mandatory; participants could choose to skip any question they did not wish to answer.

3.2 Study Deployment

The questionnaire was iteratively tested and improved, first by the authors and then by a few others. We then conducted a pilot study with 10 participants to identify logistical problems and gain an initial understanding of participation. We administered the survey by providing a link to the online study on AMT crowd work platform. To limit the impact of cultural variation, we limited participation to those from the United States. We further restricted visibility of the study to

task approval rating of 95% or higher and at least 50 completed tasks to maximize the chances of receiving high quality responses.

At the end of the study, participants received a unique randomly generated code to be entered on AMT to receive compensation for completing the study. All those who entered the correct code and passed the attention check were paid a compensation of $1.80 for completing the study. With the mean time of study completion time was 19 minutes, the compensation translates to about $6/hour which is typical of AMT based studies and in line with the minimum wage for our state. We received a total of 275 responses between November 12, 2020 and December 1, 2020. We excluded 60 responses for not agreeing to the screening question for providing high quality answers and/or failing attention checks. We filtered out 2 additional responses because they originated from non-US IP addresses. After filtering, we were left with 213 complete and valid responses.

3.3 Demographics

Participants were between 18 to 70 years of age (median 35, mean 36.3). The gender distribution was- 61.32%(n = 130) reported identifying as male, 38.2%(n = 81) as female, and 0.47%(n = 1) did not specify their genders. Most participants were white (74.52%; n = 158) with the remaining covering a variety of ethnic backgrounds: 6.06%(n = 24) Asian, 11.32%(n = 24) Black or African American, 1.4%(n = 3) American Indian or Native American, 3.30%(n = 7) Hispanic , 1.4%(n = 3) Native Hawaiian or Pacific Islander,1.47%(n = 1) as multi-ethnic. 1.08%(n = 2) chose not to report their ethnicity. The participants came from diverse professions like construction, management, IT, business, media production, art, pharmaceutical, production, etc. Most participants were married (62.6%, n = 134), 30.8%(n = 66) not married yet, and others were separated, divorced, widowed or did not disclose. The number of people living in the household (including the participant) were: 15.42%(n = 33) one, 12.61%(n = 27) two, 20.09%(n = 43) three, 31.77%(n = 68) four, 10.75%(n = 23) five and 9.32%(n = 20) six or more. 87.38%(n = 187) respondents reported living in the United States for more than 10 years or all their lives. Most participants had completed at least some college education: High school diploma (5.60%, n = 12), Some college (12.62%, n = 27), College graduate (B.S., B.A., or other 4 year degree) (54.2%, n = 116), Master's degree (23.36%, n = 50) and Doctoral degree (1.40%, n = 3).

4 FINDINGS

In the current section, we elaborate upon user privacy violations and concerns due to smartphone notifications. We examine how these concerns vary based on content from different types of app categories and relate to device sharing behavior of participants. We then highlight interplay digital difficulties and control over smartphone device state through mechanisms such as silent mode, on user privacy experiences. To investigate these matters we used relevant descriptive and inferential statistics on the numeric data as described below. For the open-ended questions, we employed three independent coders, one of whom was the first author of the paper. Each coder first independently coded the open-ended responses based a list of themes generated by the first author after detailed examination of the responses. All discrepancies among the initial codes of the three coders were resolved via detailed discussion, ultimately resulting in full agreement across all coders.

4.1 Privacy concerns and violations due to smartphone notifications

We studied privacy breaches and concerns due to smartphone notifications. One of the key findings of our study is that the majority of the participants (63.2%, n = 134) reported facing at least one negative experience in their lifetime due to smartphone notifications, as shown in the Figure 1. Hence, about 60% of smartphone participants have faced at least one instance of negative experience due to smartphone notifications (RQ1). Most of the participants (51.4%, n = 109) faced 1-5 negative

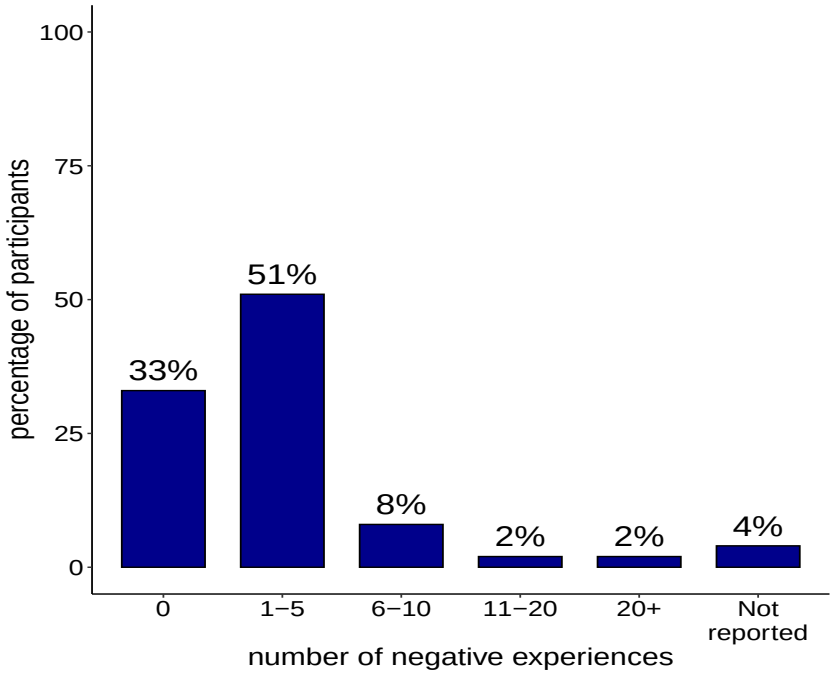

Fig. 1. Percentage of participants reporting number of times they faced negative experiences in their lives due to smartphone notifications. Around 63.2% ($n = 134$) participants reported facing at least one negative experience.

instances in their lifetime due to smartphone notifications. To understand how these negative experiences relate to privacy breaches, we analysed 95 responses received from the open-ended question that asked users to elaborate on the most negative experience. The themes that emerged from the responses answer our RQ1, as shown in Table 2. These are elaborated in the following subsections.

It can be seen that the four broad user-privacy violations arising due 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.
(4) invasions in social intimacy.

To understand if the instances of negative experiences due to notifications are associated with the type of smartphone (Android or iOS) operating system, we performed Mann-Whitney U Test with number of negative experiences as dependent variable and type of operating system as independent variable. We found no statistically significant differences in the number of negative experiences for Android and iOS ($p = 0.7449$).

4.1.1 Information disclosures due to notifications. We find that smartphone notifications deliver and disclose private content ($n = 22$), information about third-person ($n = 2$) and inappropriate content ($n = 7$). Inappropriate content refers to bad photos, videos, adult language, etc. These

Table 2. User privacy violations due to smartphone notifications.

Theme	Code	Count	Participant's comments
Information disclosure	Private content disclosed	21	"My girlfriend saw a message from one of my friends that was too private for her concern."
	Inappropriate content disclosed	9	"Someone sent me inappropriate photos without permission and my spouse seen them. She thought I was cheating."
	Content about third person was disclosed	2	"One of my friends read a message that was about her, and it made her upset."
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."
	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.," "It was adult language that a child (cousin) was able to read. I was watching a video with a younger cousin and the notification popped up."
Intrusion	Invasion (with undesired content, malware)	26	"one time i clicked the link on the notification received without studying in details resulted phone affected with virus."
	Invasion 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."
	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."
	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."
	High frequency of interruptions	14	"Just sometimes my friend likes to blow up iMessage and I get irritated or annoyed."
Intimacy breach	Invasion in a social intimacy	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."

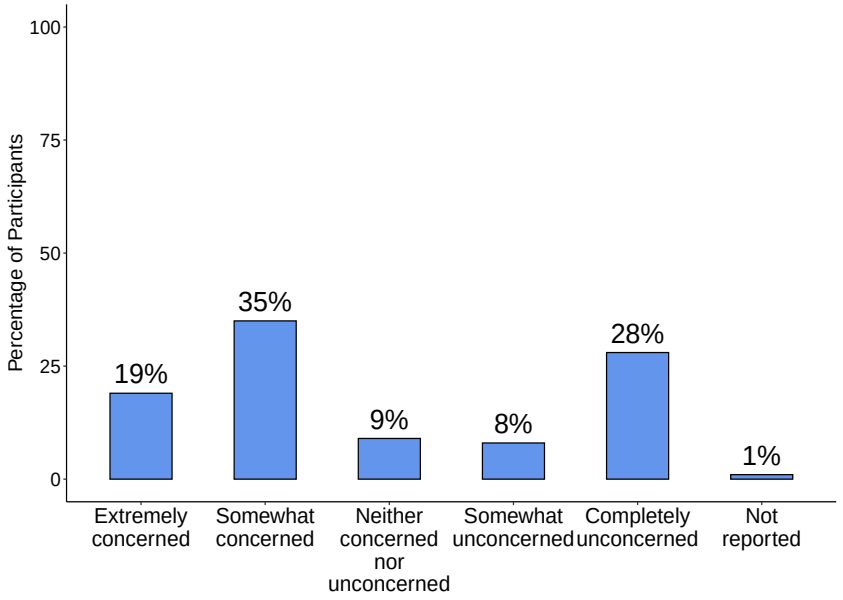

Fig. 2. Participants' concern level if someone else viewed the latest notification on their smartphone.

information disclosures often led to misunderstandings ($n = 4$) and conflicts with someone else ($n = 5$).

To identify the prevalence of risks of private information disclosure, we analysed the latest notification on the devices of participants. These notifications came from a wide variety of app categories like social media, instant messaging, news apps, e-commerce apps (like Amazon) and other types of apps like famisafe, notification bubbles, Learning Genie, Mixpanel, NUGAPP, amber alert, Line, discord, ola, okcupid, etc. Majority of the participants (54.2%, $n = 116$) reported that they were concerned (i.e. they selected somewhat concerned or extremely concerned on a 5-point Likert scale) if someone else viewed the content of the latest notification on their smartphone (Figure 2).

We then sought to identify the prevalence of risks of information disclosures about someone else. Out of total 212 participants, 87 participants mentioned that the last notification contained information pertaining to someone else. Around 72% (62/87) of these participants reported that the third person (whose information is contained in the notification) would be concerned (i.e., somewhat concerned or extreme concerned on a 5-point Likert scale) if someone other than the receiver saw the notification content, as shown in Figure 3. 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, as 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."
- "Someone sent me inappropriate photos without permission and my spouse seen them. She thought I was cheating."
- "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."

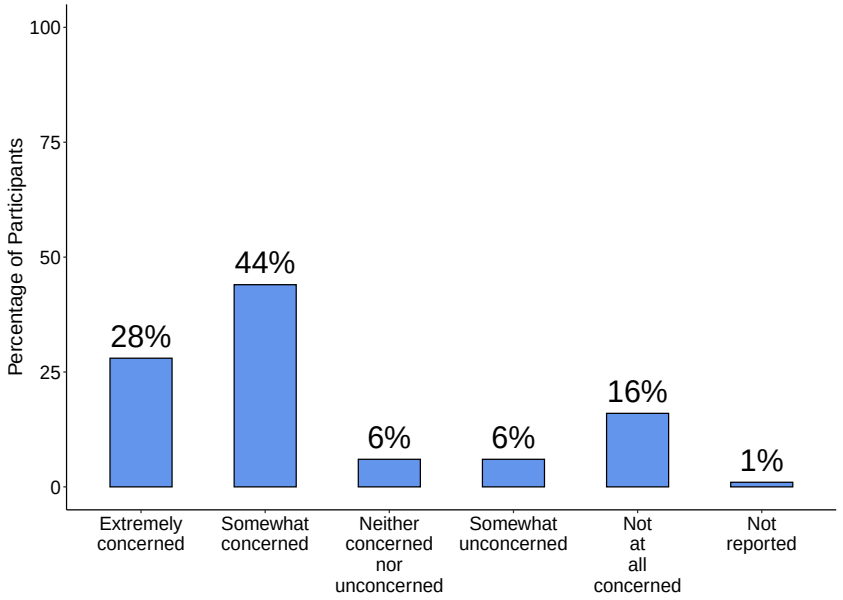

Fig. 3. Concern of the third party as perceived by the notification receiver if information about that party in the notification was seen by someone other than the notification receiver.

Table 3. 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 find that content from different apps cause different level of concerns when seen by a family member or a colleague, as shown is Figure 4 and Table 3. As per the Wilcoxon-Mann Whitney test the differences between the groups (family member and colleague) is statistically significant ($p < 0.05$) for all app categories except Dating; some apps categories that were also significant at $p < 0.01$ are: Instant Messaging, E-mail, Banking and payments.

Hence, we find 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 least sensitive.

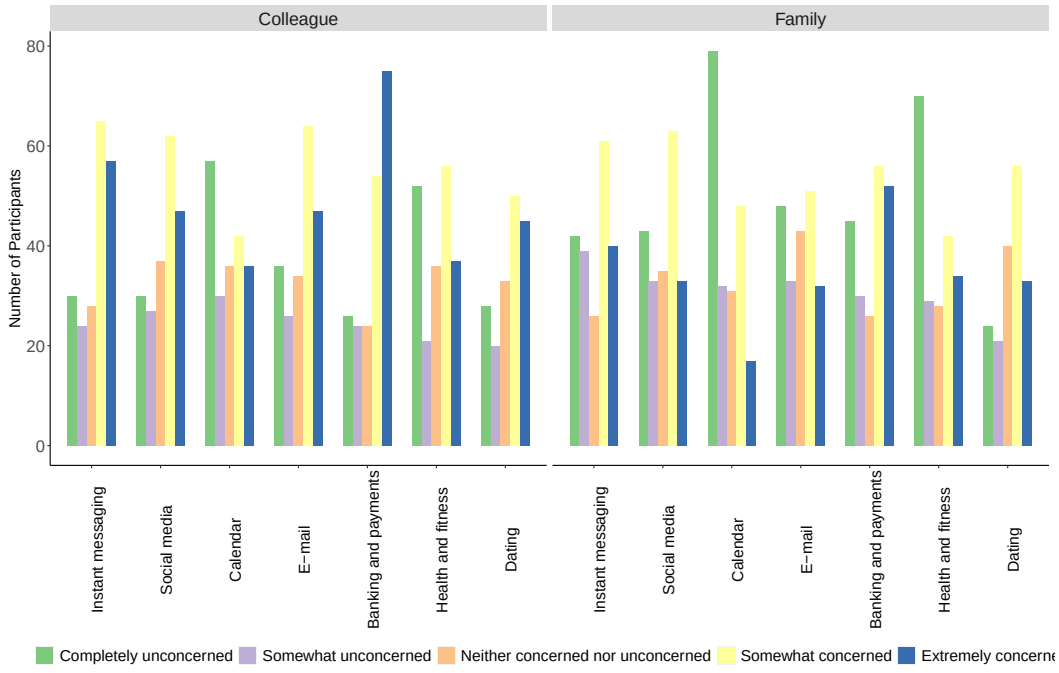

Fig. 4. Participants' concern if content from different app categories is read by either a colleague or a family member.

(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 Likert scale) by most respondents (n = 108). This is followed by Instant Messaging (n = 101).
(4) Around colleagues, content from Banking and Payment app category is seen as sensitive (i.e. participants responded with somewhat concerned or extremely concerned on 5-point Likert scale) by most respondents (n = 129). This is followed by Instant Messaging apps (n = 120).

4.1.2 Privacy invasions due to notifications. We define intrusion based on the work of Solove [43], who argues that 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). It is clear from participants' responses that smartphone notifications intrude privacy as they: cause distractions in task/ activity (n = 5), interrupt frequently (n = 7), interrupt in personal solitude (n = 6), invade in digital space (n = 14). Notifications also interrupt intimacy of social settings (n = 6). Intimacy refers to small group seclusion for members to achieve a close, relaxed, frank relationship, as defined in one of the four privacy states by Westin [47].

We describe 'invasion in digital space' as notifications that ping with unwanted content like scam links, fraudulent messages, virus links and unwanted advertisements; e.g., a user reported "some unwanted video notifications irritate me a lot time" and "Unwanted ads and information from social media" 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." Participants reported unwanted intrusions in social

Table 4. Mean scores of Perceived Intrusion and Perceived Surveillance constructs from MUIPC scale grouped by Instances of Negative Experiences.

Instances of Negative Experiences	Perceived Intrusion	Perceived Surveillance
0	14.62	14.91
1-2	15.38	15.49
3-5	15.96	16.11
6-10	16.50	16.81
11-20	18.33	17.00
More than 20	18.00	17.60

settings too due to notifications like, "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" and "notification ring in office meeting."

Table 4 shows the mean scores of 'Perceived Intrusion' and 'Perceived Surveillance' scale items from MUIPC scale for participants grouped by 'Instances of Negative Experiences' due to smartphone notifications. The spearman correlation coefficient value was 0.19 ($p = 0.007$). Kruskal-Wallis rank sum test shows 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 shared use. 46.73%($n = 100$) of the participants reported that shared their smartphone with their spouse at least once a day, as shown in Figure 5. 32.24%($n = 69$) participants shared with their smartphone device at least once a day with their siblings, 34.57% (N = 74) with their parents, 35.98%($n = 77$) with children above 13 years of age, 30.85%($n = 66$) with friends, 27.56%($n = 59$) with colleagues and 26.64%($n = 57$) with strangers. This confirms that the practice of phone sharing is prevalent in Americans, and is more frequent than it was past decade as seen in the study by Karlson et al [24].

50%($n = 107$) of the participants reported that someone else can view the contents of their smartphone notifications at least once a day, 28.04%($n = 60$) during meetings, 30.84%($n = 66$) at classes, 28.5%($n = 61$) at seminars and presentations, 28.98%($n = 62$) at cafeterias and restaurants, 28.97%($n = 62$) at social gatherings, 30.84%($n = 66$) at stores and markets and 25.7%($n = 65$) during public transport, as shown in Figure 6. A possible reason for these findings is that location characteristics have impact on users' attentiveness and receptivity to notifications and app usage, as confirmed in study by Mehrotra et al [29].

This frequent sharing of smartphone device or visibility of smartphone screen to someone other than the owner, gives rise to various user privacy concerns that participants reported. Some of them are as follows:

- "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."
- "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."
- "While giving my mobile to my sibling I forget to turn off the notification from my personal chat."

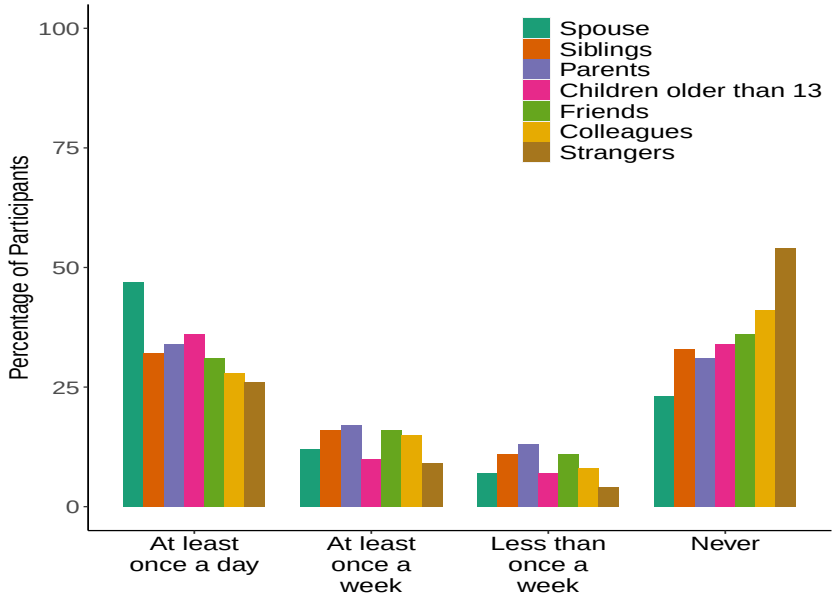

Fig. 5. Responses to the question: How frequently each respondent shares phone with (the listed) people?

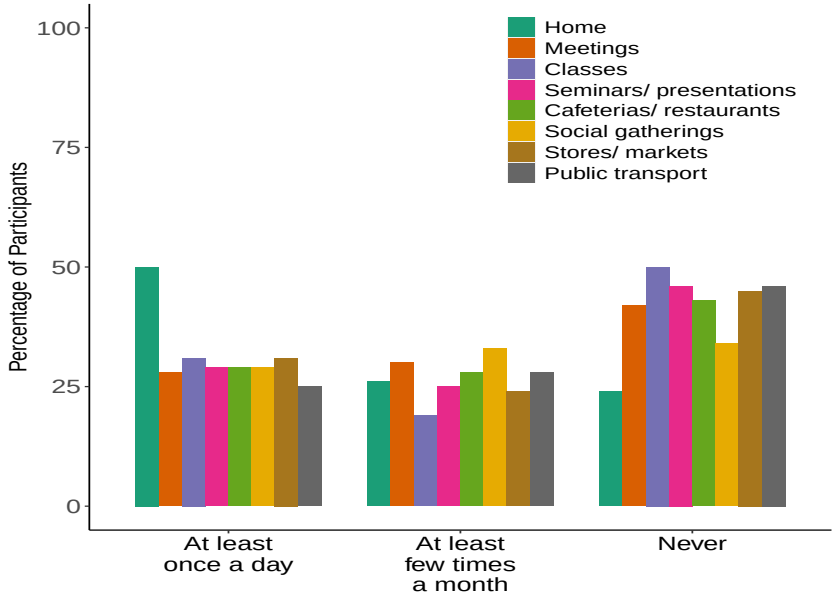

Fig. 6. Responses to the question: How frequently can someone else view the contents of notifications on your phone in any of the following places?

The prevalence of shared device use like smartphone sharing, screen casting, projecting screen towards someone else enhances user privacy concerns and risks. We report user behavior and preferences when they share their smartphones with someone else in Figure 7 and Figure 8. Around

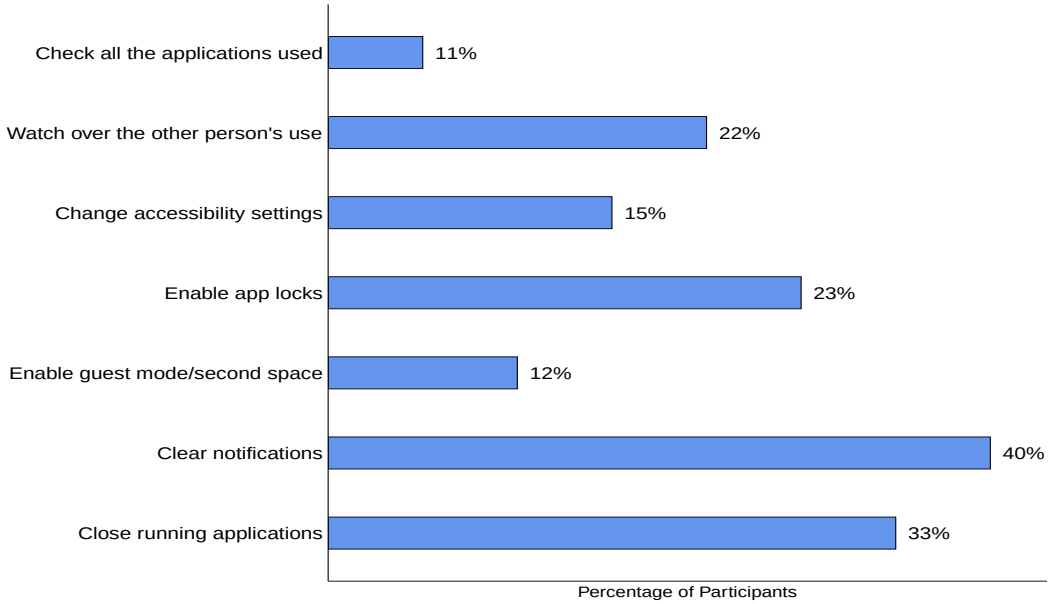

Fig. 7. User actions before handing over the device to someone else.

only 12% ($n = 25$) of the respondents mentioned that they used 'guest mode' and only 40% ($n = 85$) cleared notifications before handing over their smartphone to someone else. It is interesting to note that more than 75% of the participants did not clear their notifications before handing their device to a stranger.

Hence, users often compromise their privacy for short-term benefits like convenience as seen in previous studies (e.g., [3]). We find that the privacy paradox [35] exists in privacy management of smartphone notifications. Possible reason for the low use of privacy protective choices, such as switching to guest mode, is that users may not want to take conspicuous actions to decrease access, as that may come off as an act of distrust to the guest user. Additionally, a user may want someone else to see some specific information, which may not be accessible on the guest mode.

4.2 Control over smartphone state

We find that the use of various smartphone features to control device state, like Do Not Disturb (DND) mode, silent mode, turning off device, airplane mode and applications for notification management, is prevalent among smartphone users: 56.07% ($n = 97$) of the users reported the use of Do Not Disturb mode, 79.77% ($n = 138$) of silent mode, 44.5% ($n = 77$) turning off device, 42.77% ($n = 74$) airplane mode and 61.85% ($n = 107$) notification management apps in their smartphones for at least one hour in a typical day. The mean and median usage (in hours) of these smartphone features in a typical day is listed in Table 5. We find that users prefer to use silent mode and notification management apps over other alternative features to control their smartphone device and manage their notifications. A total of 53 participants elaborated their reasons for controlling device state through the mentioned smartphone features. The qualitative codes that emerge from various comments are shown in Table 6. Other reasons for using smartphone modes that participants reported were to save battery, to restart phone, while driving, while having lunch, only in special circumstances. It is interesting to note that participants find it helpful to make use of smartphone

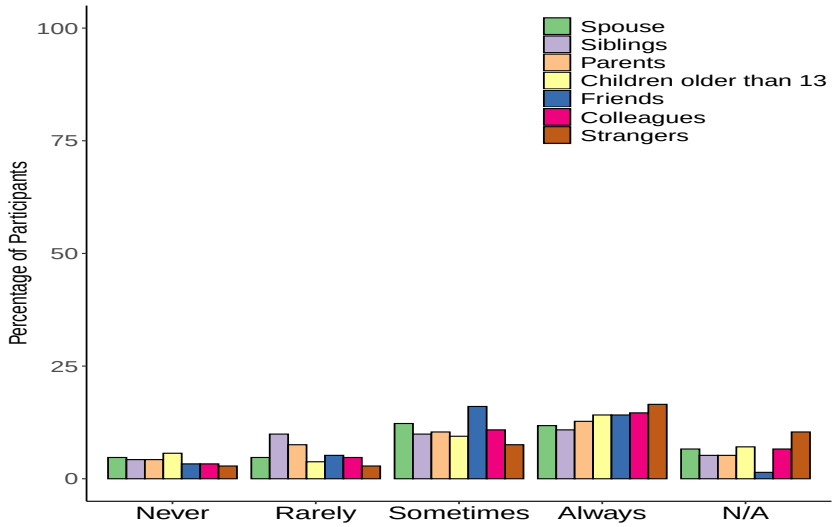

Fig. 8. Responses to the question: How frequently do you clear your notifications before handing your device to the listed people.

Table 5. Mean use of smartphone features (in hours)

Smartphone feature	Mean
Use **Do Not Disturb (DND)** Mode	2.85
Use **Silent** Mode	6.61
Turn off the device	2.19
Use **Airplane** mode	2.28
Use **notification management apps**	4.63

features to limit intrusions in personal space (e.g., while working and sleeping), in social settings (i.e. around someone else). However, participants do not report using such features to limit information disclosures, so it is unclear if they are helpful to mitigate information disclosure risks.

We find that present day smartphone features control interruptions in an all-or-none manner; though, Do Not Disturb (DND) mode allows users to make exceptions in case of incoming call, it doesn't not offer such customisation for notifications. Such binary control over smartphone state comes at the risk of missing out interruptions made in emergency situations. Interruptions from smartphone comes at the risk of decreasing its usability as various participants reported attending to their smartphone device only at their own accord, e.g., a participant mentioned "I always keep it on but I normally have it in another room so I don't hear or see it until I go back into that room. My phone isn't that important to me.ding"

We then try to understand how the use of various 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, as shown in Table 7. Kruskal-Wallis rank sum test shows significant statistical differences in use of Do Not Disturb mode ($p < 0.01$), silent mode ($p < 0.05$), turning off device ($p < 0.05$),

Table 6. User preferences for controlling device state

Theme	Code	Count	Participant's comment
Prefer to control device state	to avoid ring of phone from notifications/ calls	6	"I don't 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."
	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."
	during sleep	17	"I will use silent mode while sleeping daily," "some mid night calls are coming so i am off the airplane mode."
	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."
	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."
	customize notification settings	4	"I just set custom individual notification settings for most of my apps. If they're atrociously annoying I uninstall them.," "…I do use a notification manager from samsung to group notifications."
	other reasons	5	"…While in office hours I use Do Not Disturb mode. Device is off while eating lunch."
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."
	to stay alert to notifications	4	"I prefer to get all alerts and notifications when the arrive, regardless of the time of day."
	other reasons	7	"I never use any of the services mentioned, because I don't see the need for them.," "Since I live alone and I usually don't get late calls I leave cell on. I also leave on in case someone has an emergency."

use of airplane mode($p < 0.005$), use of notification management apps ($p < 0.001$) on instances of negative experiences. Hence, we find that the mean use of smartphone mechanisms increases till 10 instances of negative experiences as participants who had more negative experience would try to keep more control of their device state for preventing future negative experiences; it decreases after 10 negative instances as participants who had faced more negative experiences may reduce their effort or were unable (due to digital difficulties) in managing their device. In the following subsection we verify if digital difficulties play a role in the instances of negative experiences.

We calculated the correlation of the hourly use of each smartphone mechanism with the instances of negative experience, as shown in Table 8. The p values were adjusted using Bonferroni correction.

Table 7. Negative Experiences and Mean use of features (in hours)

Negative Experiences Occurrences	DND Mode	Silent Mode	Turn Off	Airplane Mode	Notification Apps
0	1.64	6.11	1.05	1.08	2.18
1-2	2.81	5.47	1.49	1.43	4.85
3-5	2.98	6.18	2.91	2.82	5.86
6-10	7.75	10.25	7.81	9.50	11.81
11-20	6.50	5.75	5.25	5.75	4.25
More than 20	2.2	4.20	0.40	0.20	2.00

Table 8. Correlation of use of smartphone features and occurrences of negative experiences due to notifications.

Smartphone Mode	Correlation values	Adjusted p-values
Use **Do Not Disturb (DND)** Mode	0.29	0.014
Use **Silent** Mode	0.033	1.00
Turn the device **off**	0.27	0.028
Use **Airplane** mode	0.28	0.024
Use notification management apps	0.26	0.036

It can be seen that weak correlation occurs in the use of Do Not Disturb Mode, Turning device off, use of airplane mode and use of notification management apps with instances of negative experiences by significant p values (less than 0.05). Therefore, it can be said that tendency to control smartphone is related to facing negative experiences due to notifications. This is interesting to note as learning user preferences for controlling smartphone can aid in training better prediction algorithms for privacy protective notifications.

4.2.1 Digital difficulties. We quantified how much someone encounters digital difficulties or experiences problems in using a smartphone or computer using a validated scale developed by Anrijs et al. [10]. We present the mean score of participants grouped by the number of instances of negative experiences in Table 9, higher score implies more digital difficulties and less digital proficiency. It can be seen that the users who do not face any negative experience with notifications face less difficulties in operating digital devices as compared to people who have faced at least one negative experience. Participants who face large number of negative experiences (more than 10) face less digital difficulties (i.e. more digitally proficient) than participants who face moderate (1-10) instances of negative experiences. Hence, the reason for decrease in use of smartphone control mechanisms by participants facing large (more than 10) instances of negative experiences, can not be attributed to their digital proficiency; the most plausible reason is their reduced effort in managing their device.

5 IMPLICATIONS

Our findings suggest a number of design recommendations for helping users optimize the benefit-privacy trade offs related to mobile device notifications:

Table 9. Digital difficulties score grouped by instances of negative experiences due to smartphone notifications.

Instances of negative experiences	mean score	median score	standard deviation
0	10.61	8.00	6.49
1-2	15.70	18.00	6.51
3-5	15.75	18.00	6.26
6-10	18.19	19.00	4.65
11-20	14.75	15.50	9.11
More than 20	11.80	8.0	8.11

5.1 Limit the number of notifications

Various participants reported feeling uneasy and uncomfortable due to notification intrusions. Participants experienced negative emotions, like annoyance and irritation, due to high frequency of notifications. Hence, limiting the number of notifications delivered to smartphone users will decrease digital intrusions from unwanted content, reduce intrusions in personal solitude and increase usability of notifications. We recommend some of the following ways to limit the number of notifications:

(1) Notify a user only when specific user defined key words are present in the notification content; e.g., *urgent, OTP, update, important* can be some of the key words which users find important. This feature can specifically be added to instant messaging apps, which often contain personal information and drive up notification response due to perceived social pressure [40].
(2) Notifications can be bundled together and be displayed only after user set time interval, like after every 3 hour, or at fixed times of the day, say 12 noon and 6 p.m.
(3) Various apps, specifically social media and instant messaging apps, can be allowed to sent not more than a set amount of notifications in an interval, e.g. up to 3 notifications in an hour.

5.2 Allow easy disabling of notifications

Many users in our study reported facing trouble because of high frequency of notifications on their device and notification interruptions during sleeping hours. The current smartphones offer ways to silence phone ring through features like turning off device,silent mode, etc. However, they also silence the ring of phone, thereby having users prone to missing important calls or text messages. For example, a participant reported- "I keep it on just in case there's an emergency and someone is trying to get hold of me."

Therefore, we recommend a handy feature to 'turn off all notifications,' including notification sound and vibration, similar to the feature of changing device ring type to silent mode. A simple button in the device hardware or software that lies under the owner's easy grasp to disable notifications will be convenient and inconspicuous to use in front of someone else. Additionally, a feature to password protect notification drawer (Android) or notification center (iOS) will aid in reducing privacy risks.

5.3 Personalize notification content and frequency of delivery

A user 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 to developers to allow users to opt in for notifications for only the most preferred content from an app. In this regard, the recent updates to the Android operating system (Android 8.0 Oreo and above) is worth studying in detail as it gives users more control over app notifications through 'channels,' which are categories that users can individually turn on and off at any time, for instance, Twitter could create separate channels for mentions, likes, follows, etc. [15].

Additionally, machine learning algorithms can be deployed to predict opportune situations to deliver notifications, based on user concern for different types of app content, sensing the presence of people around, time of the day.

5.4 Ease user privacy concerns for device sharing

Our study reveals that notifications cause unintended information disclosures during shared use of smartphones. Therefore, we recommend a feature in smartphone to automatically turn off notification pop ups after detecting if the device is handed over to someone else, screen is cast or multiple people are watching from the phone screen. Machine learning algorithms could be trained based on features such as person handling the device, temporal context (e.g., turn off notification during sleeping hours), sensor readings from environmental context [33] etc., to train algorithms to anonymize sensitive content.

6 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 regarding notification content and user practices regarding interacting with the notifications.

Moreover, our sample consists of individuals from the United States. Generalizability to other cultures requires verification. Apart from privacy concerns, device sharing practices, in particular, are likely to differ substantially in developing nations because of differences in various sociocultural factors.

Moreover, our investigation was focused on mobile devices (smartphones, in particular). With increasing adoption of smart devices (i.e., Internet of Things (IoT)), it would be interesting to examine how these results compare with notifications from such devices embedded in a user's physical environment.

7 CONCLUSION

Users of mobile devices receive dozens and sometime hundreds of notifications everyday. These notification carry wide variety of, and potentially sensitive, content from different apps stored on the device or from online websites, which is at the risk of being visible to people present around the receiver. It is crucial to counter the effects of notifications on user privacy to ensure their utility. With the broad objective of suggesting privacy and convenience optimising notification delivery strategies, we explore various privacy considerations associated with smartphone notifications. We found that privacy breaches from smartphone notifications occur in three different ways- information disclosures, leaks during shared use of device or device screen and intrusion. We also highlight how the use of smartphone control mechanisms such as silent mode, digital proficiency and content from different apps relate to privacy considerations. Finally, we note that our study can be helpful in designing privacy protective smartphone features and machine learning algorithms for notification delivery.

REFERENCES

[1] [n.d.]. .

[2] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce* (Denver, Colorado, USA) *(EC '99)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/336992.336995

[3] A Acquisti and J Grossklags. 2005. Privacy and rationality in individual decision making. IEEE Secur. Priv. 3 (1), 26–33 (2005).

[4] Piotr D. Adamczyk and Brian P. Bailey. 2004. If Not Now, When? The Effects of Interruption at Different Moments within Task Execution. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vienna, Austria) *(CHI '04)*. Association for Computing Machinery, New York, NY, USA, 271–278. https://doi.org/10.1145/985692.985727

[5] 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

[6] 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

[7] 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.

[8] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-Based Authentication Schemes. 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, 316–322. https://doi.org/10.1145/2785830.2785882

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

[10] 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.

[11] 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

[12] 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

[13] Edward B Cutrell, Mary Czerwinski, and Eric Horvitz. 2000. Effects of instant messaging interruptions on computing tasks. In *CHI'00 extended abstracts on Human factors in computing systems*. 99–100.

[14] Mary Czerwinski, Edward Cutrell, and Eric Horvitz. 2000. Instant messaging: Effects of relevance and timing. In *People and computers XIV: Proceedings of HCI*, Vol. 2. 71–76.

[15] 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].

[16] 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

[17] 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

[18] Susan Farrell. 2016. Computer-Assisted Embarrassment. https://www.nngroup.com/articles/embarrassment/ [Online; posted 27-August-2012].

[19] 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

[20] 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

[21] 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

[22] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 213–230.

[23] Edward Cutrell Mary Czerwinski Eric Horvitz. 2001. Notification, disruption, and memory: Effects of messaging interruptions on memory and performance. In *Human-Computer Interaction: INTERACT*, Vol. 1. 263.

[24] 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

[25] 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

[26] Kostadin Kushlev, Jason Proulx, and Elizabeth W. Dunn. 2016. *"Silence Your Phones": Smartphone Notifications Increase Inattention and Hyperactivity Symptoms*. Association for Computing Machinery, New York, NY, USA, 1011–1020. https://doi.org/10.1145/2858036.2858359

[27] 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

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

[29] Abhinav Mehrotra, Sandrine R. Müller, Gabriella M. Harari, Samuel D. Gosling, Cecilia Mascolo, Mirco Musolesi, and Peter J. Rentfrow. 2017. Understanding the Role of Places and Activities on Mobile Phone Interaction and Usage Patterns. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 84 (Sept. 2017), 22 pages. https://doi.org/10.1145/3131901

[30] 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

[31] Abhinav Mehrotra, Veljko Pejovic, Jo Vermeulen, Robert Hendley, and Mirco Musolesi. 2016. My Phone and Me: Understanding People's Receptivity to Mobile Notifications. 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, 1021–1032. https://doi.org/10.1145/2858036.2858566

[32] 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

[33] 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

[34] Leanne G Morrison, Charlie Hargood, Veljko Pejovic, Adam WA Geraghty, Scott Lloyd, Natalie Goodman, Danius T Michaelides, Anna Weston, Mirco Musolesi, Mark J Weal, et al. 2017. The effect of timing and frequency of push notifications on usage of a smartphone-based stress management intervention: an exploratory trial. *PloS one* 12, 1 (2017), e0169162.

[35] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.

[36] Brid O'Conaill and David Frohlich. 1995. Timespace in the workplace: Dealing with interruptions. In *Conference companion on Human factors in computing systems*. 262–263.

[37] 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

[38] 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

[39] 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 & amp; Services* (Toronto, ON, Canada) *(MobileHCI '14)*. Association for Computing Machinery, New York, NY, USA, 233–242. https://doi.org/10.1145/2628363.2628364

[40] Martin Pielot, Rodrigo De Oliveira, Haewoon Kwak, and Nuria Oliver. 2014. Didn't you see my message? predicting attentiveness to mobile instant messages. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3319–3328.

[41] 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.

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

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

[44] 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

[45] 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.

[46] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. 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, 2367–2376. https://doi.org/10.1145/2556288.2557413

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

[48] Atilla Wohllebe. 2020. Consumer Acceptance of App Push Notifications: Systematic Review on the Influence of Frequency. (2020).

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

[50] 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

(I) **Introduction**

(1) We care about the quality of our data. In order for us to get the most accurate measures of your knowledge and opinions, it is important that you thoughtfully provide your best answers to each question in this study.
Will you provide your best answers to each question in this study?
(i) I will provide my best answers.
(ii) I will not provide my best answers.
(iii) I can not promise either way.

(II) **Background**

Note: Please answer the questions in this questionnaire as they pertain to your primary smartphone and your practices during typical (i.e., NON-COVID) times.

(1) What is the Operating System (OS) of your phone?
(a) Android
(b) iOS
(c) Other. (Please specify:) [text box]

(2) Does your device use any type of lock (e.g., PIN, password, pattern, fingerprint, faceID, etc.)?
(i) Yes

(ii) No
(iii) Don't know

(3) If 'Yes' is selected for previous question- "Does your device use any type of lock (e.g., PIN, password, pattern, fingerprint, faceID, etc.)?" then ask- Who other than you can unlock your device? (Select all that apply.)
(i) Parents
(ii) Spouse
(iii) Siblings
(iv) Friends
(v) Children older than 13
(vi) Other family members
(vii) Colleagues
(viii) Other. (Please specify:) [text box]

(4) If 'Android' is selected for question- "What is the Operating System (OS) of your phone?" then ask- What settings have you enabled for lock screen notifications?
(i) Show All
(ii) Hide Sensitive
(iii) Hide All
(iv) I don't know

(5) If 'iOS' is selected for question- "What is the Operating System (OS) of your phone?" then ask- What option have you enabled for notification previews?
(i) Always
(ii) When unlocked
(iii) Never
(iv) I don't know

(6) If 'iOS' is selected for question- "What is the Operating System (OS) of your phone?" then ask- For the most frequently used app in each of the following categories, what option have you enabled for 'Show Previews'? [Choose one from the options: Always, When unlocked, Never, Notification disabled, I don't know, N/A]
(i) Instant messaging
(ii) Social media
(iii) Calendar
(iv) E-mail
(v) Banking and payments
(vi) Work based or professional purposes
(vii) Travel and navigation
(viii) Health and fitness
(ix) Dating

(III) **Notifications and smartphone features**

(1) How many notifications have you received in the last hour? NOTE: Include all types of notifications (i.e. app icon badges, notification center, lock screen, and banners).
(i) 0
(ii) 1 to 9
(iii) 10 to 19
(iv) 20 to 29
(v) 30 or more

(2) On a typical day, how frequently do you pick up your phone to check, clear, or address notifications?

(i) Once in about 5 minutes
(ii) Once in about 15 minutes
(iii) Once in about 30 minutes
(iv) Once in about 1 hour
(v) Once in about 3 hours
(vi) Once in about 6 hours
(vii) Once in about 12 hours
(viii) Once in about 24 hours
(ix) Whenever a notification is delivered
(x) Something else. (Please specify:) [text box]

(3) Does your screen wake up when a notification is delivered?
(i) Never
(ii) Sometimes
(iii) About half the time
(iv) Most of the time
(v) Always
(vi) Do not know

(4) For each of the following actions, mention how many hours in a typical day (from 0 to 24) you use it.
(i) Use Do Not Disturb (DND) Mode [a list of numbers from 0 to 24]
(ii) Use Silent mode [a list of numbers from 0 to 24]
(iii) Switch off the device [a list of numbers from 0 to 24]
(iv) Use Airplane mode [a list of numbers from 0 to 24]
(v) Use notification management apps [a list of numbers from 0 to 24]

(5) Mention the most frequently used Google service or product on your primary smartphone device. To ensure that you are participating attentively, please select the 'Translate' option. [Attention Check Question]
(i) Docs
(ii) Hangouts
(iii) Maps
(iv) Photos
(v) Scholar
(vi) Sheets
(vii) Slides
(viii) Translate
(ix) Other. (Please mention:) [Text Box]

(6) Please explain your reasons for the answers to the previous question. (Optional) [an essay type text box]

(IV) **Device sharing behaviour**

(1) How frequently can someone else view notifications on your phone in any of the following places? (Choose one from the scale: Never, Few times a month, Few times a week, Once a day, Few times a day)
(i) Home
(ii) Public Transport
(iii) Cafeterias and restaurants
(iv) Meetings
(v) Seminars and presentations
(vi) Stores and markets

(vii) Classes
(viii) Others. (Please specify:) [text box]
(2) How frequently do you share your phone with the following people? (Choose one from the scale: Never, Less than once a week, Few times a week, Multiple times a week, Once a day, Few times a day, Multiple times a day and N/A.)
(i) Spouse
(ii) Siblings
(iii) Parents
(iv) Children older than 13
(v) Friends
(vi) Other family members
(vii) Colleagues
(viii) Strangers
(3) Please explain your reasons for the answers to the previous question. (Optional) [Text Box]
(4) When you hand over your smartphone to someone else, which of the following actions do you take? (Select all that apply.)
(i) Nothing
(ii) Close running applications
(iii) Clear notifications
(iv) Enable guest mode or second space
(v) Enable app locks
(vi) Change accessibility settings
(vii) Watch over the other person's use of the phone
(viii) Check all the applications used by the person
(ix) Other. (Please specify:)[text box]
(5) If 'Clear notifications' is selected in previous question, "When you hand over your smartphone to someone else, which of the following actions do you take?", then ask- Do you clear notifications from screen before handing over your phone to the following people? (Choose one from the scale: Never, Rarely, Sometimes, Always and N/A.)
(i) Spouse
(ii) Siblings
(iii) Parents
(iv) Children older than 13
(v) Friends
(vi) Other family members
(vii) Colleagues
(viii) Strangers

(V) **Last Notification**

Think about the latest notification that you received on your smartphone. Please answer the following questions with respect to that notification.

(1) Which app sent the notification? [Text Box]
(2) If 'Android' is selected for question, "What Operating System (OS) is used by your phone?", then ask- How do you receive notifications from this app? (Select all that apply.)
(i) Lock Screen
(ii) Notification drawer
(iii) Floating notification
(iv) App Badge
(v) Do not know

(vi) Other. (Please specify:) [Text Box]
(3) If 'iOS' is selected for question, "What Operating System (OS) is used by your phone?", then ask- How do you receive notifications from this app? (Select all that apply.)
(i) Lock Screen
(ii) Notification center
(iii) Banner (permanently)
(iv) Banner (temporarily)
(v) App Badge
(vi) Do not know
(vii) Other. (Please specify:) [Text Box]
(4) How quickly did you address the notification after you first saw it?
(i) within a minute
(ii) within 5 minute
(iii) within 30 minute
(iv) within an hour
(v) within 6 hours
(vi) within 12 hours
(vii) within 24 hours
(viii) Other. (Please specify:) [Text box]
(5) What action did you take when you first became aware that you had received this notification?
(i) Read the notification preview (title)
(ii) Read the notification content
(iii) Cleared it from the phone lock screen
(iv) Cleared it from the notification center/ drawer
(v) Opened the relevant app to address the notification
(vi) Did not do anything
(vii) Prevented further notifications from the app (Please tell us how:) [Text box]
(viii) Other. (Please specify:) [Text box]
(6) How concerned would you be if someone else viewed this notification? [Choose from a 5-point Likert Scale ranging from Extremely concerned to Completely unconcerned]
(7) Please explain your reasons for the answers to the previous question. (Optional) [Text Box]
(8) Did this notification include information pertaining to another person?
(i) Yes
(ii) No
(iii) Other. (Please specify:) [Text box]
(9) If 'Yes' is selected for previous question, "Did this notification include information pertaining to another person?", then ask- How concerned do you think the person would be if the content of the notification was seen by someone other than you? [Choose from a 5-point Likert Scale ranging from Extremely concerned to Extremely unconcerned]

(VI) **Negative Experience with Notifications**

(1) How many times have you experienced negative experiences related to notifications?
(i) 0
(ii) 1-2
(iii) 3-5
(iv) 6-10
(v) 11-20
(vi) More than 20

(2) Of the negative experiences related to notifications that you have encountered, please tell us a bit about the most negative experience. [text box]
(3) If '0' is not selected in previous question, "How many times have you experienced negative experiences related to notifications? 0 Is Not Selected", then ask- What caused the negative experience?
  (i) I had given my phone to someone else when the notification arrived.
  (ii) I left the phone screen unlocked.
  (iii) I forgot to take appropriate actions to silence the notification.
  (iv) I was screen casting / projecting the device display to others (e.g., in a presentation) when the notification popped up on screen.
  (v) The notification included sensitive content. (Please specify:) [Text Box]
  (vi) Others. (Please specify:) [Text Box]

(VII) **Content sensitivity for different app categories**

Reminder: Please answer the questions in this questionnaire as they pertain to your primary smartphone and your practices during typical (i.e., NON-COVID) times.

(1) How concerned would you be if a family member reads the content of a notification from each of the app categories listed below? [Choose from a 5-point Likert Scale ranging from Extremely concerned to Extremely unconcerned or N/A.]
  (i) Instant messaging
  (ii) Social media
  (iii) Calendar
  (iv) E-mail
  (v) Banking and payments
  (vi) Health and fitness
  (vii) Dating
(2) Please explain your reasons for the answers to the previous question. (Optional) [Text Box]
(3) How concerned would you be if a colleague reads the content of a notification from each of the listed app category? [Choose from a 5-point Likert Scale ranging from Extremely concerned to Extremely unconcerned or N/A.]
  (i) Instant messaging
  (ii) Social media
  (iii) Calendar
  (iv) E-mail
  (v) Banking and payments
  (vi) Health and fitness
  (vii) Dating
(4) Please explain your reasons for the answers to the previous question. (Optional) [Text Box]
(5) Mention the most frequently used Google product. To ensure that you are participating attentively, please select the 'Translate' option. [Attention check question]
  (i) Docs
  (ii) Hangouts
  (iii) Maps
  (iv) Photos
  (v) Scholar
  (vi) Sheets
  (vii) Slides
  (viii) Translate
  (ix) Other. (Please mention:) [Text Box]

(6) Have you enabled additional locking (e.g., PIN, password, etc.) for any of the following categories of apps? (Select all that apply.) NOTE: We are asking about locking that you enabled on your own, separate from the screen lock for the device or a mandatory lock/login forced by the app.
  (i) Instant messaging
  (ii) Social media
  (iii) Calendar
  (iv) E-mail
  (v) Banking and payments
  (vi) Health and fitness
  (vii) Dating
  (viii) Apps for work
  (ix) Travel and navigation
  (x) None

(VIII) **Measuring mobile users' concerns for information privacy** [49]
(1) Please indicate your level of agreement with the following statements: [Choose one option from 7 point Likert-Scale ranging from Strongly Agree to Strongly Disagree.]
  (i) I believe that the location of my mobile device is monitored at least part of the time.
  (ii) I am concerned that mobile apps are collecting too much information about me.
  (iii) I am concerned that mobile apps may monitor my activities on my mobile device.
  (iv) I feel that, as a result of my using mobile apps, others know about me more than I am comfortable with.
  (v) I should select somewhat agree for this question. [attention check question]
  (vi) I believe that, as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.
  (vii) I feel that, as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.

(IX) **Technical Efficacy** [10]
(1) Please indicate your level of agreement with the following statements: [Choose one option from: Never, Rarely, Sometimes, Always and N/A.]
  (i) In general, I often have difficulty when using my smartphone, apps, websites, or computer programs.
  (ii) In general, I am not able to solve questions or problems on my own when using my smartphone, apps, websites, or computer programs.
  (iii) In general, I need support when trying out something new on my smartphone or computer.
  (iv) In general, I find it hard to adjust settings of my smartphone, apps, websites, or computer programs (for example, privacy or safety settings).
  (v) In general, I often have questions or problems when using my smartphone, apps, websites or computer programs after an update has been done.

(X) **Demographics**
Finally, please tell us a bit about yourself:
(1) What is your year of birth? [a list of years from 2010 to 1920]
(2) What is your gender?
  (i) Male
  (ii) Female
  (iii) Non-binary
  (iv) Prefer to self-describe: [Text Box]

(v) Prefer not to disclose
(3) What is your ethnic background? (Select all that apply.)
(i) American Indian or Native American
(ii) Asian
(iii) Black or African American
(iv) Native Hawaiian or Pacific Islander
(v) White
(vi) Hispanic
(vii) Other. (Please specify:) [Text Box]
(viii) Prefer not to say
(4) What is the highest level of education you have completed?
(i) Less than high school
(ii) High school diploma
(iii) Vocational training
(iv) Some college
(v) College graduate (B.S., B.A., or other 4 year degree)
(vi) Master's degree
(vii) Doctoral degree
(viii) Professional degree after college (e.g., law or medical school)
(ix) Other. (Please specify:) [Text Box]
(x) Prefer not to say
(5) What is your current employment status? (Select all that apply.)
(i) Employed full time
(ii) Employed part time
(iii) Unemployed looking for work
(iv) Unemployed not looking for work
(v) Homemaker
(vi) Student
(vii) Retired
(viii) Disabled
(ix) Other. Please specify: [Text Box]
(x) Prefer not to say
(6) If 'Employed full time' or 'Employed part time' or 'Unemployed looking for work' is selected for question "What is your current employment status?", then ask- What is your current employment status? What is your profession? [Text Box]
(7) If 'Student' is selected for question "What is your current employment status?" then ask- What is your field of study? [Text Box]
(8) What is your current annual household income before taxes?
(i) Less than $10,000
(ii) $10,000 to $19,999
(iii) $20,000 to $29,999
(iv) $30,000 to $39,999
(v) $40,000 to $49,999
(vi) $50,000 to $59,999
(vii) $60,000 to $69,999
(viii) $70,000 to $79,999
(ix) $80,000 to $89,999
(x) $90,000 to $99,999

(xi) More than $100,000
(xii) Prefer not to disclose

(9) How many years have you lived in the United States of America? [List of numbers from 1 to 10 and the option- 'More than 10 or All my life']
(10) Including yourself, how many people live in your household? [List of numbers from 1 to 10 and the option- 'More than 10']
(11) What is your current marital status?
(i) Married
(ii) Widowed
(iii) Divorced
(iv) Separated
(v) Never Married
(vi) Prefer not to disclose
(vii) Other. (Please specify:) [Text Box]

(XI) **Closing**

(1) Is there anything else you would like to tell us? [Text Box]