

Studying Preferences and Concerns about Information Disclosure in Email Notifications

Yongsung Kim*
Northwestern University
Evanston, IL
yk@u.northwestern.edu

Adam Fourney
Microsoft Research
Redmond, WA
adamfo@microsoft.com

Ece Kamar
Microsoft Research
Redmond, WA
eckamar@microsoft.com

ABSTRACT

People receive dozens, or hundreds, of notifications per day and each notification poses some risk of accidental information disclosure in the presence of others; onlookers may see notifications on a mobile phone lock screen, on the periphery of a desktop or laptop display. We quantify the prevalence of these accidental disclosures in the context of email notifications, and we study people's relevant preferences and concerns. Our results are compiled from a retrospective survey of 131 respondents, and a contextual-labeling study where 169 participants labeled 1,040 meeting-email pairs. We find that, for 53% of people, at least 1 in 10 email notifications poses an information disclosure risk, and the real or perceived severity of these risks depend both on user characteristics and the meeting or email attributes. We conclude by exploring machine learning for predicting people's comfort levels, and we present implications for the design of future social-context aware notification systems.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → *Empirical studies in ubiquitous and mobile computing*.

KEYWORDS

Notifications, information disclosure, privacy, virtual assistants

ACM Reference Format:

Yongsung Kim, Adam Fourney, and Ece Kamar. 2019. Studying Preferences and Concerns about Information Disclosure in Email Notifications. In *Proceedings of the 2019 World Wide Web Conference (WWW '19)*, May 13–17, 2019, San Francisco, CA, USA. ACM, New York, NY, USA, 11 pages. <https://doi.org/10.1145/3308558.3313451>

1 INTRODUCTION

Estimates suggest that people receive dozens, or hundreds, of notification messages per day [21, 30, 31] delivered to a range of connected devices that people carry with them, or that are ever-present in the environment (e.g., wearables, smartphones, computers or – increasingly – internet of things devices). Extensive prior research has explored the productivity costs of mal-timed notifications [13, 20, 21], but little is known about the privacy cost of such

*Work done while at Microsoft Research.

This paper is published under the Creative Commons Attribution 4.0 International (CC-BY 4.0) license. Authors reserve their rights to disseminate the work on their personal and corporate Web sites with the appropriate attribution.

WWW '19, May 13–17, 2019, San Francisco, CA, USA

© 2019 IW3C2 (International World Wide Web Conference Committee), published under Creative Commons CC-BY 4.0 License.

ACM ISBN 978-1-4503-6674-8/19/05.

<https://doi.org/10.1145/3308558.3313451>

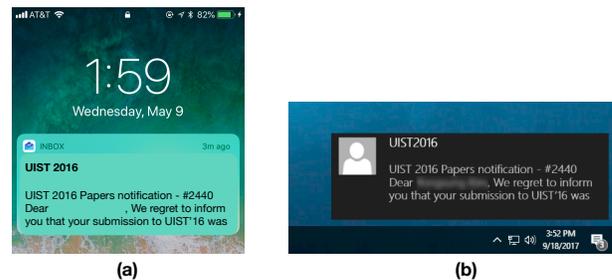


Figure 1: An example of an email notification on an iPhone (a) and on a computer with Windows 10 (b). The notification reveals the email's sender, subject, and first sentence from the message body. When in the presence of others (e.g., during meetings), users may be uncomfortable receiving notifications and revealing these data to onlookers.

messages; people are frequently in the presence of others when notifications arrive, and, in these contexts, each notification poses some risk of accidental information disclosure. For example, email notifications often reveal the sender and subject fields of messages, and may be visible above the lock screen of a mobile phone (Figure 1a), on the periphery of a co-located desktop or laptop (Figure 1b), on a projection screen during a presentation, or on a smart TV [38]. As Susan Farrell writes in [9]:

"By making smart devices ubiquitous, we've exposed ourselves to computer-assisted embarrassment. We must expand our usability methods to cover not only the isolated user in one context of use, but also the social user, who interacts with the system in the presence of others."

With the ultimate goal of designing more contextually-relevant notification strategies, we sought to understand the information disclosure risks arising from notifications received when people are in the presence of others. Specifically, we ask the following research questions:

- **RQ1:** How often do email notifications pose an information disclosure risk? I.e., How often are emails received while in the presence of others, and how often do these emails contain sensitive information?
- **RQ2:** To what degree are people's preferences and concerns dependent on user characteristics (personal preferences, job role, etc.) versus being context-dependent with respect to the content disclosed by the notification, and the people in the room?
- **RQ3:** To what degree can a machine-learned system anticipate information disclosure risks? If such predictions are possible, what features are important?

To answer RQ1 and RQ2, we conducted two studies in an enterprise environment grounded in the scenario of a person receiving an email notification on their notification-capable devices while attending a meeting. We focus on emails because they are the primary source of notifications in this environment: 86% of professionals cite email as their primary means of communication, and an average 112.5 billion business emails were exchanged per day in 2015 [14]. Moreover, email often carries notifications for other services (Twitter, Facebook, Slack), suggesting that our findings are likely to provide insights about notifications generated by other communication platforms.

We first conducted an exploratory retrospective online survey (N=131) that asked respondents about hypothetical situations involving recent emails and meetings. From this survey we gained an understanding about the existence and prevalence of the accidental information disclosure problem, and we learned about people's preferences and concerns.

Findings from the retrospective survey guided design decisions for the second study, which provides a deeper, data-centric investigation into information disclosure risks in enterprise settings. This study employed a custom-built labeling tool, to collect labels and preferences for email-meeting pairs. The labeling tool integrated directly with participants' email and calendaring accounts (N=169), allowing the tool to systematically identify emails that were actually received during meetings, focusing labeling on non-hypothetical cases. For each email-meeting pair, the tool automatically extracts features summarizing high-level characteristics of the user, the content of the email message, and the properties of the meeting; and, it does so in a manner that maintains participant anonymity.

Finally, to answer RQ3, we leverage the data collected by the aforementioned contextual labeling tool to explore feature sets and machine learning algorithms to predict information disclosure risks. Here we explore: (a) features that are associated with users (e.g. job title); (b) features that describe a particular email message (e.g. number of recipients in an email); and (c) features that describe a meeting instance (e.g., whether or not a manager is present).

The rest of the paper is structured as follows: We review related work, then discuss the findings of the exploratory retrospective survey. We describe the second study, which involved the deployment of a custom contextual-labeling tool, then describe relevant findings. Finally, we explore machine learning algorithms to predict people's comfort levels, and we present implications for the design of future social-context aware notification systems.

2 RELATED WORK

2.1 Productivity Cost in Notifications

Previous works in notifications mainly focused on the negative impact of interruptions on productivity, and seek to identify low-cost interruptible moments to send notifications. Studies show that the cognitive load of current tasks [6, 20], task transitions [11, 16], physical activities, user interactions on devices [27], and other context such as time and location [29] can be used to identify interruptible moments for notifications. In office settings, for example, Fogarty et al. [13] show that sensor-based statistical models can be used to predict one's interruptibility by leveraging features such as: phone

use, ambient noise (e.g., to detect conversations), mouse and keyboard usage. Likewise, Horvitz et al. [18] use computer activity, calendar information, audio and video signals, and location data to predict users' availability. Notification policies then use inferred levels of availability and interruptibility to determine the ideal time to deliver notifications. Research has also recognized that there can be costs associated with delaying notifications, suggesting that such policies should consider both the cost and benefits of delays [17, 19].

Our work is distinguished in that we study the privacy costs associated with notifications, as opposed to productivity costs. As such, the scenarios we consider are privacy-sensitive, and this has implications for our methodology. We have taken careful steps to respect respondents' privacy in our studies.

2.2 Privacy Cost in Notifications

2.2.1 Privacy Attitudes and Behaviors. A first step in understanding the potential privacy cost of ill-timed notifications is to understand people's general attitudes towards privacy. Pioneering work in this space includes the Westin Privacy Segmentation Index [39], that categorizes people into three groups: privacy fundamentalist, marginally concerned, and pragmatist. *Privacy fundamentalists* are those who are very concerned about their privacy and very reluctant to share any of their information. *Marginally concerned* are generally willing to share details or data about themselves. *Privacy pragmatists* are people who are somewhat concerned about their privacy, but are willing to compromise some privacy for convenience.

Numerous follow-up studies have adopted the Westin Index [1–3, 28], but have reported that people's preferences are nuanced and context sensitive, with complex interactions between the types of disclosures and the audiences who bear witness. For example, Ackerman et al. show that people are generally comfortable sharing their favorite TV shows, favorite snacks, and even email addresses with websites, but are much less comfortable when there is a chance that the website could share the information with others in an identifiable way, or if the information were instead provided by a child under their care [1]. Likewise, Olson et al. show that, even among one's trusted inner circles, one's willingness to disclose information varies greatly depending on the nature of the information being shared [28]. For example, respondents were often uncomfortable disclosing work-related documents with family members, or health information (e.g., pregnancy status) with co-workers.

Adding to this complex motif, past work reports that privacy attitudes are not always correlated with behaviors [2, 26, 33]. For example, participants' behavior in an online shopping scenario was different from their self-reported privacy preferences [33], and one's privacy attitude was a poor predictor of whether participants would share location information [5]. Like privacy attitudes, privacy behaviors are context-specific [5, 12, 40] and multi-dimensional [23].

In this paper we recognize the potential for these complex context-dependent attitudes and behaviors. We designed both of our studies to collect a multitude of signals that characterize how information, audiences, and contexts interact with one another to create situations in which people are uncomfortable (or comfortable) receiving notifications. Additionally, we designed our second study such that it grounds data collection on specific historical instances rather

than asking people about general or hypothetical scenarios and attitudes.

2.2.2 Difference in Disclosures and Privacy Management Strategies. In addition to understanding privacy attitudes in a broader context, it is also important to understand how notifications may differ from the scenarios explored in past work. Here, prior work has mainly examined intentional sharing of information with websites or social networking services (SNSs) [2–4, 36, 37]. Granted that when people disclose their information to these services they don't have perfect knowledge of the consequences, with few exceptions, they have agency in deciding which information to disclose. As such, people often perform an informal risk-benefit analysis before taking actions that may have privacy implications [7, 8, 25, 40]. People also enact preventive strategies, including self-censoring, managing access control groups, and taking actions to conceal their identity [24, 37].

Agency and control is not available in cases where people receive push notifications. Instead, the notification scenario bears resemblance to the scenario in which people are tagged in photos shared to SNSs without consent [24] or posts being unintentionally shared on SNSs as a consequence of *if-this-then-that* (IFTTT) [34]. Here, users can often take corrective actions by either untagging the photos or deleting the contents before more people see the posts. With push notifications, disclosures are instantaneous, and it is unclear what corrective actions can be taken after the event.

A similar situation arises with the accidental disclosure of web browsing history [15]. Through a survey of 155 people, Hawkey et al. found that, as before, comfort level is related to one's level of control (e.g., control over the mouse and keyboard). Moreover, people's comfort is higher when disclosures are to spouses or close friends, and lower with colleagues.

Most closely related to our work is on examining the privacy costs of receiving notifications on a smart TV when watching in a social setting [38]. From a survey of 167 participants, Weber et al. assessed people's comfort levels with different notification variants, and found that the comfort level is higher when the notification reveals less information (e.g. notification indicators). Our work is inspired by these findings, but both extends them to an enterprise setting, and considers a richer set of contexts (e.g. meeting type or location, social structure of people in the room, etc.).

2.2.3 Limitations and Trade-offs in Existing Notification Strategies. Finally, we note that existing mobile devices and applications provide some minimal options for managing notifications. Typically, such options are binary (e.g. turning on and off notifications, enabling notifications for "important" emails in Gmail, and enabling notifications to show previews). Recognizing the privacy risks of notifications, some applications (e.g., WhatsApp) and mobile devices (e.g., iPhone X) have disabled notification previews by default, preferring instead to provide generic indicators (e.g., "You have a new message.") These solutions are context independent, and employ a one-size fits all strategy. Users must accept the trade-offs between minimizing privacy risks (e.g., suppressing notifications) and maintaining timely access to information. In contrast, our work takes into consideration both user contexts and notification contents.

As more and more internet-connected devices and services become capable of displaying information via notifications, there is a

need to better understand people's preferences and concerns about notification-induced information disclosures. There is also a need to develop designs and strategies that can adapt both to a notification's content and the user's context.

3 STUDY #1: EXPLORATORY RETROSPECTIVE SURVEY

As a first step, we describe the results of an exploratory retrospective survey which was designed to gain our initial understanding of the following: (1) How often notifications pose an information disclosure risk? (2) How do features of the notifications, meetings and individuals contribute to the perceived risk? As noted in the introduction, the methods employed here allow a broad investigation covering numerous contexts (e.g., personal vs. work, email topics and themes, etc.)

3.1 Procedure

The survey began by collecting basic demographic information including education, job role, age, gender, notification-capable device use, average number of meetings in a day. It then asked participants to answer questions about a notification scenario, which was evolved slowly over several sections of the questionnaire, as follows:

- (1) Respondents were first asked to consider their most recent meeting. Respondents answered questions about their role in the meeting, their relation to each of the meeting's attendees, and the meeting's time and location, and the types of notification-capable devices that were present (including Desktop PC, Laptop, Smartphone, Smartwatch, and Smart speaker).
- (2) The survey then asked respondents to open their primary work email inbox, consider their 10 most recent emails (excluding the survey invitation), and imagine a scenario in which they received notifications for those emails during the aforementioned meeting. Respondents were asked about the age of the 10th email.¹ Furthermore, we asked participants to imagine that their notification-capable devices' screens were visible to meeting attendees, and answer how many email notifications (out of the ten emails) they would have been uncomfortable sharing with the people in the room. We refer to this scenario as a *hypothetical information disclosure event*, or *HIDE*.
- (3) The questions above were then repeated for the 10 most recent emails in respondents' personal email inboxes.
- (4) Respondents were then asked to select one email (could be from either work or personal email inbox), if applicable, that they would have been most uncomfortable receiving in the scenario outlined above. We refer to this email as the *HIDE email*. Respondents were asked to rate their comfort level in sharing the HIDE email notification with the people in the

¹We decided to only rely on a respondent's 10 most recent emails to (a) convey a simple and consistent sampling criteria in the retrospective survey, and (b) minimize response and counting errors by allowing respondents to observe their emails within a single window pane (the decision made after pilot testing). To partially compensate for this limitation, we additionally asked the age of 10th email, which enables us to calculate the incoming email rate.

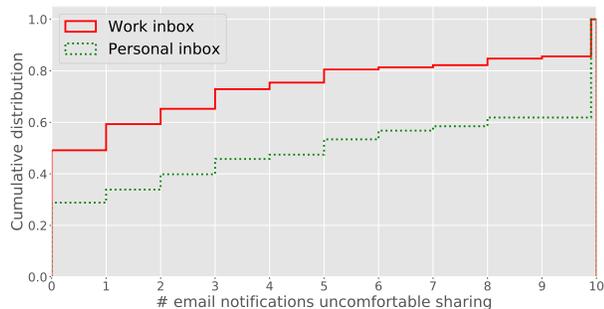


Figure 2: Cumulative distribution of the number of work (red, solid) and personal (green, dotted) emails that people felt uncomfortable sharing with meeting attendees.

room with a 5-point Likert scale (1: Very uncomfortable, 5: Very comfortable). Respondents then were asked to describe general features of the HIDE email, including their relation to its sender, the number of recipients, the type of the inbox (work or personal), the type of content contained therein, and to explain, in broad terms, why receiving notifications for this email would be uncomfortable.

The survey was deployed by emailing a random sample of 800 employees within a large IT corporation. There were 21 email delivery failures, for various technical reasons, resulting in 779 individuals successfully receiving the invitation. We describe our findings next.

3.2 Results

3.2.1 Participants. We received 118 completed, and 13 partially completed responses (response rate = 17%, completion rate = 90%). Of the 131 total respondents, 85 were male (65%), 44 were female (34%), 2 preferred not to answer. Ages were distributed as follows: 18 – 24 years old (5%), 25 – 34 (24%), 35 – 44 (31%), 45 – 54 (27%), 55 – 64 (8%), ≥ 65 (2%), and 2% declined to answer.

Participants reported occupying a diverse set of job roles including: program managers (28%), software developers (19%), marketing and sales people (8%), and IT support staff (8%). The remaining 49 individuals (37%) worked in diverse roles such as administrative assistants, data scientists, designers, attorneys or other roles in the legal department, and human resources.

3.2.2 Prevalence of the information disclosure risk. One key finding from the retrospective survey, and a partial answer to our first research question, is that the majority of respondents (53.4%) reported that *at least one* of their ten most recent work emails would have resulted in an uncomfortable disclosure of information had the email arrived during their most recent meeting. This increases significantly to 73.3% when respondents were asked to consider the ten most recent emails delivered to their personal accounts (two tailed difference of proportions test, $p < 0.001$, $Z = 3.33$). While these findings demonstrate the potential for risk, we cannot be sure how many emails were actually received during the meetings. We address this limitation in the second study.

3.2.3 Three groups of respondents. Figure 2 extends the above analysis by presenting the cumulative distribution for work emails

(red) and for personal emails (green) that participants indicated they would be uncomfortable receiving in their most recent meeting. There are two notable features of these distributions: first, there is a sharp rise at $x = 10$ emails, with 17% of respondents noting they would be uncomfortable receiving *any* work email notification in the presence of others. This increases to 40% for personal emails. We also note that the y -intercepts of the two curves are rather high: 47% of respondents reported that *none* of their ten most recent work emails were sensitive. This decreases to 25% for personal emails. The remaining 36% and 35% of respondents were more selective, and reported that *some* of their work and personal emails were sensitive, respectively.

On the surface, these three groups bear some resemblance to Westin’s three categories, but we are sensitive to the fact that privacy concerns are complex and multidimensional. The responses we collected may be dependant on user characteristics (e.g. personal preferences, the nature of their occupation), contents in the notifications, and the contexts and their relationship with the people in the meeting. For example, one participant explained that she was uncomfortable sharing the information in notifications due to the nature of her occupation:

“I deal with a lot of privileged and confidential information on an hourly, daily basis. I am not able to share the information and it should not be visible to others.”—P122

We could also see that some of the respondents are less concerned about the email notifications divulging information because they personally are less concerned about the contents of notifications being shared with the other people in the room. As P81 reported:

“...But I’m generally not embarrassed by who and what I am. Plus, humor is a good way to diffuse why I get the spam I get.”

Also, worth noting that the floor and ceiling effects we observe may simply reflect limitations in our ability to sample the most/least sensitive contexts, contents, and emails for some users. Our second study will use more sophisticated sampling method to address such limitations.

To sum up, the distribution of responses indicate the three distinct groups of respondents. While some of the open-ended survey responses – like the ones above – highlight the relationship between respondents’ occupation, personality and demographics [32] on notification preferences, some indicate that their preferences depend on the context. To understand this relationship, in the next sections, we extend the analysis by examining the content disclosed by notifications, and the people attending the meeting.

3.2.4 Notification fields and their content. Given prior research [28], we suspect that one’s comfort level depends both on the types of information disclosed by notifications, and on the audience witnessing the disclosure. Addressing the former, participants were asked to select one email that they would have been uncomfortable sharing in their most recent meeting from among their 10 most recent emails. As noted earlier, we refer to this as a hypothetical information disclosure event (HIDE). Participants were asked to answer questions about their HIDE emails, and to describe, in their own words, the types of information that rendered a notification sensitive. We limit the remaining discussion to the 62 respondents

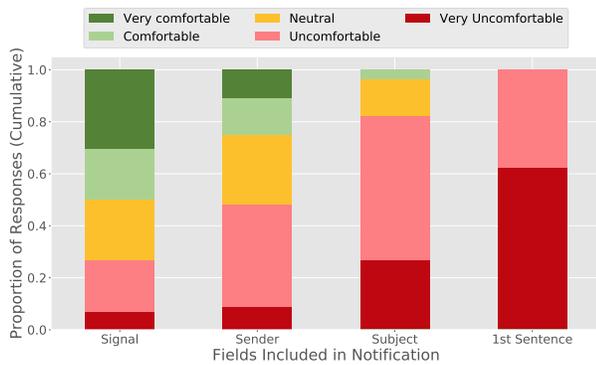


Figure 3: Distribution of respondent comfort levels for sharing different fields included in typical email notifications for HIDE emails.

(47%) who both identified a HIDE email, and who fully completed this portion of the survey questionnaire. We describe the general properties of HIDE emails, then analyze open-ended responses.

In most cases (72.6%), respondents elected to describe HIDE emails that were delivered to their work email inboxes – perhaps reflecting that the survey invitation was sent during business hours. Among these emails, most were sent by work colleagues (75.6%), including: direct superiors (15.6%), team members (28.9%), and other members of the organization (28.9%). Conversely, external senders included: clients or customers (8.9%), family and friends (4.4%), and one instance each from a doctor, and from an insurance company. Conversely, when HIDE emails were delivered to personal inboxes, most were from friends and family (76.5%), but also included messages from: doctors, banking institutions and external recruiters.

In the majority of cases (62.9%) respondents were the only recipient of their HIDE emails – though there were 11 cases (12.9%) where the email was sent to 5 or more people (via the to: or cc: lines). This finding agrees with the intuition that emails sent only to one person are, perhaps, more likely to contain private information. We explore this hypothesis further in the second part of this paper.

As noted above, we asked participants to describe, in broad terms, what types of information rendered these emails sensitive. Open-ended responses were analyzed, and themes identified, following open coding practices [22]. Among the top themes were: unspecified personal life details (14 instances), unspecified confidential work documents (11 instances), details of ongoing projects (10 instances), health information (7 instances), personal successes or failures (7 instances), financial communications (4 instances), and messages that mention people attending the meeting (3 instances). These themes largely overlap those identified by Olson et al. in [28].

As email notifications can reveal numerous email fields (Figure 1) including: sender, subject, and the first sentence of the email body, we asked participants to rate how comfortable would they have been if the people in the room saw the different email fields. Each field-type reveals a different class of information, and, to varying degrees, poses an information disclosure risk. For example, the sender field reveals that a respondent is in correspondence with a particular individual, while the subject reveals the topic of discussion. Correspondingly, among HIDE emails 25% of survey respondents were comfortable with email notifications that revealed the sender’s

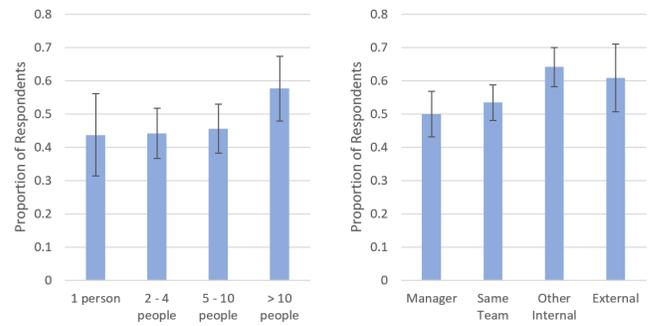


Figure 4: Proportion of respondents reporting HIDE emails, partitioned by the number of people attending the meeting (left) and the attendees’ relationships to the respondent (right). Error bars show standard error; none of the pairwise differences are statistically significant at the $\alpha = 0.05$ level.

identity, while only 3.6% were comfortable with notifications that reveal the email subject. This difference is highly statistically significant ($p = 0.001$, $Z = 3.20$). Figure 3 provides further details, breaking down respondent comfort levels by field-type.

3.2.5 Audience features. We explored whether meeting properties (e.g., location, attendance, etc.) impacted the proportion of respondents who identified a HIDE email among their 10 most recent messages. Though this analysis revealed no statistically significant results, we present our findings to: (1) characterize the meetings our respondents attend, (2) offer points of comparison with the results from our second study, and (3) identify weak trends that may yet become features in machine-learned models.

The majority of respondents reported that their most recent meeting occurred in a conference room (52.7%), though people also reported hosting meetings in their own offices (22.9%), attending meetings in someone else’s office (15.3%), and attending meetings in other common spaces such as a lounge or atrium (8.4%). Among respondents whose meetings occurred in conference rooms, 50.7% were able to identify an email they would have been uncomfortable receiving in that context. Likewise, among respondents meeting in offices, 46.6% were able to identify such an email. These differences are not statistically significant ($p = 0.61$, $Z = 0.509$).

When asked how many people attended the respondent’s most recent meeting, the mode response was “5 – 10 other people” (35.1%). Other response categories included: “2-4 other people” (32.8%), “10 or more people” (14.5%), and “1:1 meetings” (12.2%). Again, we examine the proportion of respondents who were able to identify an email they would have been uncomfortable receiving in each of these contexts. This proportion monotonically increases with the size of the meeting (Figure 4, left), but the pairwise differences are not significant.

Finally, we report that meetings were attended by team members (65.6%), direct superiors (41.2%), other members of the respondent’s organization (51.1%), as well as people external to the organization (17.6%). In each case, we examine the proportion of respondents who were able to identify an email they would have been uncomfortable receiving in the meeting. Figure 4 (right) shows that the proportion increases as the meeting’s attendee list grows beyond one’s own

Project: Randomly Chosen Meeting

Hello, [Name] Show my answers Tutorial About Log Out

We do **NOT** store any personally identifiable information about your emails and meetings. Here is an example of survey data being stored.

Survey completed: 0%

Meeting

Subject: 1:1 Weekly Meetings

From 8/16/2017 11am till 8/16/2017 12pm at [Name]'s Office (Organized by [Name])

Attendees: [Name], [Name]

Email

From: [Name]

To: [Name]

Subject: your talk topic for Aug 31st

Body: Hi,

You are scheduled to give a talk on August 31st.

Could you please send me a title and a couple sentences about your talk topic before 8/24?

We have 3 speakers slotted for this lunch, so talks should be about 15min.

Thanks!

Survey questions

Question 1: Did you attend the meeting above?

Yes

Question 2: While attending the meeting, were there other people in the same room as you?

Yes

Question 3: How comfortable would you have been if the people in the room noticed new email indicator (e.g. banner icons, "You have a new email")?

Very uncomfortable Neutral Very comfortable

Question 4: How comfortable would you have been if the people in the room saw the sender of the email?

Very uncomfortable Neutral Very comfortable

Question 5: How comfortable would you have been if the people in the room saw the subject of the email?

Very uncomfortable Neutral Very comfortable

Question 6: How comfortable would you have been if the people in the room saw the first sentence of the email?

Very uncomfortable Neutral Very comfortable

Figure 5: Interface for survey questions about email-meeting pairs. (a) Meeting pane that shows a randomly chosen meeting, time and location of the meeting, attendees, and subject of the meeting; (b) Email pane that shows a randomly chosen email that was received during the meeting, the sender, recipients, subject, and body of the email; (c) survey questions about their comfort level in sharing different fields of the email, type of the email, preferences for different devices and disclosure level.

team. Though this agrees with intuition, the differences are not statistically significant. We revisit this observation later (§4).

In summary, results from the exploratory retrospective survey provide a key set of initial insights about the prevalence of the information disclosure risks posed by notifications, and about how email topics and fields may contribute to this risk. Moreover, we found that respondents could be clustered into three distinct groups based on the proportion of emails they received that would result in uncomfortable notifications.

While the survey was designed to ground responses in respondents' actual emails and meetings, it is limited in two important ways. First, to convey a simple and consistent sampling criteria and to minimize response or counting errors, the survey asked respondents to comment only on a single meeting, and on their single most-sensitive email. Second, it asked respondents to consider *hypothetical* situations in which they receive the most-sensitive email during the most recent meeting. Together, these survey design choices limit our ability to measure actual incidence rates, and to model the overall distribution of risk. To address these limitations, we developed and deployed a custom-built contextual labeling tool, which we describe in the next section.

4 STUDY #2: CONTEXTUAL LABELING STUDY

Based on the insights we gained from the exploratory retrospective study, we developed and deployed a tool (Figure 5) to extract various features and collect labelled data for learning a context-dependent predictive model of disclosure risk. The tool allows participants to view emails that they received during meetings, view the details

of those meetings, and rate their comfort-levels in receiving the corresponding email notification in that context. We described the procedure, apparatus, and results below.

4.1 Procedure and Apparatus

The contextual-labeling study was deployed within the same large IT company as the initial retrospective survey. Participants shared a common computing environment. In particular, they stored their emails and calendars in a common email and calendar web service. This homogeneous environment greatly simplified the administration of the study, and the implementation of the tool.

4.1.1 Procedure. Participants were recruited by emailing a random sample of 4000 employees, distinct from the 800 who were contacted for the retrospective survey. The invitation email described the study's purpose and procedure, and provided sufficient information to validate the authenticity of the invitation (e.g., links to internal systems and pages documenting the experiment, and the results of both an internal review process, and IRB review). Crucially, the invitation also included a link to the web application that hosted the labeling tool.

Upon navigating to the web application, participants were first shown the purpose of the study (i.e. characterizing people's preferences about information disclosed by desktop and mobile notifications that arrive when the intended recipient is in the presence of others). Then, participants were asked to authenticate to the tool using their corporate credentials, and to grant the tool time-limited access to their corporate email and calendaring accounts. Once participants were authenticated, they were presented with a brief tutorial of the labeling tool, and its three regions:

- The top region (Figure 5a) displayed a recent meeting, randomly selected from a day. Visible fields included: meeting subject, time, location, organizer, and a list of attendees.
- The left region (Figure 5b) displayed a randomly selected email that arrived during the meeting. Visible fields included: the sender, recipient list (the ‘to:’ and ‘cc:’ lines), subject, and email body.
- The right region (Figure 5c) contained a short survey, where participants could answer questions about the email-meeting pair. Questions asked about participants’ comfort levels in having notifications disclose various fields of the email to the people attending the meeting with a 7-point Likert Scale (1: Very uncomfortable, 7: Very comfortable).²

To collect data across a wide range of email-meeting pairs, the tool samples one email-meeting pair per day, moving backward in history one day at a time until 10 pairs are labeled. In each day, a meeting was randomly selected and then an email that was received during the meeting was randomly selected as well. If participants indicated that they did not attend a scheduled meeting, or that the meeting was conducted via teleconference, the tool selected another email-meeting pair for labeling.

Upon inputting labels for 10 email-meeting pairs, participants were presented with a debriefing page, and an optional invitation to take part in a raffle for one of three \$50 Amazon.com gift cards. This sweepstakes was conducted in appreciation for their participation.

In addition to collecting user-provided labels and preferences, the labeling tool collected high-level features of the emails and meetings (Table 1). Importantly, the study was conducted completely anonymously: users were assigned random session ID, the participation sweepstakes was conducted on a separate unconnected system, and the features were chosen to be non-personally identifiable. We provide more details about these features in the next section.

4.2 Feature Extraction

Table 1 presents a list of features automatically collected by the labeling tool. Features are broadly categorized into three groups. User features are those that are associated with the participant, but not with a particular email-meeting pair. For example, this class includes the average number of emails a person received during meetings in the past 7 days, their depth in the organization chart, and their job title. To preserve anonymity, we used k-anonymization ($k = 50$) at the organizational level for full job titles, and separately, for job-title bigrams. Email features are those that describe a particular email message. Examples of these features include the number of recipients, Linguistic Inquiry and Word Count (LIWC, [35]) feature vectors, mentions of people, locations, and organizations, and whether the email is machine-generated. For LIWC categories, we tokenized the body, categorized each token into the pre-defined psychological and linguistic categories in LIWC, then computed the percentage of tokens in each category relative to the email body as a whole. We used the Stanford named entity recognizer [10] to detect mentions of people, places and organizations. To check whether or not an email is autogenerated, we used a simple

²Since our exploratory survey results exhibited ceiling and floor effects, we extended the scale to 7 points to allow for more nuanced responses.

	Feature	Description
User	jobTitle	k-anonymized job title
	orgDepth	depth in the organizational chart
	numEmails	number of emails received in the past week
	numMeetings	number of meetings scheduled in the past week
	avgEmlPerMtg	average number of emails received in meetings
Email	numMtgWithEml	number of meetings interrupted by emails
	numRecipients	number of recipients in the email
	numDistList	number of distribution lists as the recipient
	numThreads	number of threads in the email
	isAutogenerated	is autogenerated email
	numPplMentioned	number of attendees mentioned in the email
	numAttachment	number of attachments
	attachment[type]	type of attachment in the email
	isSenderInternal	is the sender internal to the organization
	numSubjectWords	number of words in the email subject
numBodyWords	number of words in the email body	
entity[type]	mentions of people, locations and organizations	
LIWC[cat]	feature vector over email body	
Meeting	location	meeting location
	numAttendees	number of people attending the meeting
	isManagerPresent	is the person’s manager present
	numDirectReports	number of direct reports present
	numOrgAbove	number of attendees above in the org chart
	numOrgBelow	number of attendees below in the org chart
	numExternal	number of attendees external to organization
	numSubjectWords	number of words in the meeting subject
	numBodyWords	number of words in the meeting body
LIWC[cat]	feature vector over meeting body	

Table 1: A list of user, email and meeting features that the labeling tool automatically computed for each email-meeting pair labeled by participants.

heuristic to check whether or not an email contains ‘Unsubscribe.’ Meeting features describe the meeting instance, and include details such as the number of attendees, and whether a person’s manager is in attendance. Organizational relationships were computed by cross referencing the attendee information from the calendar and the company’s organizational chart as follows: for each attendee, we checked whether or not the attendee was the person’s manager, direct report, above or below the org chart. Finally, we include one hybrid feature which counts the number of meeting attendees mentioned in the email.

4.3 Results

We sought to replicate the analyses we conducted in the exploratory retrospective survey, when possible. As we will show, the consistency of their results helps bolster our confidence in their validity and reliability. Now, we discuss our main findings of this study.

4.3.1 Participants. In total, we received 1,040 meeting-email pairs labeled by 169 participants. Similar to the retrospective survey, job roles were diverse. The largest two categories included software developers (21.3%) and program managers (13.6%). An additional 52 individuals (30.8%) occupied various roles including: marketing managers, attorneys, sales specialists, business planners, etc. Finally, the job roles of 58 participants (34.3%) were filtered by k-anonymization.

In addition to collecting job demographics, the labeling tool collected general measurements of the participants’ calendars and email inboxes. For performance reasons, these coarse measurements are constrained to examining users’ 300 most recent emails, together with the last 7 days of their calendar. 75.15% of participants’ inboxes contained fewer than 300 emails received during this 7-day window (average: 103.7), allowing a full measurement of email-meeting co-occurrences during the week. These participants’ 7-day calendars

	10 Uncomfort	Mixed	10 Comfort
Labeling Study	23%	36%	41%
Study1 (work)	17%	36%	47%
Study1 (personal)	40%	35%	25%

Table 2: Distribution of three groups of respondents in both the retrospective and contextual-labeling study. “10 Uncomfort” indicates respondents who labelled all 10 emails as uncomfortable, “10 Comfort” indicates all 10 emails as comfortable, and “Mixed” indicates a mixture of both comfortable and uncomfortable emails.

contained an average of 13.84 meetings (SD: 9.04). On average participants received emails during 7.35 (53%) of these meetings (SD: 6.10). In other words, slightly more than half of all meetings were interrupted by email.

A similar analysis can be performed for the remaining 24.85% who received more than 300 emails. Here, the results cover a variable time frame that is necessarily shorter than a week. For these participants, their most recent 300 inbox emails co-occurred with an average of 8.74 meetings (SD: 6.14). These participants’ 7-days calendars contained an average of 18.83 meetings (SD: 11.66), suggesting that *at least* 46% of their meetings are interrupted by email.

The remaining analysis considers specific email-meeting pairs that are sampled from participant’s calendars and inboxes. Unlike the above-mentioned aggregate measures, the sampling procedure is not constrained by the 7-day, 300-email, limit.

4.3.2 Prevalence of the information disclosure risk. As detailed in the procedure section, participants were asked to answer questions about 10 email-meeting pairs. To generate these pairs, we randomly sampled a meeting, then randomly sampled an email received during the meeting. Mirroring the analysis of the retrospective survey, 90 out of 169 people (53.3%) had at least one email whose notification they rated as uncomfortable sharing (i.e., they selected a comfort rating of ≤ 4 on the 7-point Likert scale for sharing the sender, subject and first sentence of the email). This proportion is nearly identical to that which was found in the retrospective survey for emails delivered to work inboxes (53.4%, Figure 2).

4.3.3 Three groups of respondents. Earlier, when we analyzed the results of the retrospective survey, we observed that respondents fell into three groups based on their responses to a hypothetical scenario in which they received notifications of their 10 most-recent emails while attending their most recent meeting. In this labeling study, participants were asked to label 10 emails known to have actually arrived during 10 distinct meetings. This allows a more ecologically valid analysis of this phenomenon. For comparison purposes we transform the 7-point Likert scale to a binary scale. Here scores > 4 (neutral) affirm that the user is comfortable with the notification. Results are presented in Table 2, together with the distribution reported in our retrospective survey. The results show that 23% of the respondents were uncomfortable sharing any of 10 emails in the respective meetings (“10 Uncomfort”), while 41% of the respondents were comfortable sharing all of the

10 emails (“10 Comfort”), and 36% of them were uncomfortable sharing some emails (“Mixed”). Notably, the distribution of users is roughly consistent across both the retrospective survey and the labeling tool (for work inboxes). This suggests that, although the retrospective survey involved a hypothetical situation, its findings closely match those of real-world scenarios. The distribution of the groups also resembles the classical trichotomy of the Westin Index; but, again, we are sensitive to the fact that these preferences can be highly nuanced and context-sensitive. To that end, we explore contextual factors below, as well as later in the section 5.

4.3.4 Email and meeting properties. When reporting the results of the retrospective survey, we examined various properties of emails and meetings that might indicate, or themselves constitute, an information disclosure risk. We now reexamine those criteria.

Number of email recipients: In the retrospective survey, we found that the number of people in an email’s recipient list may influence users’ comfort levels. Specifically, we observed that the majority of HIDE emails (62.9%) had only a single recipient. We can report a similar statistic for data collected via the labeling tool but must first filter the data such that they are directly comparable: In the retrospective survey, users were asked to discuss the most sensitive email from among those they would be uncomfortable sharing in a meeting. When we apply the same criteria to label-tool data, we find that 46.8% of emails have only a single recipient.

The labeled data also allows for a more deliberate examination of this phenomenon. This is because it contains examples of both sensitive and non-sensitive email-meeting pairs. Over all 1040 pairs, 406 (39%) emails were delivered to a single recipient (i.e., contains no other recipients in either the ‘to:’ or ‘cc:’ fields). For 131 (32.3%) of these emails, participants indicated that they would be uncomfortable with meeting attendees seeing the resultant email notifications. This number falls to 23.2% for emails delivered to multiple individuals. This difference is statistically significant ($Z = 3.228, p = 0.001$), suggesting that, when multiple people are in an email thread, the likelihood of the email containing sensitive information may be lower.

Number of external meeting attendees: Results from the earlier retrospective survey also suggested that meeting attendance might influence how comfortable people are with sharing their email notifications.³ Specially, the presence of people outside of one’s team or organization *might* increase levels of discomfort. Again, the labeled-data allows for a more ecologically valid and sensitive analysis: Of the 1040 email-meeting pairs, 298 (27.8%) were attended by people from outside of the organization.⁴ Participants reported that in 95 cases (32.3%), they would be uncomfortable sharing the email notification with meeting attendees. This proportion falls to 24.4% for meetings in which all attendees are fellow employees of the same organization. This difference is statistically significant ($Z = 2.78, p = 0.005$), suggesting that meeting attendance may indeed influence comfort levels about email notifications.

Together, these findings reinforce and extend our answers to the first two research questions: people are often interrupted by

³Results from the retrospective survey were not statistically significant, but suggested a possible trend worth further investigation (Figure 4).

⁴External to the organization via the *numExternal* feature. Note, the organization chart used in the labeling tool was not sufficiently fine-grained to determine if a fellow employee was a member of a different team.

Classifier	AUC	Pr	Re	F1
Boosted tree ensemble	0.85	0.71	0.63	0.67
kNN	0.59	0.39	0.23	0.29
SVM	0.58	0.78	0.03	0.06

Table 3: Results of the classifiers that predict if a respondent would be uncomfortable revealing a given email notification in a particular meeting context (i.e., an email-meeting pair).

Top 10	Top 11-20
U.avgEmlPerMtg (1)	M.numExternal (0.57)
U.numEmails (0.86)	E.numThreads (0.54)
U.numMtgWithEml (0.78)	E.LIWC[posemo] (0.53)
M.orgChartAbove (0.73)	E.numSubjectWords (0.49)
E.LIWC[money] (0.7)	U.orgDepth (0.47)
M.LIWC[negemo] (0.62)	M.LIWC[bio] (0.47)
M.numSubjectWords (0.6)	U.SENIORPROGMNG (0.45)
E.numBodyWords (0.58)	E.numCC (0.44)
M.LIWC[posemo] (0.58)	E.entity[org] (0.43)
U.numMeetings (0.58)	E.numDistList (0.41)

Table 4: Top 20 most informative features for the boosted tree ensemble classifier. The number in the parentheses indicates the information gain, normalized such that the most informative feature scores a 1.0. The prefixes ‘U’, ‘E’, and ‘M’, denote user, email, and meeting features, respectively.

emails when in meetings, in a sizable minority of cases people are uncomfortable sharing the resultant email notifications with the people in the room (RQ1). These levels of discomfort may depend on individual characteristics, as well as on features of the meetings and emails (RQ2). This, in turn, hints at the possibility of using machine learning to predict when email notifications pose an information disclosure risk. We examine this in the next section, and, in doing so, answer our final research question (RQ3).

5 PREDICTING COMFORT LEVEL

To further explore the problem space, we developed binary classifiers that, given an email-meeting pair, decide if the delivery of an email notification would result in an uncomfortable situation. In constructing these classifiers, we both: (1) gain a deeper understanding of how combinations of user, email and meeting features may contribute to one’s concerns about email notifications, and (2) explore modeling decisions and requirements that can lead to context-dependent predictions accurate enough to be used to manage users’ notifications in real-world settings.

5.1 Prediction Results

For training and evaluation we use the 1040 labeled examples collected in the second study, above. Training and evaluation is done using 10-fold cross-validation, stratified the data such that, for each user, 7 labeled data points are included in the training set, and 3 labeled data points are included in the test split, and optimized to maximize the area under the receiver operating characteristic curve (AUC). We train boosted tree ensemble, SVM with linear kernel, and k-nearest neighbor (k=3) classifiers.

Detailed results are presented in Table 3. There are a few points to note. Our best performing classifier, the boosted tree ensemble, achieved an AUC of 0.85 which is well above chance. However, with our best performing model achieving a precision of 0.71, and a recall of 0.62, the classifiers are likely to be less useful in high-risk applications. Nevertheless, our explorations reveal that generic features provide some information about the information disclosure risks of an email-meeting pair.

For example, we looked at the 20 most informative features with our best performing classifier, the boosted tree ensemble (Table 4). In addition to the user features that might be indicative of potential exposure (the number of emails a user receives in a week, the average emails per meeting, the number of meetings), and email features that are related to email contents and length, we found features related to meeting context. Notably, the fourth most informative feature was one that counted how many meeting attendees were above the recipient in the organizational chart. Again, we also found that people were more uncomfortable sharing emails when the meeting description contains strong negative or positive emotion words categorized by LIWC [35].

To this end, we have answered our research questions. In the next section, we offer design implications, then conclude with a brief discussion of limitations and future work.

6 DESIGN IMPLICATIONS

In this section, we discuss some of the implications for designing contextually-relevant notification systems and policies.

Personalization matters. Both our exploratory retrospective survey and the contextual labeling study revealed three general and distinct groups of respondents. If a user can be quickly characterized as *Always Comfortable* or as *Always Uncomfortable*, then the notifications policies are rather straightforward: unconditionally allow all notifications for the unconcerned, and turn off notifications for those *Always Uncomfortable* unless the system is certain the user is alone. However, there exists a much richer strategy space for the *Mixed Comfortable* group, where various notification actions can be designed by hiding certain fields of messages, or delivering notifications only to certain devices.

Even simple context is helpful. As discussed above, for some people an effective notification policy might need only know if a person is alone, and examining a user’s calendar may serve as an acceptable approximation. More sophisticated policies might consider whether an email was delivered to multiple people, or whether a meeting will be attended by people from outside the organization. These possibilities make clear that interesting notification policies can be developed from simple, easy-to-compute, signals.

Better sensing is likely to help. Both the retrospective survey and the contextual-labeling study included questions that could not be automatically answered based on calendar appointments and emails alone. For example, we asked participants if they attended meetings, and whether meetings were conducted via teleconference. With richer sensing capabilities, it is possible that these features could be reasoned about automatically.

Choose your notification fields wisely. Finally, our studies revealed that some notification fields are less sensitive than others. However, these preferences weren’t universal, and varied even

within a single user’s responses. For example, an email’s sender field may pose little risk in some cases (e.g., an email from a known collaborator), but pose significant risk in others (e.g., an email from a medical specialist). Systems should leverage these preferences, but also be expressive enough to allow exceptions. Systems should also scale their services, opting for more conservative notification strategies when there is uncertainty in predicting comfort level.

7 ETHICAL SAFEGUARDS FOR OUR STUDIES

In our studies, we sought to ensure participant anonymity and to avoid collecting any personally identifiable information. To make participation anonymous, we assigned participants random session identifiers in the labeling tool study, and hosted participation sweepstakes on a separate unconnected system. To preserve anonymity in feature extraction, for example, we used k -anonymization ($k = 50$) for full job titles and job-title bigrams. To avoid collecting personally identifiable information, we asked participants to describe their emails in broad terms in open-ended questions and cautioned participants not to include any personally identifiable information. Further in the labeling tool study, we chose email and meeting features that were not personally identifiable. For example, instead of collecting exact words that an email contained, we only collected LIWC feature vectors of the email. Finally, due to the sensitive nature of the topic we investigate, we also allowed participants to see the data being collected, and allowed them to delete their responses should they change their mind during or after the study.

8 DISCUSSION AND LIMITATIONS

In this paper, we characterized information disclosure risks that arise when people receive notifications in the presence of others. Specifically, we focused on emails that arrive during meetings. We employed multiple lines of evidence, including a large retrospective survey, and data collected in a second study via a purpose-built labeling tool. We report similar findings in both datasets, and are encouraged by this consistency.

Nevertheless, we caution readers against overgeneralizing our findings. Both the survey and labeling tool were deployed within a single large U.S.-based information technology company. Though respondents occupied a wide variety of job roles, it remains to be demonstrated that our findings generalize to other companies, company cultures, and industries. For example, it seems likely that people working in financial, legal, and medical industries may be more sensitive to information disclosure risks. It is also possible that preferences and concerns may vary by country and culture. Thankfully the *features* we described in this paper are very general, and are likely to be available in other companies and industry settings. As such, we expect replication efforts to be rather straightforward.

We would also like to extend our analysis to personal emails and contexts (e.g., social gatherings, etc). The retrospective survey revealed that people perceive a higher risk when personal emails arrive during work meetings. One wonders: Is the same true for social gatherings? How might work notifications be perceived in non-work contexts? We believe this line of investigation will be fruitful future research.

Likewise, our studies focused exclusively on email notifications. This choice was deliberate and practical; as noted in the introduction, email is often a carrier for other types of notifications (e.g., social networks). In the future, we hope to explore the privacy risks of other notification types, including: instant messages, calendar appointments, reminders, and other information proactively displayed by virtual assistants. Studying these notifications requires deeper technical integration with devices and platforms. Our studies were also exclusively performed from the perspective of the notification recipient. We recognize that the senders of emails are also subject to disclosure risks. When such risks are present, message originators can take some limited preventive actions to mitigate risks (e.g., by using the email subject to indicate that an email is sensitive, or by adding blank lines to the beginning of a message).

One goal of this paper is to assess the basic feasibility of machine learned classifiers, and in doing so, to identify features that help predict notification comfort levels. Our top classifier achieved an AUC of 0.85, and its strongest features capture aspects of notifications that were deemed important in our survey. Moving forward, we hope to improve accuracy, and this likely requires the collection of more data—our sample of 1040 labeled email-meeting pairs is rather small for state-of-the-art classifiers, and this data scarcity is confounded by the fact that the labels are likely correlated; the 1040 labeled pairs represent only 169 individuals. With more data, we hope to improve prediction accuracy enough to implement real-time notification policies for virtual assistants.

Finally, we recognize that there are costs to delaying notifications and hiding notification fields [17, 19]. Our studies did not measure these costs, and cannot directly experiment with formal notification policies. Nevertheless, we feel our analysis has showcased the need and opportunity to develop such policies, and has provided hints about which features and properties are likely to be informative.

9 CONCLUSION

In this paper, we report results from a retrospective survey and a larger contextual labeling study. Our research necessitated that we ask users to discuss sensitive scenarios. Specifically, we asked user to describe sensitive emails, and to discuss why they would feel uncomfortable receiving notifications for those messages when in the presence of others. To this end, we designed our studies to carefully respect participant privacy, and we believe these considerations were instrumental in allowing us to recruit a combined total of 300 individuals. From these individuals, we learned:

- (RQ1) Email notifications indeed pose an information disclosure risk.
- (RQ2) The real or perceived severity of these risks depend both on user characteristics (e.g. the nature of occupation) and attributes of the meeting or email (e.g., the number of recipients or attendees).
- (RQ3) Machine-learned models can learn attributes, patterns and signals associated with risky email-meeting pairs. Here, user-level features are more informative than generic meeting or email-level features.

Taken together, our findings present a rich picture of notifications, as viewed through the lens of privacy. We hope that our findings will inform the design of future notification systems.

REFERENCES

- [1] 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 (EC '99)*. ACM, New York, NY, USA, 1–8. <https://doi.org/10.1145/336992.336995>
- [2] Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*. Springer, 36–58.
- [3] Bettina Berendt, Oliver Günther, and Sarah Spiekermann. 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Commun. ACM* 48, 4 (2005), 101–106.
- [4] Camille Cobb and Tadayoshi Kohno. 2017. How Public Is My Private Life?: Privacy in Online Dating. In *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 1231–1240. <https://doi.org/10.1145/3038912.3052592>
- [5] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, when, & What People Want to Share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05)*. ACM, New York, NY, USA, 81–90. <https://doi.org/10.1145/1054972.1054985>
- [6] Edward Cutrell, Mary Czerwinski, and Eric Horvitz. 2001. Notification, Disruption, and Memory: Effects of Messaging Interruptions on Memory and Performance. IOS Press, 263–269.
- [7] Paul Dourish and Ken Anderson. 2006. Collective information practice: exploring privacy and security as social and cultural phenomena. *Human-computer interaction* 21, 3 (2006), 319–342.
- [8] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors Toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 5228–5239. <https://doi.org/10.1145/2858036.2858214>
- [9] Susan Farrell. 2016. Computer-Assisted Embarrassment. <https://www.nngroup.com/articles/embarrassment>.
- [10] Jenny Rose Finkel, Trond Grenager, and Christopher Manning. 2005. Incorporating Non-local Information into Information Extraction Systems by Gibbs Sampling. In *Proceedings of the 43rd Annual Meeting on Association for Computational Linguistics (ACL '05)*. Association for Computational Linguistics, Stroudsburg, PA, USA, 363–370. <https://doi.org/10.3115/1219840.1219885>
- [11] 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 (MobileHCI '11)*. ACM, New York, NY, USA, 181–190. <https://doi.org/10.1145/2037373.2037402>
- [12] Martin Fishbein and Icek Ajzen. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*.
- [13] James Fogarty, Scott E. Hudson, Christopher G. Atkeson, Daniel Avrahami, Jodi Forlizzi, Sara Kiesler, Johnny C. Lee, and Jie Yang. 2005. Predicting Human Interruption with Sensors. *ACM Trans. Comput.-Hum. Interact.* 12, 1 (March 2005), 119–146. <https://doi.org/10.1145/1057237.1057243>
- [14] The Radicati Group. 2015. Email Statistics Report, 2015–2019.
- [15] Kirstie Hawkey and Kori M. Inkpen. 2006. Keeping Up Appearances: Understanding the Dimensions of Incidental Information Privacy. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, New York, NY, USA, 821–830. <https://doi.org/10.1145/1124772.1124893>
- [16] Joyce Ho and Stephen S Intille. 2005. Using context-aware computing to reduce the perceived burden of interruptions from mobile devices. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 909–918.
- [17] Eric Horvitz, Carl Kadie, Tim Paek, and David Hovel. 2003. Models of Attention in Computing and Communication: From Principles to Applications. *Commun. ACM* 46, 3 (March 2003), 52–59. <https://doi.org/10.1145/636772.636798>
- [18] Eric Horvitz, Paul Koch, Carl M. Kadie, and Andy Jacobs. 2002. Coordinate: Probabilistic Forecasting of Presence and Availability. In *Proceedings of the Eighteenth Conference on Uncertainty in Artificial Intelligence (UAI'02)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 224–233. <http://dl.acm.org/citation.cfm?id=2073876.2073903>
- [19] Eric Horvitz, Paul Koch, Raman Sarin, Johnson Apacible, and Muru Subramani. 2005. Bayesphone: Precomputation of Context-Sensitive Policies for Inquiry and Action in Mobile Devices. In *User Modeling 2005*. Springer, Berlin, Heidelberg, 251–260. http://link.springer.com/chapter/10.1007/11527886_33 DOI: 10.1007/11527886_33.
- [20] Shamsi T. Iqbal, Piotr D. Adamczyk, Xianjun Sam Zheng, and Brian P. Bailey. 2005. Towards an Index of Opportunity: Understanding Changes in Mental Workload During Task Execution. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '05)*. ACM, New York, NY, USA, 311–320. <https://doi.org/10.1145/1054972.1055016>
- [21] Shamsi T Iqbal and Eric Horvitz. 2010. Notifications and awareness: a field study of alert usage and preferences. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work*. ACM, 27–30.
- [22] Harry Hochheiser Jonathan Lazar, Jijuan Heidi Feng. 2010. *Research Methods In Human-Computer Interaction* (1 ed.). Wiley & Sons.
- [23] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71, 12 (Dec. 2013), 1144–1162. <https://doi.org/10.1016/j.ijhcs.2013.06.003>
- [24] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 3217–3226. <https://doi.org/10.1145/1978942.1979420>
- [25] Yuan Li. 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems* 54, 1 (2012), 471–481.
- [26] 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 (June 2007), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- [27] Tadashi Okoshi, Julian Ramos, Hiroki Nozaki, Jin Nakazawa, Anind K. Dey, and Hideyuki Tokuda. 2015. Reducing Users' Perceived Mental Effort Due to Interruptive Notifications in Multi-device Mobile Environments. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 475–486. <https://doi.org/10.1145/2750858.2807517>
- [28] 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 (CHI EA '05)*. ACM, New York, NY, USA, 1985–1988. <https://doi.org/10.1145/1056808.1057073>
- [29] 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 (UbiComp '14)*. ACM, New York, NY, USA, 897–908. <https://doi.org/10.1145/2632048.2632062>
- [30] 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 (MobileHCI '14)*. ACM, New York, NY, USA, 233–242.
- [31] Alireza Sahami Shirazi, Niels Henze, Tilman Dingler, Martin Pielot, Dominik Weber, and Albrecht Schmidt. 2014. Large-scale Assessment of Mobile Notifications. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 3055–3064.
- [32] Kim Bartel Sheehan. 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society* 18, 1 (2002), 21–32.
- [33] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*. ACM, 38–47.
- [34] Milijana Surbatovich, Jassim Aljuraaidan, Lujo Bauer, Anupam Das, and Limin Jia. 2017. Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes. In *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 1501–1510. <https://doi.org/10.1145/3038912.3052709>
- [35] Yla R. Tausczik and James W. Pennebaker. 2010. The Psychological Meaning of Words: LIWC and Computerized Text Analysis Methods. *Journal of Language and Social Psychology* 29, 1 (2010), 24–54. <https://doi.org/10.1177/0261927X09351676> arXiv:<https://doi.org/10.1177/0261927X09351676>
- [36] Sadeh Torabi and Konstantin Beznosov. 2016. Sharing Health Information on Facebook: Practices, Preferences, and Risk Perceptions of North American Users. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*.
- [37] Jessica Vitak and Jinyoung Kim. 2014. "You Can'T Block People Offline": Examining How Facebook's Affordances Shape the Disclosure Process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '14)*. ACM, New York, NY, USA, 461–474. <https://doi.org/10.1145/2531602.2531672>
- [38] Dominik Weber, Sven Mayer, Alexandra Voit, Rodrigo Ventura Fierro, and Niels Henze. 2016. Design Guidelines for Notifications on Smart TVs. In *Proceedings of the ACM International Conference on Interactive Experiences for TV and Online Video (TVX '16)*. ACM, New York, NY, USA, 13–24. <https://doi.org/10.1145/2932206.2932212>
- [39] Alan F Westin. 1991. Harris-Equifax consumer privacy survey 1991. *Atlanta, GA: Equifax Inc* (1991).
- [40] Allison Woodruff, Vasyli Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a privacy fundamentalist sell their DNA for \$1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *Symposium on Usable Privacy and Security (SOUPS)*, Vol. 5. 1.