Addressing The Privacy Paradox through Personalized Privacy Notifications

COREY BRIAN JACKSON, School of Information Studies, Syracuse University, USA
YANG WANG, School of Information Studies, Syracuse University, USA

Privacy behaviors of individuals are often inconsistent with their stated attitudes, a phenomenon known as the "privacy paradox." These inconsistencies may lead to troublesome or regrettable experiences. To help people address these privacy inconsistencies, we propose a personalized privacy notification approach that juxtaposes users' general privacy attitudes towards specific technologies and the potential privacy riskiness of particular instances of such technology, right when users make decisions about whether and/or how to use the technology under consideration. Highlighting the privacy inconsistencies to users was designed to nudge them in making decisions in a way that aligns with their privacy attitudes.

To illustrate this approach, we chose the domain of mobile apps and designed a *privacy discrepancy* interface that highlights this discrepancy between users' general privacy attitudes towards mobile apps and the potential privacy riskiness of a particular app, nudging them to make app installation and/or permission granting decisions reflecting their privacy attitudes. To evaluate this interface, we conducted an online experiment simulating the process of installing Android apps. We compared the privacy discrepancy approach with several existing privacy notification approaches. Our results suggest that the behaviors of participants who used the privacy discrepancy interface better reflected their privacy attitudes than the other approaches.

CCS Concepts: • **Security and privacy** → **Privacy protections**; **Usability in security and privacy**; *Domain-specific security and privacy architectures*; • **Human-centered computing** → *Empirical studies in HCI*;

Additional Key Words and Phrases: Privacy interfaces, warnings, notice and choice, personalization, privacy attitudes, privacy behavior, privacy paradox, mobile apps, permission systems

ACM Reference Format:
Corey Brian Jackson and Yang Wang. 2018. Addressing The Privacy Paradox through Personalized Privacy Notifications. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 68 (June 2018), 25 pages. https://doi.org/10.1145/3214271

1 INTRODUCTION

People often face privacy threats as they embrace different technologies from the Internet to mobile devices to the Internet of Things (IoTs). Prior research has shown that people's actual behaviors sometimes divert from their stated privacy attitudes, a phenomenon known as the *privacy paradox* [34]. Privacy attitudes represent people's views of what aspects of their privacy they consider important and/or how their privacy should be protected, whereas privacy behaviors denote their actual actions that might impact their privacy.

The privacy paradox occurs in situations where the relationships between user intentions and user behaviors across privacy–related contexts seem rather contradictory. In turn, these inconsistencies may lead to troublesome or regrettable experiences. For example, while people often express concerns about disclosing their information to companies, nevertheless they share their personal information when creating accounts in online shopping

Authors' addresses: Corey Brian Jackson, School of Information Studies, Syracuse University, 343 Hinds Hall, Syracuse, NY, 13210, USA, cjacks04@syr.edu; Yang Wang, School of Information Studies, Syracuse University, 343 Hinds Hall, Syracuse, NY, 13210, USA, ywang@syr.edu.

2474-9567/2018/6-ART68 $15.00
https://doi.org/10.1145/3214271

sites to enjoy small discounts, not realizing the potential ramifications (e.g., being profiled, receiving targeted ads, their data being sold or shared to third parties). Furthermore, while people would like to maintain their privacy on Facebook, they post content about themselves that they later regret [38].

Scholars such as Acquisti have suggested that these privacy behaviors can be irrational or sub optimal and the ability for users to act rationally to invoke privacy preserving behaviors might be subservient to the immediate gratification they may gain (e.g., buying things at a discounted price) [1]. While people can reap the benefits of using discounts, they often do not know or underestimate the full implications of disclosing their personal information to companies.

To help people address the inconsistencies between privacy attitudes and behavior, we propose a personalized privacy notification approach that brings such inconsistencies to the fore, when users make privacy decisions. In this paper, we focus on the domain of mobile apps where they request users for permissions to access various resources or information (e.g., contact book, location or camera) on their mobile devices. A line of prior research has shown that users are often unaware of the adverse impact of granting apps access to certain permissions [14, 18, 25, 30, 31].

We designed a *privacy discrepancy* interface that juxtaposes individual users' privacy attitudes towards mobile apps with the potential of these apps to violate user privacy, thus highlighting the discrepancy between a users' attitudes and their behavior with respect to the permissions being requested by mobile apps. Our interface is an attempt to mitigate the effects of privacy paradox by bringing this contradiction to the fore during the app installation process. Our intuition is showing users this juxtaposition or discrepancy might nudge them to make decisions in line with their privacy attitudes. To the best of our knowledge, this key idea of explicitly showing and leveraging the juxtaposition of the discrepancy between individuals' privacy attitudes and the impact of technology use to nudge them to privacy–appropriate behaviors is novel.

To operationalize and measure people's general privacy attitudes towards mobile apps, we adopted the Mobile Users' Information Privacy Concerns (MUIPC) [40] survey, a validated scale designed for the mobile context. This scale measures individuals' privacy concerns about *intrusion* into personal data, *surveillance* of activities, and *secondary use* of data in the mobile context.

To evaluate our privacy discrepancy interface, we conducted an online experiment that simulated the process of installing Android apps. We compared the privacy discrepancy interface to four privacy notification alternatives. First, a *control* interface mimics the default app installation interface on Android (version 5.1, Lollipop) where no additional information about permissions is shown. The second interface (*privacy personal*) displays users' general privacy concerns about mobile apps as measured by the MUIPC scale. The third interface (*privacy rating*) shows users the potential privacy riskiness of specific apps' permission requests. Finally, there exists a (*non-privacy*) interface that looks the same as the privacy discrepancy interface but represents different underlying semantics (accessibility rather than privacy) to serve as a sanity check to confirm that people are actually responding to privacy information rather than just the visual appearance of the interface. Our study results suggest that the behaviors of participants who used the privacy discrepancy interface better reflected their privacy attitudes than the other approaches tested.

This paper makes two main contributions. First, we propose a personalized privacy notification approach to nudge users towards behaviors that reflect their privacy attitudes. This approach provides direct feedback so users can modify permissions to match their privacy concern levels. This approach can also be applied to other domains, especially those with a permission system, such as social applications on Facebook or plugins for web browsers. Second, we present empirical results from an online experiment, showing that the privacy discrepancy approach better aligned users' privacy behaviors to their attitudes than the other approaches tested.

2 PRIVACY NOTIFICATIONS

Communicating privacy risks to users via notifications has been an active line of research. In the context of mobile apps, prior work on designing notifications alerting users about potential privacy risks has often adopted a soft–paternalistic approach (e.g., [2, 5, 6, 9, 11, 23, 25]), where researchers and/or designers analyze apps' permission requests and data use to make value judgments about whether specific apps (or permission requests) pose a privacy threat. Soft paternalism (or nudging) avoids coercion with the goal of steering users towards desired behaviors [2] and are frequently based on researchers' (or crowds') views of acceptable levels of data access. These prior efforts on privacy notifications can be grouped into two broad categories: one that does not consider the potential individual differences of users, and another that does.

Prior studies in the first category aim to increase users' knowledge about the purpose of permission requests (e.g., [9, 23, 25]) and/or help users guard against potentially malicious activities by apps (e.g., [5]). For instance, Almuhimedi et al. [5] designed a system to inform users about data collection practices of apps installed on their devices. After downloading an app, users are periodically nudged to review and adjust (i.e., restrict or permit) permission settings. Kelley et al. [23] designed Privacy Facts, a "just-in-time" privacy display warning users when sensitive information such as location is being requested. Lin et al. [25] showed users results from "the crowd" that revealed the degree to which permission requests break users' expectations. Using this approach, users rely on the ratings of other users about permission requests of mobile applications [25].

Prior studies in the secondary category consider individual users' personal data, preferences of app permissions, or past behaviors (e.g., [16, 19, 27, 28, 39]). Therefore, these approaches are personalized because they are tailored to individual users as decision makers determining or negotiating their own privacy boundaries. Liu et al. analyzed usage of Privacy Guard, a system notifying users when apps attempt to use sensitive permissions [28]. Notifications are based on four user-defined access permission levels: always grant, always deny, dynamically alert, and the default logic provided by Privacy Guard to protect privacy. By clustering similar user profiles, Privacy Guard takes users' aggregated download behaviors and predicts the apps users would download [28]. Securacy, developed by Ferreira et al. [16], asks users to pre-specify permissions they are uncomfortable allowing apps to access and alerts users accordingly. Harbach et al. [19] enhanced the install interface to allow users to contextualize privacy requests by showing personal data taken from their devices. Tsai et al. [36] designed TurtleGuard, a system that can automatically predict user decisions regarding app permission requests and also allows users to audit and modify any decisions made by the algorithm.

Our privacy nudges consider individual users' general privacy concerns regarding mobile apps and thus are personalized, falling into the second broad category. However, our approach differs from other personalized notification approaches in two ways. First, while previous studies explicitly ask permission for categories accessed by apps users are most uncomfortable with (i.e., privacy preferences), we instead capture users' general privacy concerns of mobile app use via an established and validated privacy scale focusing on three types of concerns (intrusion into personal data, secondary use of data, and surveillance of activities) on mobile devices. Relying on people's pre-specified privacy preferences has three important limitations: (1) mobile users might not understand the implications of permissions especially when users are not technically savvy; (2) people are often uncertain about their own privacy preferences [4]; and (3) their preferences may change over time. For these reasons, we argue that our approach is more reliable because people do not need to be technically savvy to have general attitudes or concerns and these general attitudes tend to be more stable as they reflect high-level values that people support. Second, our approach displays the discrepancy between a users' general concerns and app behaviors to trigger user behavioral changes. This is done by bringing the discrepancy to the forefront when users make app permission decisions.

On the web, Privacy Bird warns users about discrepancies between privacy policies of websites and users' web privacy preferences [12]. When website privacy policies permeate privacy boundaries established by users,

Privacy Bird notifies users via colored icons representing different levels of risk [12]. Our privacy discrepancy approach could also be applied to web privacy, where our interface would juxtapose users' general privacy attitudes towards websites and the riskiness of a particular website in addition to the discrepancy of the two. In some way, Privacy Bird only shows the discrepancy, whereas ours would show not only the discrepancy but also the two constituents of such discrepancy.

Our main research question is: *to what extent do different privacy notification approaches affect users' decisions to install mobile apps and adjust their permissions?* To answer this research question, we compared the behaviours of users in each experimental condition where they saw a particular type of privacy notification. Our specific research hypothesis is: *people who use the privacy discrepancy interface will make privacy decisions that better match their privacy concerns than other alternatives.*

3 SYSTEM DESIGN

The key idea behind our privacy discrepancy interface is to explicitly juxtaposes individual users' general privacy attitudes towards mobile apps with the privacy riskiness of these apps (as a result of its permissions granted), then the highlighted discrepancy could nudge users to make app permission decisions that align with their general privacy attitudes precisely when making such decisions. Our inspiration was that bringing the privacy paradox to the fore might trigger users to engage in behaviors that reduce such inconsistencies. This is somewhat similar to the phenomenon around cognitive dissonance, which refers to people's state of facing contradictions or discrepancies of thoughts or behaviors [17]. This can cause some feeling of discomfort, which may then trigger people's behaviors in reducing the discrepancy [17].

Our design was also in part inspired by the theory of contiguity [29] which suggests that spatial and temporal display of a stimuli and response impacts outcomes. Kumaragururu et al. used this contiguity principle to develop privacy training materials placing images and relevant text descriptions contiguously in the instructions and found better learning results [24]. Our design placed the privacy discrepancy information with app permission information contiguously on the app install interface to assist users in making more informed decisions. In addition, our design also learned from existing interfaces such as Privacy Bird [12] and Privacy Grade [25, 26], which use colored icons/letters to signal the level of privacy riskiness.

Our privacy discrepancy interface was built on two key components: individuals' privacy attitudes towards mobile apps, and the privacy riskiness of mobile apps. We first present how we operationalize these two concepts before describing the visual aspect of the interface.

3.1 Measuring Individual Users' Privacy Attitudes towards Mobile Apps

We chose to utilize individual users' privacy attitudes rather than preferences. DePaula et al. note a constant difficulty for users to foresee and specify their privacy preferences before using a system because privacy needs are contingent and context-dependent and thus hard to specify a priori [13]. Therefore, rather than utilizing users' privacy preferences, we chose to use their general privacy attitudes which are arguably more stable and easier to obtain. To understand users' privacy preferences of Android app permissions, one might need to ask at least one question for each (dangerous) permission. There are over 200 permissions in Android including 22 dangerous permissions. In comparison, one would need a much smaller set of questions to understand the different dimensions of his or her privacy attitudes.

More specifically, we operationalized and measured individuals' general privacy attitudes towards mobile apps using the Mobile Users Information Privacy Concerns (MUIPC) [40], a validated privacy scale specifically designed for mobile contexts. Other privacy concern scales such as Concern for Information Privacy (CFIP) [21] or Internet Users' Information Privacy Concerns (IUIPC) [32] are more general while the MUIPC is built on these scales and focuses on mobile contexts. The MUIPC scale contains nine questions (using a 5-point Likert

scale), measuring three constructs: user concerns about perceived intrusion, secondary use of information, and perceived surveillance. We developed a single score by averaging the responses to questions pertaining to each construct. To operationalize the score into discrete levels for later visual representation (using the three-color traffic light metaphor, which we will detail later), we divide the 5-point score by three: 1-1.66 representing low privacy concern, 1.67-3.33 as medium concern, and 3.34-5 representing high concern. It is important to note that our privacy discrepancy approach is not locked in this particular working scheme to measure individuals' privacy attitudes on a three-level scale and depending on the application domain, the researchers can use a privacy riskiness measurement approach deemed appropriate. The MUIPC dimensions/constructs and questions are included in Appendix A.

3.2 Measuring Privacy Riskiness of Mobile Apps

To operationalize and measure the privacy riskiness of specific apps, we coded app permissions vis-à-vis their relevance to the three MUIPC constructs. We first established a baseline for permission requests. Prior research [15, 35] found that, on average, apps request 4-5 permissions. Therefore, as a working definition, we chose to consider apps requesting 1-3 permissions associated with each construct as having low risk, 4-7 as medium, and 8 or more to be high risk. For instance, if a certain app requests four permissions related to perceived surveillance, then we consider this app to contain a medium-level riskiness of surveillance. How we determined whether permission requests are related to a MUIPC construct (we called it permission rating) is detailed below. Similar to our working scheme of measuring privacy attitudes, we note that our privacy discrepancy approach is not locked in this working definition of different levels of privacy riskiness. Researchers or designers can replace this definition with one they deem more appropriate for their application domain.

The permissions requested by each app needed to be coded individually since the same permission can be used differently by various apps. In addition, how apps use the data collected from a particular permission could be related to one or many constructs. We conducted permission ratings using two complementary approaches.

First, we leveraged the permission analysis of Privacy Grade[1], a project that has analyzed 20 sensitive permissions [25, 26]. Using primarily a static code analysis, Privacy Grade examines the downstream use of each fine-grained permission requested and provides a description of how each app uses each permission. For example, Privacy Grade analyzed the Instagram app (version 6.19.0) and found the app requesting eight sensitive permissions such as *Full network access, Find accounts on the device, Record audio, and Precise location (GPS and network-based)*. Privacy Grade then determined that the *Full network access* permission was requested by Instagram for three use purposes: internal use consistent with the app's functionality, social networking services, and general utility functions. For our analysis of particular apps, we collected fine-grained permissions requested and Privacy Grade summaries of use for each permission. Next, for each summary of use, we coded whether the use had potential to contribute to two MUIPC constructs: secondary use and intrusion. Since Privacy Grade summaries do not speak to the concept of surveillance, we coded and counted the requested permissions that were related to surveillance to measure their surveillance risk. In particular, our coding was guided by Solove's [33] definition of surveillance as "the watching, listening to, or recording of an individual's activities." For a given app, we considered any permission that contributed to watching, listening to, or recording as fitting with the definition of surveillance. For example, *read sensitive log data* was not examined by Privacy Grade but since this permission could collect user information, we considered it as having surveillance potential.

Second, for any fine-grained permissions not analyzed by Privacy Grade, we conducted our own analysis to identify the potential for intrusion, secondary use and surveillance. If we were unsure about a particular permission, we consulted the official Android Developers website. It is worth noting that each fine-grained permission can also be associated with none or all three MUIPC constructs since apps can use permissions for

[1] http://www.privacygrade.org

different purposes. In both approaches, coding was conducted in two rounds by three researchers including one professional Android app developer. In the first round, each researcher read the description of the MUIPC constructs and independently coded each fine-grained permission. After this round of coding, the results were reviewed and converged when necessary. For example, there was disagreement on the permission request of *view network connections*. The Android Developer site describes that this permission "allows the app to see what networks the device has access to." Based on this description, we decided this permission has the potential to enable location-based ads because the app could infer the device location based on the network it connects to. Thus, this permission could contribute to secondary use (e.g., location-based ads). This round of coding yielded Cohen's kappa values for our inter-coder reliability of: .70 (intrusion), .71 (secondary use), and .70 (surveillance). All values were at or above the acceptable threshold of .70 [10]. In the second round, permissions were independently coded using the updated code book.

3.3 The Privacy Discrepancy Interface

The privacy discrepancy interface built on the default app install interface in Android 5.1 (Lollipop) by adding several privacy components. Figure 1 (a) shows the privacy discrepancy interface when none of the three privacy icons is clicked and (b) shows the same interface when only one of three privacy icons is clicked.

3.3.1 Design of Privacy Icons. A major component of this interfaces is the display of three privacy warning icons for perceived intrusion, secondary use of information, and perceived surveillance, respectively. These icons were at the bottom of the interface, shown in Figure 1 (a). To display these three constructs, we adopted the three-color approach used in Privacy Bird [12]. Leveraging a familiar metaphor of traffic lights, green represents low risk, yellow represents medium and red represents high risk. The difference in our interface is the semantics behind these icons and how the colors are determined. Each construct has a warning level computed using two variables - user privacy attitudes/concerns and app privacy riskiness.

Figure 1 (a) shows the current design of these three icons. We first prepared six candidate icons to represent each MUIPC construct. These icons were inspired by images from the Noun Project [2] and from Aza Raskin's (Mozilla web browser) privacy icon designs [3]. We then conducted a study on Amazon Mechanical Turk (AMT) to determine the best icons. We recruited 100 workers, presented them with six candidate icons for each MUIPC construct, and asked them to select the icon that best represents each construct. We then used the most frequently selected icons in the interface. In addition to the icons, we also included two features to help users better understand the logic behind the warning levels.

3.3.2 Associated Permissions. When users clicked one of the three privacy icons, the permissions associated with that MUIPC construct will be highlighted. This feature allows users to know which permissions to adjust if they wish to reduce the risk level for that construct. Figure 1 (b) shows this feature. When users click a privacy icon in (3), the permissions associated with such icon are highlighted in (2). If users desire to reduce the privacy risk of intrusion, they can un–check (1) the permission. In this example, in-app purchases was un–checked. The app's risk is dynamically updated and a new risk level is shown (3).

3.3.3 The Discrepancy Sub-Graph. The key idea behind the privacy discrepancy interface is the juxtaposition of individual users' general privacy attitudes (here we operationalized using MUIPC concerns) towards mobile apps and the privacy riskiness of such apps. When users click a privacy icon (in this case, intrusion), the aforementioned concepts are represented as two bar graphs in Figure 1 (b) (6). The top bar "App Riskiness" represents the current app's privacy riskiness (calculated based on the number of allowed permissions related to intrusion). The bottom bar "My Comfort Zone" represents the inverse of users' average answers for the three intrusion MUIPC questions.

[2] https://thenounproject.com
[3] http://www.azarask.in/blog/post/privacy-icons/

For example, if users reported a high level of privacy concern about intrusion (average score 4.5), then their "My Comfort Zone" would be (5-4.5=.5) low. By juxtaposing these two values, this part of the interface highlights the mismatch between their concern and the app permission requests. By double-tapping each icon, users can view the discrepancy between their concerns and the riskiness of each app. Figure 1 (b) (5) displays a definition of the intrusion MUIPC construct and upon clicking the permission users can view a description of each permission (Figure 1 (b) (4)).

3.3.4 The Colors of Privacy Icons. The colors of the privacy icons in Figure 1 (b) (3) are determined by considering the difference between users' privacy concerns and privacy riskiness of each app, shown as the two bar graphs in Figure 1 (b) (6). Intuitively, if users are very concerned about surveillance in using mobile

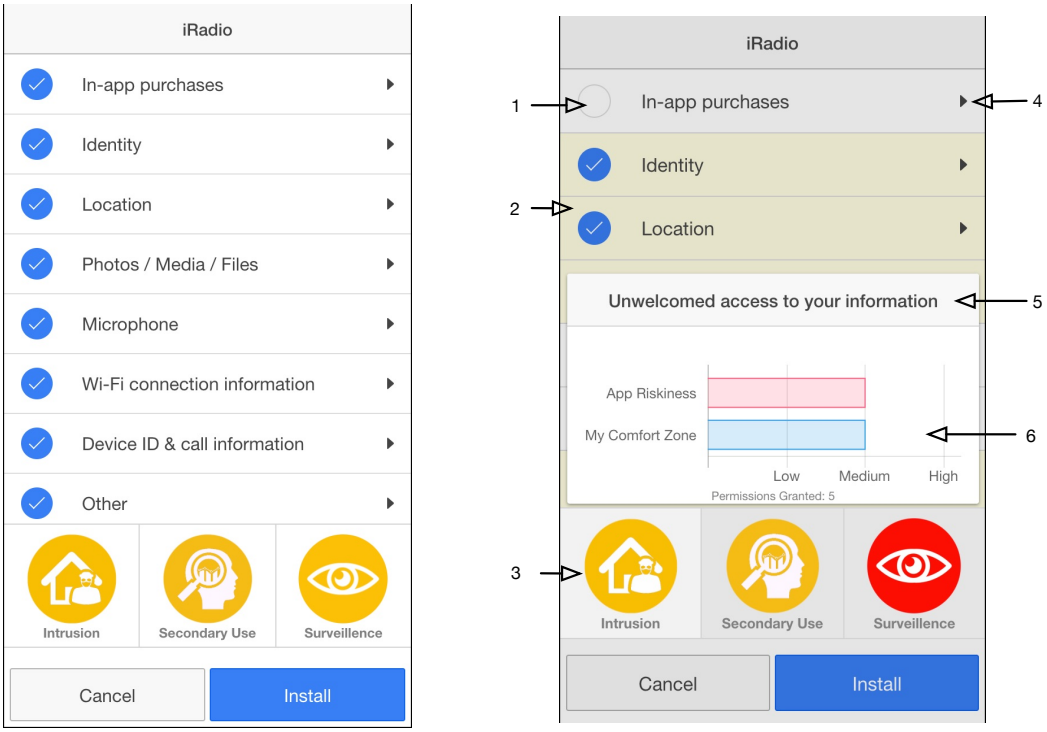

Fig. 1. The privacy discrepancy interface when none of the three privacy icons is clicked (a), and the privacy discrepancy interface when one privacy icon is clicked (b). The figure (b) shows all the privacy features. For instance, when users click the intrusion icon, the privacy discrepancy interface shows: (1) check/un-check the permission button to grant or deny an app's permission request, (2) the default checked permissions that were requested by the app and were associated with the intrusion MUIPC construct, (3) the MUIPC construct and its associated risk level represented by the icon color, (4) expanding tab for permission description, (5) summary definition of the intrusion MUIPC construct, and (6) the top bar shows the level of privacy riskiness of the app in terms of intrusion, and the bottom bar represents the user's privacy comfort zone in terms of intrusion, which is the inverse of the user's MUIPC intrusion concern score (e.g., if the average intrusion concern score is 3, then the comfort zone score is 5-3=2). The colors of privacy icons were determined by the mappings shown in Figure 2. When users adjust permissions, the bars in (6) will be re-calculated and the icon colors in (3) will be updated accordingly.

apps (thus low in "My Comfort Zone" bar) and the app under consideration has a high level of riskiness in surveillance (because the app requests too many permissions that can lead to surveillance), these decisions would essentially divert from their privacy attitudes/concerns towards surveillance if users accept all permission requests. Therefore, the color of the surveillance icon would be red, signaling a high level of discrepancy between users' privacy concerns and the privacy riskiness of surveillance for each app. Figure 2 shows our scheme to determine the color of privacy icons based on users' privacy concerns and the privacy riskiness of specific apps. In general, the increasing levels of discrepancy would map to the icon colors of green, yellow, and red.

3.4 Privacy Notification Interfaces

Besides the privacy discrepancy interface, we designed four additional interfaces to compare with the discrepancy interface. These five interfaces were tested in our study, which we will describe in the next section. Below we briefly explain these interfaces.

(1) *Control.* This interface mimics the app install interface in Android 5.1 (Lollipop). At the time we launched the study, Lollipop's permission model showed users permissions requested by apps and forced users to either accept all permissions or not install the apps. No new information about each app is displayed to users. However, since all other interfaces we tested allow users to adjust permissions, we decided to add this permission adjustment feature to this control interface so that we can control for the effect of users' ability to adjust permissions when comparing different interface conditions. This control interface looked the same as the non–privacy interface shown in Figure 3 (a) without the three colored icons at the bottom.
(2) *Privacy Rating.* The privacy rating approach highlights the privacy riskiness of each app and is shown in Figure 3 (b). This interface represents the approach where researchers or third parties assess the riskiness of apps. Users can see the "App Riskiness" bar for each MUIPC construct by double-tapping each privacy icon. The colors of the privacy icons are determined by the level of app riskiness (e.g., red means a high level of riskiness).
(3) *Privacy Personal.* This approach provides users with a reminder of their own privacy attitudes. This approach represents a user-centered approach to privacy notifications. The colors represent user's level of privacy concern about mobile apps, based on the the user's MUIPC concern score (e.g., red means a high level of concern). This interface is shown in Figure 3 (c). Users can view the "My Trust Level" bar (i.e., inverse of his or her MUIPC concern score) by double-tapping each privacy icon.
(4) *Privacy Discrepancy.* This approach was designed to highlight the discrepancy between people's privacy concerns (i.e., MUIPC scores) and the riskiness of each app's permission requests. Users can view the

			User Concern		
			High [3.34-5]	**Medium** [1.67-3.33]	**Low** [1-1.66]
App Score	**MUIPC Constructs** Intrusion Secondary Use Surveillance	**High** [>= 8]	Red	Red	Yellow
		Medium [4-7]	Red	Yellow	Green
		Low [1-3]	Yellow	Green	Green

Fig. 2. Our scheme of determining icon colors for the *Privacy Discrepancy* interface.

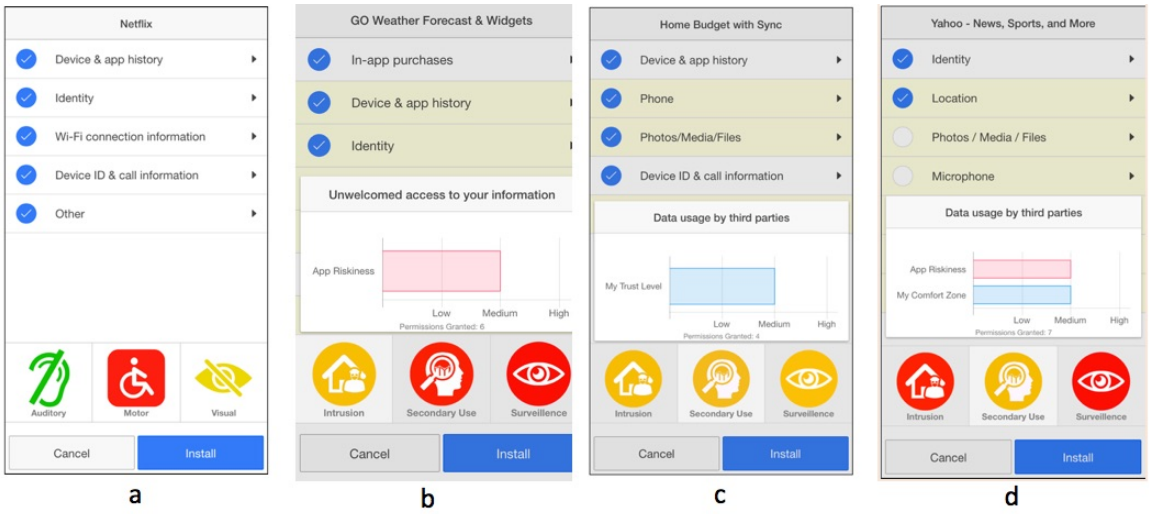

Fig. 3. User interfaces used in four conditions in our study (control excluded). The control condition is essentially the non–privacy interface (a) without the three colored icons at the bottom. In each case users can de-select permissions to reduce the apps' riskiness. From left to right: (a) the non–privacy interface; (b) privacy rating; (c) privacy personal; and (d) privacy discrepancy (d) are shown. For the rating, personal, and discrepancy conditions the interface can look the same except that the icon colors are determined differently. When each icon is clicked once, the permissions associated with the icons are highlighted. When users double-click the icons, additional privacy information is displayed.

"My Comfort Zone" (i.e., inverse of his or her MUIPC concern score) and "App Riskiness" bars for each MUIPC construct by double-tapping the corresponding privacy icon. The icon colors represent the level of discrepancy between these two bars (e.g., red means a high level of discrepancy).

(5) *Non–Privacy.* This interface was designed and included as a sanity check to verify that users would not simply make permission adjustments to change the icon colors without knowing the underlying (privacy) semantics. This non–privacy interface showed icons related to how accessible each app is for users with physical, motor, and visual impairments. The idea is similar to assessing app privacy riskiness except we assessed how well apps supported individuals with these three impairments. We added three questions to the beginning of the user concern survey to measure their level of impairment concerns (i.e., *I have serious difficulty hearing; I have serious difficulty seeing, even when wearing glasses; and I have serious difficulty using a mouse, clicking on small links, or operating dynamic elements on a web-page effectively*). However, we did not use their responses to display the warning levels; we simply used the privacy discrepancy approach and changed the three icons to represent the discrepancy for visual, motor, and hearing impairments. This interface is shown in Figure 3 (a). The only difference between the non–privacy interface and the privacy discrepancy interface was a difference in icon shapes (the former representing accessibility semantics while the latter represented privacy semantics). If users adjust a similar amount of permissions in these two conditions, then it would call into question whether users actually understand the underlying privacy semantics of the icons or only react to the icon colors.

Figure 4 shows the processes by which different interfaces were generated (or how colors of the privacy icons were determined). The privacy rating interface was generated based on app privacy riskiness, which was in turn assessed by researchers. The privacy personal interface was generated based on users' responses to the MUIPC

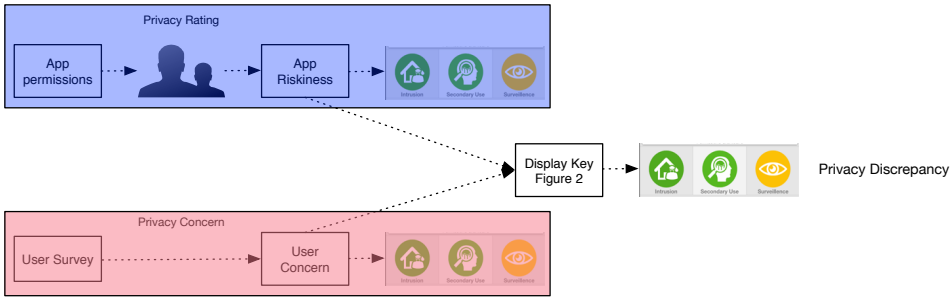

Fig. 4. The flow for displaying the privacy icons. The top represents the privacy rating interface and the bottom represents the privacy personal interface. The middle represents the privacy discrepancy interface.

concern survey. The privacy discrepancy interface was generated by combining the information from both app privacy riskiness and a users' privacy concerns.

4 STUDY METHODOLOGY

To assess and compare the impact of five different privacy notification interfaces (four shown in Figure 3 and the default Android interface as control) on users' app installation and permission decisions, we conducted an online experiment beginning in August 2016. This study was approved by our University's Institutional Review Board.

4.1 Pilot Study

We conducted a pilot study to solicit feedback related to our interfaces. We asked four friends to think aloud while they used the various interfaces. They also went through the entire study answering the MUIPC questions and interacting with the permissions screen to adjust/install apps. Based on their feedback, we made adjustments to the interfaces. For instance, we refined the images used to display the privacy icons for the MUIPC constructs.

4.2 Study Design

Our study consisted of a sequence of twenty app-choice tasks. Each task required participants to review particular apps and the permissions requested by each app and make a decision to either install or reject each app. Since modifying the official Google Play store is unrealistic, we conducted our study via the web to simulate the Android app installation process by showing participants an app information page and the permission lists with our interfaces. A prior study of mobile privacy notifications (about app data collection rather than permission requests) has found that their field experiment and online simulation study of the same interface design yield similar results [7]. This suggests that online simulations can be a reasonable alternative for testing new mobile privacy notifications. In our study, we had five experimental conditions, corresponding to five privacy notification interfaces: control (i.e., a mimic of the Android 5.1 Lollipop app install interface), non-privacy, privacy rating, privacy personal (concern), and privacy discrepancy. The study had a mixed design, where each participant was randomly assigned to use one privacy notification interface (between-subject) to conduct 20 app tasks (with-in subject). We included both popular and less popular mobile apps. In our study instructions, we only requested participants to install or reject apps and did not explicitly ask them to interact with the privacy interface nor adjust permissions.

4.3 Selecting Apps

The primary task required each participant to make decisions about whether or not to install the same list of 20 apps. We chose 20 apps by visiting the web version of the Google Play Store where apps are grouped into one of 17 categories (e.g., References, Music) based on their purpose. We randomly selected ten categories. For each, we then randomly selected one app in the higher download range and one in a lesser download range. We preferred apps analyzed by Privacy Grade since it has already examined the apps' requested permissions. If one particular app was not analyzed by Privacy Grade, we tried to replace the app with a similar one analyzed by Privacy Grade. The 20 apps used in our study were: *Yahoo - News, Sports, and More, The Weather Channel, iRadio, Pharmacy Pill ID & Drug Info, Home Budget, Noon Walk Pedometer: Fitness, GO Weather Forecast & Widgets, Netflix, theScore, Photobucket, Family Budget, Marvel Comics, Pedometer, Viewster, Daily Mail, First Aid & Symptom Checker, Fox Sports, Flickr, Rage Comics, and Pandora.* Every participant saw all apps and each app once. Since it was the same set of apps for all interface conditions, we expect the popularity of the apps to affect all conditions uniformly and thus to have minimum impact on the comparisons of user behaviors under different conditions.

4.4 Experiment Procedure

In terms of the study procedure, Figure 5 outlines the sequence of tasks users were asked to complete. We recruited participants from Amazon Mechanical Turk (MTurk) where they selected our human intelligence task (HIT). We described the study stating that we "...wanted to understand how users make decisions about installing applications on their mobile devices." We refer to our participants as "users" henceforth. If users wished to continue, they clicked a link in the HIT and were directed to a screening survey hosted on Qualtrics, an online survey platform. Once they provided their informed consent in the survey, they were asked questions to determine whether they were qualified to complete the study. If they met the qualifications (e.g., over 18, Android users), we then supplied a link to our online study and a participant ID so we can link their survey responses to the study responses. Using a round-robin scheme, each participant was placed in one of five experimental conditions (corresponding to the five privacy notification interfaces). At the first screen, users were asked to enter their participant ID. Once entered, users were asked to complete the MUIPC survey to measure their privacy concerns as well as other non-privacy items (accessibility). For consistency, users in all conditions were asked the same questions even for those users assigned to the non-privacy condition. Next, users viewed a one-minute video tutorial explaining the interface (assigned to them), for instance, which buttons could be clicked and what additional information would be presented. The videos for the privacy rating and privacy discrepancy interfaces also explained the meaning of each icon and how selecting/de-selecting permissions could change the privacy rating or discrepancy and thus colors of the privacy icons. Users were then directed to the list of 20 apps they needed to decide whether or not to install. The default requested/checked permissions of each app in our study were the same permissions that the app would request in practice.

Users had to cycle through all 20 apps; the order of the apps was randomized for each user. When viewing each app, users could use the features described in the previous section (e.g., checking/un-checking permissions, clicking privacy icons to see more information). Users could choose to reject or un–check any requested permission. Users then decided either install or reject each app. Once users made a decision regarding installing or rejecting the app, they were redirected back to the list to evaluate the remaining apps. Users could not revisit the app after submitting their decision.

After cycling through the 20 apps, users were directed to another Qualtrics survey where we asked them to complete a exit survey (see Appendix items C and D). Here, we asked open-ended questions about the interfaces such as whether they understood the meaning of the privacy icons and how the icon colors were determined. We also included questions from the System Usability Scale (SUS) , an instrument for measuring usability. The

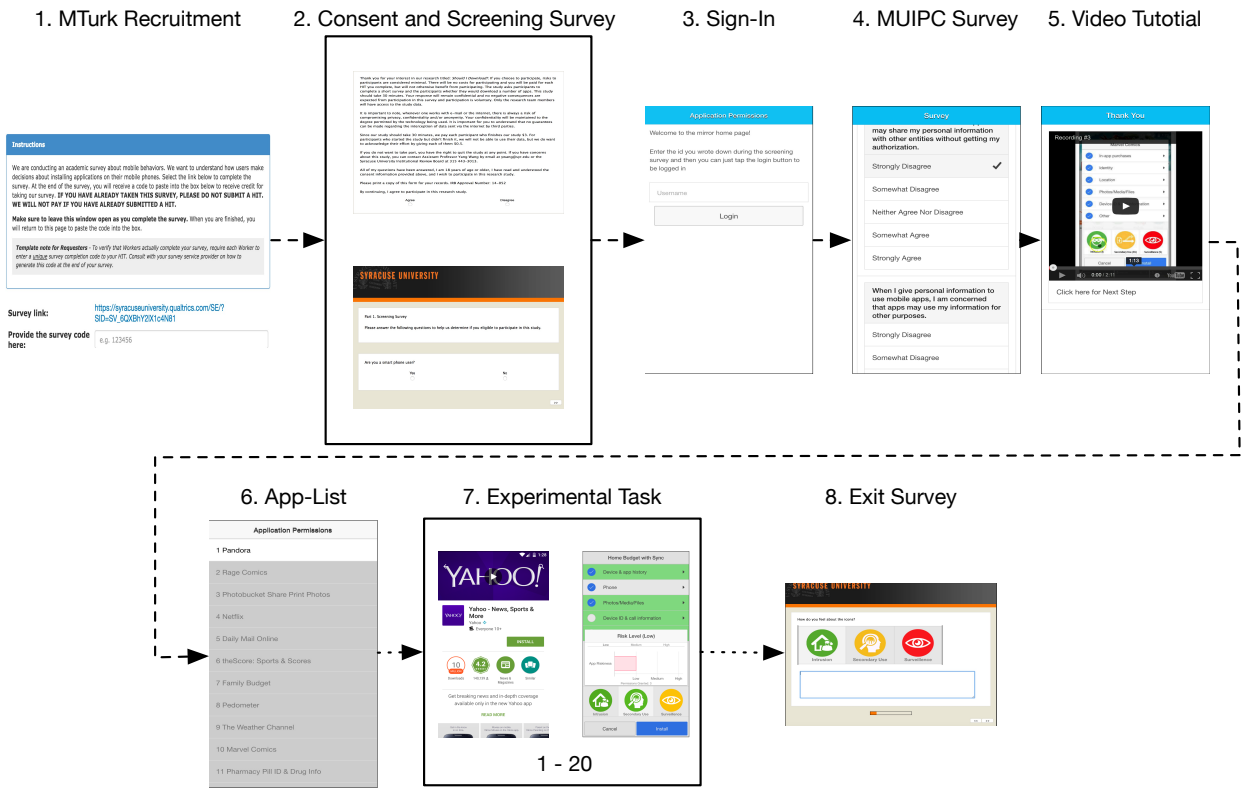

Fig. 5. The study procedure showing: (1) the MTurk advertisement, (2) the consent and screening survey on Qualtrics, (3) the first screen of the simulated interface asking users to sign-in, (4) the MUIPC privacy concern survey and non-privacy questions (see Appendix A and B), (5) the video tutorial [20], (6) the list of 20 apps, (7) the app information screen and the privacy notification interface with the permission list, and (8) the exit survey (see Appendix C and D).

SUS (see Appendix item D) consists of of a ten-item questionnaire with Likert-type scale responses ranging from Strongly Agree to Strongly Disagree.

4.5 Participants Recruitment and Screening

We recruited participants on MTurk. To ensure we received quality responses, we required participants to have HIT approval rates greater than 90%, be located in the United States, and be users of Android devices. We performed several checks to verify the participants actually met these criteria. First, we asked questions about their devices such as their phone model and the OS version installed. Second, a common problem with MTurk studies is MTurk workers with multiple accounts complete HITs more than once. The survey phase of our study was conducted using Qualtrics, a survey platform that collects geo–location information (e.g,. latitude, longitude, and IP Address). In cases where an IP address was observed more than once, user responses were removed. Finally, we read responses to open-ended questions to determine if users made effort an answering the questions. We also removed records when their responses were illegible or incoherent. After the quality checks, 241 respondents remained. On average, the study took 25 minutes to complete and we paid $3 to each participant who completed

the study. To avoid priming users about privacy, we deliberately avoided the word "privacy" in all recruitment materials and throughout the study.

4.6 Data Analysis

To test our hypothesis: *people who use the privacy discrepancy interface will make privacy decisions that better match their privacy concerns than other alternatives*, we logged participants' answers to the MUIPC survey, their interactions with the privacy interfaces as well as their app installation and permission adjustment behaviors.

The quantitative data from our study was mostly analyzed using linear mixed effects modeling (LMM). Mixed models allow us to examine the data as repeated measures and allow us to account for the individual variability for each user. LMM contains both fixed and random effects. Fixed effects are factors of interest manipulated in our study (e.g,. experiment conditions). Random effects are factors that measure the individual variability (in technical terms, a random intercept) for some variable (e.g., user) which we wish to generalize. Including random effects allows us to correlate measures across the same subject since users are repeated in the data. To assess the fit of each model, we compared them using the likelihood ratio test (LR rest), which produces the chi-squared goodness-of-fit. The analyses were carried out in the R programming environment using the lme4 package [8].

To test our hypothesis, we mainly focused on two analyses. First, we examined the effect of each privacy interface on users' decisions to install an app. Thus, a mixed–effect regression with logistic function was used to model binary outcome variables (1= install, 0=reject). Second, we examined whether differences exist in the number of permissions granted for each MUIPC construct among different experiment conditions using LMMs.

Finally, we conducted a thematic analysis of the open-ended survey responses. We independently coded responses from the exit survey. We then met twice to discuss the themes and then consolidated the code book to settle on a handful of themes for the questions we asked participants. In the qualitative results, we present major themes emerged from users' responses.

5 RESULTS

We first describe participant demographics and their privacy concerns. We then address the question of whether our participants only paid attention to the icon colors and ignored the underlying meaning of the icons. Subsequently, we describe how users interacted with the privacy interfaces. Next, we address our primary research question and hypothesis, reporting participants' behaviours regarding app installation and adjustment of permissions, as well as the alignment between privacy behaviors and attitudes. Finally, we report the usability evaluation results of the privacy interfaces.

5.1 Participant Demographics

A total of 241 participants completed our study: 151 participants (63%) were male, 89 participants (37%) were female, and one participant (< 1%) chose not to answer. In terms of age, the majority of participants were between 21-30 (N=121, 50%), followed by 31-40 (N=83, 34%), and 41-50 (N=23, 10%). Other age groups were less than 1% each. Every participant answered the MUIPC survey containing nine 5-point Likert scale questions (see Appendix A). Each of the three constructs (surveillance, intrusion, and secondary use) consists of three questions. We computed each privacy concern score for each construct by averaging the three constituent questions: 5 indicates high concern and 1 indicates low concern. Overall, participants had a high level of privacy concern: surveillance (M=4.05, SD=0.82), intrusion (M=3.99, SD=0.94), and secondary use (M=3.79, SD=0.91).

To verify whether participants in different experiment conditions had significant differences in privacy concerns, we conducted an ANOVA analysis for each construct. We did not find significant differences among the five groups for the three constructs: surveillance $F(5,302)=0.57$, $p > 0.05$; intrusion $F(5,302)=0.32$, $p > 0.05$; and secondary use $F(5,302)=0.56$, $p > 0.05$. This suggests participants across conditions had comparable privacy concerns.

5.2 Sanity Check: Did Participants Only Focus on Icon Colors and Ignore The Underlying Meaning?

Before we dive into the comparative analysis between different privacy interfaces, there is an important question to answer - whether participants simply used the icon colors without understanding what the colors represented to guide their decisions in adjusting permissions. To analyze whether this was the case, we compared the discrepancy condition (56 users) to the non–privacy condition (48 users), which was used as a sanity check. The two interfaces only differed in the icons displayed and the underlying meaning of the icons. Participants in these two conditions also had comparable risk (warning level) distributions and thus saw comparable distributions of privacy icon colors (non–significant difference, $p > 0.05$). The non–privacy condition displayed icons related to accessibility rather than privacy.

If participants only made permission adjustments to reduce the warning levels (i.e., icon colors) and did not understand or care about the underlying privacy meanings, we would expect there to be non-significant differences in the number of permissions rejected between these two conditions.

In contrast, our results suggest that was not the case. On average, participants rejected a significantly larger number of permissions in the discrepancy condition for intrusion (M = 1.49 vs. M = 1.07), secondary use (M = 1.95 vs. M = 1.38) and surveillance (M = 2.36 vs. M = 1.76). The differences were significant: intrusion $t(1444.5) = 5.72$, $p < 0.001$; secondary use $t(1452.5) = 6.08$, $p < 0.001$; and surveillance $t(1447.5) = 5.22$, $p < 0.001$. These results suggest that our participants did not simply focus on reducing the warning level (i.e., changing icon colors) and that the underlying privacy meanings of icons made a difference in users' decisions. Since we ruled out this confound, we excluded the non–privacy condition for subsequent analyses.

5.3 User Interactions with Privacy Interfaces

When users installed apps, they interacted with our interfaces adjusting permissions prior to installing each app 61% of the time. There are many ways participants interacted with our interfaces. We focused on the following aspects or types of interactions: time spent on the interface, clicks on privacy icons, clicks on interface features (e.g., component (6) in Figure 1 (b)), and permission adjustments. Overall, 34 users (14%) viewed the additional information about the privacy riskiness of each app and their privacy concerns. The privacy icon users clicked the most was surveillance (199 times, 46.3% of all instances where privacy icons were clicked), followed by secondary use (124 times, 28.8%) and intrusion (107 times, 24.8%). Although the additional information feature provided more information about the privacy warnings, this was only used 135 times (<1% of all app install instances). This feature was used most often in the privacy discrepancy condition where as it was used in 55 app install instances, followed by 41 in the privacy personal interface and 39 in the privacy rating interface.

All privacy interfaces in our study allowed participants to adjust fine–grained permissions by either disabling or enabling permissions the apps requested. Each user made decisions about 120 different permission requests. Of the 193 study participants (in the control, rating, personal, and discrepancy conditions), 37 chose not to disable permissions in any app situation. We examined the characteristics of permission adjustments in cases where users installed the apps (resulting in 16,777 fine-grained permission adjustment decisions). Overall, when participants installed apps, they enabled 58% (N = 9,756) of permissions. When users adjusted permissions, they most often rejected personal information such as Contacts (56.7%), Device ID & Call Information (55%), Photos/Media/Files (49%), and Location (41%).

Next, we looked deeper into several user behaviors with apps and permissions during our study, such as the number of apps installed, permissions installed, and permission adjustments. Table 1 shows the average values for these measures for participants in the four interface conditions, excluding the non–privacy interface only used for sanity check as described in the previous section. While we did round-robin assignment of participants to conditions, the number of participants in the privacy discrepancy condition was larger than other conditions, as Table 1 shows. This was mainly due to some participants not qualifying after our screening.

Table 1. User behaviors by interface condition. Each number represents the average for users in that condition. We compared each column (except users) as a dependent variable using a mixed-effect linear model. We only found significant differences among different conditions in terms of permissions adjusted (i.e., the number of checking or un-checking permissions).

	Users	Apps Installed	Permissions	
			Allowed	Adjusted
Control	44	14.8	3.54	53.36
Rating	48	15.46	3.03	76.06
Discrepancy	56	13.9	3.42	76.36
Personal	45	14.69	3.84	50.56

To evaluate the impact of privacy interfaces on participants' behaviors, we analyzed group differences in the number of apps participants installed, permissions adjusted, and permissions granted. For each comparison, we first built a null model: a mixed-effects logistic regression model with binary dependent variables (either to install or not to install apps/permissions) as well as users and apps as random effects (assuming individual users and apps have varying, idiosyncratic effects on the app/permission decisions). Next, we built an expanded model, adding privacy interface as a fixed effect. We then used a likelihood ratio test to compare the two models. If the test yields statistically significant results, this indicates significant differences in app/permission decisions among different interface conditions. We found significant differences on permissions adjusted ($\tilde{\chi}^2 = 12.91$, $p = 0.01$) but not on apps installed ($\tilde{\chi}^2 = 4.04$, $p = 0.4$) and permissions installed ($\tilde{\chi}^2 = 8.32$, $p = 0.139$). Participants in the privacy rating interface and the privacy discrepancy interface had significantly more permission adjustments than the control and privacy personal interfaces; there was no statistically significant difference between the rating interface and the discrepancy interface.

5.4 Aligning Concerns with Behaviors

Our main research hypothesis states – people who saw the privacy discrepancy interface better aligned their behavior (i.e., accepted or rejected permission requests for apps that they installed) with their privacy concerns than other interface conditions. To visualize the pattern in our data, we first plotted the relationship between privacy concern and the number of permissions users granted when they installed apps, as shown in Figure 6. We observed a negative relationship across the board, where as concern increases, the number of permissions granted decreases. This suggests users who were not concerned granted more permissions. Another important observation was that the lines of the privacy discrepancy condition (diamond-shaped in Figure 6) had the steepest slopes compared to that of other conditions. This suggests that as the privacy concern level increased, the privacy discrepancy condition was associated with the largest reduction of permissions granted.

We then analyzed the impact of each privacy interface on the ability to effectively align user behaviors (i.e., permissions granted) to user concerns using linear mixed models. For each condition, we analyzed the relationship between individual users' privacy concerns and privacy concerns related permissions (e.g., secondary use). If an interface facilitates the match between privacy behaviors and attitudes, then one would expect a negative effect of privacy concern on privacy behavior, i.e., as concern increases the number of permissions accepted decreases. This analysis required tests for four conditions (control, rating, personal, discrepancy) for each MUIPC construct (intrusion, secondary use, surveillance) - resulting in twelve tests. We had five interface conditions where the non-privacy interface was only used as a sanity check so we excluded it from this analysis. To account for the number of tests required, we adjusted the cut-off p–value by a Bonferroni correction to $p < 0.004$. A likelihood ratio test was conducted to compare two models: the null model included the number of privacy concern related

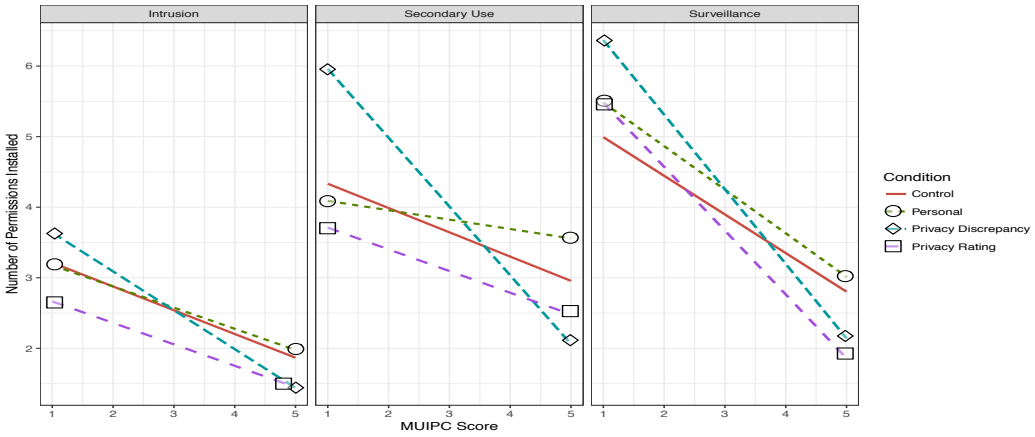

Fig. 6. A line chart showing the relationship between MUIPC concern scores and the number of related permissions granted by users in each experiment condition. The x-axis shows a user concern score while the y-axis shows the average number of permissions granted. The privacy discrepancy condition (diamond-shaped lines) had the most negative slopes.

permissions (e.g., secondary use) granted as the dependent variable and users as a random effect; the extended model added user privacy concerns as a fixed effect. Table 2 shows the results of the comparisons. As shown in Table 2, the expanded model was a significant improvement over the null model only in the discrepancy condition: intrusion (β = -0.48, S.E. = 0.19) at $\tilde{\chi}^2$ = 8.85, p = 0.002; secondary use (β = -0.83, S.E. = 0.17) at $\tilde{\chi}^2$ = 10.18, p = 0.001; and surveillance (β = -0.87, S.E. = 0.27) at $\tilde{\chi}^2$ = 8.69, p = 0.003. The β coefficients are negative, which means as privacy concern increases, the number of permissions granted decreases. These findings suggest that the discrepancy interface nudged participants' permission granting behaviors closer to their privacy concerns than did other interfaces. This empirical evidence supports our hypothesis that the privacy discrepancy interface allowed users to better align their privacy behaviors to their privacy concerns than other interface conditions.

Table 2. For each interface condition, we used linear mixed models to examine the relationship between individual users' privacy concerns (e.g., secondary use) and privacy concern related permissions granted. If an interface facilitates the match between privacy behavior and concerns, then one would expect a negative effect of privacy concern on privacy behavior, i.e., the higher the privacy concern, the lower the number of privacy concern related permissions accepted. We only observed such a significantly negative effect in the discrepancy interface condition, suggesting its value in reducing the discrepancy between privacy behaviors and concerns. * marks statistical significance (p <0.004 after Bonferroni correction).

	Intrusion				**Secondary Use**				**Surveillance**			
	β	S.E.	χ^2	p	β	S.E.	χ^2	p	β	S.E.	χ^2	p
Control	-0.34	0.12	2.65	0.04	-0.39	0.28	1.88	0.17	-0.38	0.17	2.62	0.04
Rating	-0.22	0.19	1.16	0.28	-0.19	0.3	0.39	0.53	-0.74	0.29	5.49	0.02
Discrepancy	-0.48	0.09	8.85	***0.002****	-0.83	0.17	10.18	***0.001****	-0.87	0.27	8.69	***0.003****
Personal	-0.33	0.18	3.11	0.07	-0.16	0.32	0.23	0.634	-0.67	0.36	3.09	0.078

5.5 Perceptions of Privacy Interfaces

We now report our participants' qualitative feedback from the exit survey on the privacy interfaces, particularly the privacy discrepancy interface. In addition to answering questions from the System Usability Scale (SUS), we asked participants to explain what each icon represented and whether the icons influenced their decisions as they considered which permissions to grant and which apps to install. The following subsections address the key themes that emerged from our thematic analysis of the questions in the exit survey (see Appendix C).

5.5.1 Participants' Feelings about the Icons. Most users felt positively about the privacy interfaces. In terms of the System Usability Score (SUS), we conducted pair-wise t-tests where we found no significant difference between any two conditions after adjusting the p value for multiple comparisons (p =.016). We asked users how they felt about the icons (what they liked and disliked), and our thematic analysis revealed several themes from users' answers. Below, we present several high–level themes emerging from the exit survey questions Q2 - Q4 (Appendix C).

Simple and Intuitive Design. Many users said they liked the privacy interfaces and noted the simplicity in design and the color warnings scheme was intuitive given their experience with traffic lights in their daily lives. These colors helped them understand circumstances under which they should be concerned. One user in the privacy discrepancy condition stated: *"I like how they are color coded, so you know when an app may not be that secure with your information. It makes it easy to tell if an app could end up using your information or the app itself for other purposes."* This user not only paid attention to the icon colors but also the underlying privacy implications of the icons. Users also noted that having the warnings prior to installing an app helps provide a succinct summary of the permission situation. One user in the privacy personal condition noted: *"The icons are a good way to flag app permission concerns without actually having to look at the app permissions. They do a good job of categorizing the main concerns."* Another user in the privacy discrepancy condition noted several of the features were helpful, stating: *"I liked that I could determine what selections contributed to the problem area the icon covered. I like that their colors changed. I liked the double click feature that let me see the underlying risk levels."* This user leveraged both the icon colors and the additional information that explained the underlying privacy risk.

Using Permission Adjustment. Several respondents noted the permission adjustment feature helped them feel more comfortable installing apps. Allowing users to adjust permissions increased the sense of control they had over their data. In relation to the permission adjustment feature, users also noted the dynamic adjustment helped them to understand the risk at time of installation. For example, one respondent in the discrepancy condition stated: *"I am not comfortable sharing certain information as described in the permissions. The icons help me gauge which permissions are influencing each risk level, and that helps me manage which permissions to accept or reject."* The discrepancy interface allowed this user to see the connections from permissions to privacy risk and to manage permissions to achieve her comfortable level.

Problems with Icon Representations. While many users noted the icons and the color scheme were intuitive, 58 (N= 37%) users suggested aspects of the icons can be improved. One aspect is the pictorial representations of the icons. Users noted that the secondary use icon was particularly confusing and they had difficulty inferring what the icon represented. In addition, some users felt they needed additional information from the icons and suggested we include additional descriptions in the interface. We actually did include more information about the permissions, icons, and how the warnings were derived, however, few users used these features. One user in the privacy rating condition noted: *"I don't like how ambiguous the icons can be. Without knowing why an app was given a particular rating, I can't really make an informed decision on whether or not I want to download it. I need more information, which I'm not getting from these icons."* Based on our analysis of user interaction data, most participants did not interact with the features providing the additional information they reported as missing. For example, Figure 1 (b) shows information that pops up when users click the intrusion icon. They can see the

construct definition, i.e., "Unwelcomed access to your information," the number of permissions associated with the icon (5), and the app riskiness (Medium) and their comfort with intrusion (Medium).

5.5.2 Influence on Decision Making. A major benefit of the privacy interfaces is the extent to which they influenced how users behaved. Most participants who saw the privacy icons (67%) indicated that these icons influenced their decision to install (exit survey questions Q6 and Q7) and accept permissions (questions Q8 and Q9). The privacy rating condition and discrepancy conditions had the highest percentages of participants who reported the icons influenced their ability to accept and reject apps (75% and 74% respectively), followed by the personal condition (49%). The same order also applied to participants' reporting the icons influenced their decisions to grant/reject permission requests (privacy rating 75%, privacy discrepancy 74%, and privacy personal 50%). Only 21 (38%) users in the control condition felt the interface influenced their decision to accept/reject permissions and install an app. When we asked how the interfaces influenced their decisions, users' responses fell into two major themes: risk communication, and exercising ownership over data.

Succinct Risk Communication. Communicating privacy risk was the main goal of the privacy interfaces and most users reported this to be the main factor that influenced their decisions. The privacy warnings provided summaries of risks informing users how to act. One user in the privacy rating condition mentioned: *"They told me how risky certain permissions were when installing an application. If the icon was red that meant that it's probably not a good idea to install."* In addition, several users mentioned the privacy icons made it easier to digest permissions. They found deciding about privacy risks in three icons was easier than scrolling through each permission. One user in the privacy discrepancy condition stated: *"The change of color in the icons informed me on the safety of the app and influenced my decision on outweighing the risks and benefits of installing the app."* For these participants, the privacy icons allowed them to explore the cost-benefit trade-off between installing an app and the potential privacy risks as their permission adjustments could change the colors of the icons.

Exercising Data Ownership. Some participants were more expressive in describing the specific ways the privacy icons helped them make decisions. Users wrote about managing their data with two specific mechanisms. First, they noted the icons helped them to exercise personal heuristics in managing their data. Several users spoke of avoiding red icons altogether. For instance, one user in the privacy discrepancy condition commented: *"They influenced my decision to install apps based on the color they were. I was hesitant to install an app when the icons were all red unless it was an app that I really wanted. Even then, I would un–check the options I did not want the app to have access to. I preferably wanted the icons to be green or yellow because I knew I was giving away less information then."* Others were not as rigid and noted cases where apps could justify the permission requests they would accept regarding the red warning icons. We also found some users who were particularly concerned about particular privacy threats. Most users reported denying permissions to reduce the risk of surveillance. Several users also noted how the interface helped them combat over-privileged apps since the permissions were linked to privacy constructs. For example, if surveillance–related permissions (e.g., Location) were requested by apps not required to monitor users (e.g., Marvel Comics) they were more cautious to grant the permission. One user in the personal condition wrote: *"Some of the apps seemed to need permissions that were represented by several of these icons. I would be really reluctant to download those because that seems too much trouble to have the app."*

5.5.3 Understanding How Icon Colors Were Determined. We wanted to understand the extent to which users who saw the privacy rating, privacy discrepancy, and privacy personal interfaces could articulate how the colors of the privacy icons were determined (exit survey question Q10). Many users wrote statements about how they interpreted the icon colors rather than how the icon colors were determined. One user in the personal condition wrote: *"I think green is a go ahead, I think yellow is to proceed with caution, i think red indicates a strong signal of not to allow install or the permission."* This is not untrue, however, this participant's response did not really explain how we derived the icon colors. In addition, several respondents wrote only about part of the "algorithm" to determine icon colors. For instance, several users in the privacy discrepancy condition gave partial answers

where they explained permissions were related to risks, but failed to mention the use of their responses to the MUIPC survey questions. We coded responses based on their degree of accuracy rather than the binary true and false responses. As a result, most participants' answers (N = 76) were partially accurate, 26 accurately described the approach, 36 said they did not know or supplied responses we could not decipher, and 11 provided inaccurate descriptions. We observed that most users who answered correctly were in the privacy rating condition (N = 12) compared to eight in the privacy personal condition and six in the privacy discrepancy condition. Several participants did not articulate how we determined icon colors in part because they did not click the privacy icons to see the detailed information.

While our analysis revealed that most respondents partially understood the algorithm, we take solace in the fact that participants understood the warnings conveying privacy risks.

6 DISCUSSION

Our goal was to design a personalized privacy notification approach juxtaposing users' general privacy attitudes towards technology types and the potential privacy riskiness of a particular instance of each type – particularly when users make decisions about whether and/or how to use the technology under consideration. In this paper, we focus on the domain of Android mobile apps. In particular, we designed a privacy discrepancy interface that aimed to emphasize the discrepancy between users' privacy attitudes towards mobile apps and the potential privacy riskiness of each app (because of their permission requests). The results of our study suggest the privacy discrepancy interface better aligned user behaviours (granting/rejecting app permissions) to user privacy attitudes towards mobile apps than providing no additional information (i.e., control), warnings derived only from researchers (i.e., privacy rating), and warnings derived only from users' own privacy attitudes (i.e., privacy personal). By bringing the elements of privacy discrepancies to the forefront, users were able to pay attention to the inconsistencies between their attitudes and specific apps/permissions altogether, which in turn motivated users to behave in a way that reduces such inconsistencies.

6.1 Increased Control over Privacy

In all conditions except the control condition, the privacy interfaces provided features giving users more knowledge and abilities to control their data during the app installation process. Allowing users to deny specific permissions at app install time is not supported by the most recent Android version (Android Oreo), but it does allow users to revoke specific permissions after an app is installed. Our data on users' interactions with the interfaces suggests that users were eager to be involved in permission management and they made adjustments in manipulating application permission requests to achieve a level of risk that they deemed acceptable. Placing the stimuli (i.e., permission requested/granted) and the outcome (i.e., risk level) contiguously in the interface allowed users to dynamically explore and update the risk profile for the app under consideration.

Participants in the privacy discrepancy and privacy rating conditions had higher average numbers of permission adjustments per user (76.06 and 76.36, respectively) than that of the control and privacy personal conditions (53.36 and 50.56, respectively). Since users in the control had no information for which to base their adjustments and users in the personal condition saw the same warning levels (i.e., colors of the same privacy icon) in all 20 app tasks, we suspect a lack of reference caused them to make fewer permission adjustments. Overall, these findings imply that users are likely to take control over their data in mobile apps if given the opportunity to do so.

An important aspect of the privacy interface design was the additional information we provided to define the MUIPC constructs and describe the rationale behind the warning levels. However, our data on user interactions with the interfaces revealed that only a minority of users (34, about 23% of all users who saw interfaces that provided such additional information) engaged with these features in a small number of app tasks (N = 135). We suspect most users were unaware of these features. However, these mechanisms can provide users some

insight into what some have labelled the "black box" of algorithms (of determining warning levels and thus icon colors). Displaying the rationale behind the warnings supports an increased call for algorithmic transparency. This design is also inline with the idea of scrutable personalization where designers should provide ways for users to scrutinize and understand personalized services or recommendations [22]. For example, sites like Facebook now include a "Why am I seeing this?" section for ads on the platform to help users understand and control how the ads they encounter are selected potentially based on information about them.

The exit survey responses helped us consider additional elements for designing a more educational interface for users. While several participants in our study noted the need for additional information, we did provide additional information albeit our participants seldom made use of these features. We suspect that the features providing additional privacy information were not conspicuous enough to users. A helpful addition is a tutorial overlayed on the interface allowing users to see and experience elements of the interface. Another idea for improvement is to add more descriptive text for the features to alert users to additional information. For example, rather than double–tapping an icon, placing an information symbol ⓘ next each privacy icon may help users know there are additional features or details. We can also enhance the text displayed to users, for example, adding descriptions such as "Why am I seeing this warning", which could provide more scrutability and lead to a more detailed explanation of such warnings.

6.2 Aligning Behaviours with Attitudes

Our main research question sought to explore which privacy notification approach could align users' privacy behaviors with their general privacy attitudes or concerns. We expected that as concern increases, the number of permissions granted decreases. While this negative relationship was present in all conditions, it was most salient in the privacy discrepancy condition. Our results suggest users in the privacy discrepancy condition granted or rejected permissions requests that better matched their privacy concerns than those in other conditions such as privacy risk and privacy personal. This also implies showing users warnings based on privacy risk determined by researchers or based on users' personal privacy concerns alone was not as effective as showing both, highlighting the value of the privacy discrepancy approach juxtaposing the two constituents of the discrepancy.

6.3 Addressing Privacy Discrepancies through Personalized Nudges

Our privacy discrepancy approach can be considered as a privacy nudge, which refers to the idea of designs that nudge rather than force users to make privacy decisions in certain directions [2]. Some designs nudge users towards a direction that third parties (e.g., researchers) deem appropriate (e.g., privacy nudges for Facebook posting [37]). However, a key limitation to this type of design is its reliance on third parties rather than users themselves judging what is appropriate or rational. While nudges are supposed to mitigate certain behavioral or cognitive biases people may have (e.g., status quo bias, meaning people tend to stay with the default) when making decisions [2], having external parties determining how users should behave can be troublesome. Why are third parties (e.g., researchers) always in a better position than people themselves in making such judgments? This is particularly challenging for privacy decisions, which many contextual factors can influence whether or not a decision is rational. To mitigate this methodological challenge of nudges, some of the more recent nudge designs focus on nudging users towards their own preferences [3]. Our privacy discrepancy approach followed a similar strategy as it was designed to nudge users towards privacy behaviors reflecting their own privacy attitudes or concerns. Our results suggest displaying discrepancy is promising approach to address the privacy paradox.

While we focus on Android app permissions, we believe this privacy discrepancy approach in general (i.e., juxtaposing one's own privacy attitudes/concerns and the potential privacy risk of decisions at hand) can be applied to other permission-based settings such as Facebook app permissions, and web browser plugin permissions.

This approach can also be adopted to other domains more broadly such as the Internet of Things. For instance, the discrepancy interface can show users' general privacy attitudes or concerns about smart home devices and the potential privacy risk of devices with a particular configurations (e.g., encryption on or off). The interface can allow users to explore the privacy space and adjust the device configuration to arrive at a privacy risk level they are comfortable with.

6.4 Limitations

As we explore a new approach of personalized privacy notifications, our work inevitably has many limitations.

First, we do not claim our results can be generalized to precisely represent Android users' behaviors in the real world. Since we could not modify the official Google Play Store, we simulated the Android app installations on web pages. We also asked our participants to scroll through twenty apps and make decisions to install or reject each app, which were essentially hypothetical scenarios for participants.

Despite these limitations in ecological validity and thus generalizability, we believe observing differences between interface conditions (even in a controlled setting) suggests the privacy discrepancy approach has the potential to more effectively impact user behaviors more than other approaches. We applied sanity checks to ensure our participants took each task seriously and triangulated data from different sources (e.g., behavioral data such as the number of permission adjustments and qualitative data from the exit survey) in our analysis to ensure the reliability of our results. For instance, the inclusion of the non–privacy interface showed users did not simply check/un-check permissions to change the icon colors. In addition, our quantitative data suggests participants did take these app installation tasks seriously and selectively chose to reject some apps and permissions but not others.

Second, while we either developed or followed a systematic way to operationalize certain concepts (how we measured individual users' general privacy attitudes towards mobile apps and privacy risk level of each app as well as how we determined the warning level and thus the icon color), these working schemes or definitions are not meant to be perfect nor irreplaceable to our privacy discrepancy approach. On the contrary, researchers can develop or adopt other schemes that they think better fit their application domains. For instance, while we systematically coded the privacy riskiness of apps and achieved reasonable inter-coder reliability, the coding scheme was based on our own interpretations of the permissions (as described by Google's official developer guide and/or analyzed by Privacy Grade's static code analyses). As such, much of the app rating was based on our subjective beliefs about what permissions constitute intrusion, secondary use, and surveillance. Since the task of relating permissions to specific privacy concerns has not been studied in the literature, this aspect of our work is novel, but exploratory, and necessary for the functionality of our interfaces. Future work can explore other schemes and use them in a similar manner within the privacy discrepancy approach. As another example, splitting the privacy levels in thirds and the mappings from privacy concern level and app riskiness to icon colors are also subjective. However, our interface designs are agnostic to how app riskiness is calculated or how the color mappings are determined. One could explore other coding and mapping schemes. Furthermore, we manually coded and analyzed the privacy ratings and discrepancies of the twenty apps tested in our study. Future work could explore the use of static and dynamic code analyses along with some crowdsourcing scheme (e.g., similar to Privacy Grade [25, 26]) to automate this privacy risk analysis.

Third, while our present implementations of the interfaces were designed for app install time, Android has since moved to a runtime permission request model where users will receive permission requests only when running apps need to access certain resources protected by the corresponding permissions. In addition, while our implementations only support pre-installation permission adjustments, the latest Android model only supports post-installation permission adjustments. Despite these differences, we believe that our design and evaluation of the privacy discrepancy approach is still novel and valuable because our approach transcends these specific

system settings. For instance, we argue that providing users useful privacy information at app install time can complement the runtime model because of the proactive nature of install-time (pre-installation) notifications. If users could have already decided at install time that they would not use an app because of its intrusive permission requests, why would they install the app, find out they do not like it and then (hopefully) uninstall it? Our point is not to discredit the runtime model, which could allow users to make permission decisions when apps need them and with the usage context. Instead, our view is that both install-time and runtime notifications could serve different use cases and complement each other. Furthermore, the privacy discrepancy interface could be easily adopted for runtime permission requests and post-installation permission adjustments, for instance, by showing the clickable privacy icons on the corresponding interface.

Lastly, while we deliberately avoided using the word "privacy" throughout the study, we asked all participants to answer the MUIPC survey before the app installation tasks. This could potentially prime them to think about privacy and thus influenced their subsequent behavior. However, this step was necessary to capture their privacy concerns and was integral to the provisioning of our privacy interfaces. Since every participant answered the MUIPC survey before the actual tasks, it is reasonable to assume the effect of priming would evenly distribute across different interface conditions and would cancel out when comparing different conditions.

7 CONCLUSION

Similar to human behaviors in other life domains, people's privacy behaviors may divert from their stated attitudes (i.e., the privacy paradox). These inconsistencies can be troublesome and problematic, for instance, engendering regrettable experiences or ramifications. To help people address this privacy paradox, we propose a novel approach of providing personalized privacy interfaces that juxtaposes users' general privacy attitudes towards certain technologies and the potential privacy riskiness of a particular instance of such technology – precisely when users make decisions about whether and/or how to use the technology. To explore the value of this approach, we chose the domain of mobile apps, designed a privacy discrepancy interface, and tested it along with other interface alternatives in an online simulation experiment. This discrepancy interface provided useful feedback to users, dynamically updating to show how changes in granting/rejecting permissions impact privacy risk, and how this privacy risk of currently granted permissions compares to users' general privacy comfort zones. The quantitative and qualitative results from our study suggest users who saw the privacy discrepancy interface made permission decisions better reflecting their privacy attitudes or concerns than other interfaces. In other words, these promising results indicate the discrepancy approach was more effective at nudging users to behave in line with their privacy attitudes. We advocate that this discrepancy approach can be applied more broadly to assist users in making privacy decisions in other application domains.

ACKNOWLEDGMENTS

We thank our participants for sharing their insights. We also thank Amandine Lemonnier, Eddie Huang, Saurabh Patel, Yaxing Yao, Huichuan Xia, and Jordan Hayes for their assistance as well as the anonymous reviewers for their thoughtful feedback. The work is supported by the National Science Foundation under Grant No.: 1464347.

REFERENCES

[1] Alessandro Acquisti. 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce (EC '04)*. ACM, New York, NY, USA, 21–29. https://doi.org/10.1145/988772.988777

[2] Alessandro Acquisti. 2009. Nudging Privacy: The Behavioral Economics of Personal Information. *IEEE Security and Privacy* 7, 6 (2009), 82–85.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[4] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (Jan. 2015), 509–514. https://doi.org/10.1126/science.aaa1465

[5] 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 (CHI '15)*. ACM, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

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

[7] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '15)*. ACM, New York, NY, USA, 63–74. https://doi.org/10.1145/2808117.2808119

[8] Douglas Bates, Martin Mächler, Ben Bolker, and Steve Walker. 2015. Fitting Linear Mixed-Effects Models Using lme4. *Journal of Statistical Software* 67, 1 (2015), 1–48. https://doi.org/10.18637/jss.v067.i01

[9] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. 2013. Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing. In *Information curators in an enterprise file-sharing service*. Springer Berlin Heidelberg, Berlin, Heidelberg, 74–91.

[10] Jacob Cohen. 1960. A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement* 20, 1 (April 1960), 37–46.

[11] L F Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J on Telecomm & High Tech L* (2012).

[12] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM transactions on computer-human interaction (TOCHI)* 13, 2 (June 2006), 135–178.

[13] RogÃČÂĭrio de Paula, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David F. Redmiles, Jie Ren, Jennifer A. Rode, and Roberto Silva Filho. 2005. In the eye of the beholder: A visualization-based approach to information system security. *International Journal of Human-Computer Studies* 63, 1 (2005), 5 – 24. https://doi.org/10.1016/j.ijhcs.2005.04.021 HCI research in privacy and security.

[14] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. *I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns*. ACM, New York, New York, USA.

[15] Adrienne Porter Felt, Kate Greenwood, and David Wagner. 2011. The Effectiveness of Application Permissions. In *Proceedings of the 2Nd USENIX Conference on Web Application Development (WebApps'11)*. USENIX Association, Berkeley, CA, USA, 7–7. http://dl.acm.org/citation.cfm?id=2002168.2002175

[16] Denzil Ferreira, Vassilis Kostakos, Alastair R. Beresford, Janne Lindqvist, and Anind K. Dey. 2015. Securacy: An Empirical Investigation of Android Applications' Network Usage, Privacy and Security. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '15)*. ACM, New York, NY, USA, Article 11, 11 pages. https://doi.org/10.1145/2766498.2766506

[17] Leon Festinger. 1957. *A theory of cognitive dissonance*. Stanford University Press.

[18] Christopher S Gates, Jing Chen, Ninghui Li, and Robert W Proctor. 2014. Effective Risk Communication for Android Apps. *Dependable and Secure Computing, IEEE Transactions on* 11, 3 (2014), 252–265.

[19] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *CHI '14*. ACM Press, New York, New York, USA, 2647–2656.

[20] Corey Brian Jackson. 2016. Privacy Discrepancy. https://www.youtube.com/watch?v=PcRngDsXVc4&t=121s

[21] Kathy A. Stewart. 2002. An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research* 13, 1 (March 2002), 36–49. https://doi.org/10.1287/isre.13.1.36.97

[22] Judy Kay. 2006. Scrutable Adaptation: Because We Can and Must. In *Adaptive Hypermedia and Adaptive Web-Based Systems*. Springer Berlin / Heidelberg, 11–19.

[23] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3393–3402.

[24] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2010. Teaching Johnny Not to Fall for Phish. *ACM Trans. Internet Technol.* 10, 2, Article 7 (June 2010), 31 pages. https://doi.org/10.1145/1754393.1754396

[25] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *UbiComp '12: Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM Request Permissions, New York, New York, USA, 501.

[26] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. 2014. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *Symposium on Usable Privacy and Security (SOUPS)*.

[27] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 27–41.

[28] Bin Liu, Jialiu Lin, and Norman Sadeh. 2014. Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?. In *Proceedings of the 23rd International Conference on World Wide Web (WWW '14)*. ACM, New York, NY, USA, 201–212. https://doi.org/10.1145/2566486.2568035
[29] Richard E Mayer and Richard B Anderson. 1992. The instructive animation: Helping students build connections between words and pictures in multimedia learning. *Journal of Educational Psychology* 84, 4 (Dec. 1992), 444–452.
[30] Alexios Mylonas, Dimitris Gritzalis, Bill Tsoumas, and Theodore Apostolopoulos. 2013. A Qualitative Metrics Vector for the Awareness of Smartphone Security Users. In *Trust, Privacy, and Security in Digital Business*. Springer Berlin Heidelberg, Berlin, Heidelberg, 173–184.
[31] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. 2013. Delegate the Smartphone User? Security Awareness in Smartphone Platforms. *Comput. Secur.* 34 (May 2013), 47–66. https://doi.org/10.1016/j.cose.2012.11.004
[32] 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
[33] Daniel J Solove. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (July 2006), 477–560.
[34] 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 (EC '01)*. ACM, New York, NY, USA, 38–47. https://doi.org/10.1145/501158.501163
[35] V F Taylor and I Martinovic. 2016. Quantifying Permission-Creep in the Google Play Store. *arXiv* (2016). arXiv:related:Y-kixjgTwKMJ
[36] Lynn Tsai, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. 2017. Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 145–162.
[37] 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 (CHI '14)*. ACM, New York, NY, USA, 2367–2376. https://doi.org/10.1145/2556288.2557413
[38] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I regretted the minute I pressed share": a qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11)*. ACM, New York, NY, USA, 10:1–10:16. https://doi.org/10.1145/2078827.2078841
[39] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. In *2017 IEEE Symposium on Security and Privacy (SP*. IEEE, 1077–1093.
[40] Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John M Carroll. 2012. Measuring mobile users' concerns for information privacy. In *Thirty Third International Conference on Information Systems*.

A MOBILE USERS INFORMATION PRIVACY CONCERN (MUIPC)

Perceived surveillance

1. I believe that the location of my mobile device is monitored at least part of the time.
2. I am concerned that mobile apps are collecting too much information about me.
3. I am concerned that mobile apps may monitor my activities on my mobile device.

Perceived intrusion

1. I feel that as a result of my using mobile apps, others know about me more than I am comfortable with.
2. 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.
3. I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.

Secondary use of personal information

1. I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.
2. When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.
3. I am concerned that mobile apps may share my personal information with other entities without getting my

authorization.

B NON-PRIVACY QUESTIONS

1. I have serious difficulty hearing.
2. I have serious difficulty seeing, even when wearing glasses.
3. I have serious difficulty using a mouse, clicking on small links, or operating dynamic elements on a webpage effectively.

C EXIT INTERVIEW QUESTIONS

1. Enter your SID.
2. How do you feel about the icons?
3. Is there anything you like about the icons? If so, please describe what you like about the icons.
4. Is there anything you don't like about the icons? If so, please describe what you don't like about the icons.
5. Please explain what you think each icon represents?
6. Do the icons influence your decision to install/not install an app? How so?
7. How do the icons influence your decision to install/not install an app?
8. Do the icons influence your decision to accept/reject a permission?
9. How do the icons influence your decision to accept/reject a permission?
10. Please describe how we determined the color of each icon. What information or process do you think we use?
11. Rate how much you agree with the following statements regarding the app install interface you were shown (See item D for System Usability Scale questions).

D SYSTEM USABILITY SCALE QUESTIONS

1. I think that I would like to use this system frequently.
2. found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

Received August 2017; revised March 2018; accepted April 2018