Information Leakage through Mobile Motion Sensors: User Awareness and Concerns

Kirsten Crager, Anindya Maiti, Murtuza Jadliwala, and Jibo He
Wichita State University, USA
Email: krcrager@shockers.wichita.edu, a.maiti@ieee.org, murtuza.jadliwala@wichita.edu, jibo.he@wichita.edu

***Abstract*—Smart phones and wearable devices have replaced personal computers and desktops as the primary platform for accessing online applications and services. However, these mobile devices bring forth new and additional forms of security and privacy risks, which were non-existent in traditional personal computers. For instance, several recent research efforts have shown that motion sensors such as accelerometer and gyroscope on-board these mobile and wearable devices can be maliciously used to infer private information from users' keystrokes (e.g., PINs and passwords). The problem is that, unlike traditional security and privacy risks that are typically associated with personal computers, most users may not be aware of these novel risks associated with mobile devices. An adversary may use this lack of user-awareness to target specific user-demographics for successfully carrying out such attacks. There has been some progress in the direction of protection mechanisms against such attacks, however, without user-awareness these protection mechanisms are unlikely to be used effectively (if at all). In order to further understand these issues, we conduct a structured and comprehensive user-study involving users from diverse demographic backgrounds to investigate user-awareness and perceptions related to mobile motion sensor based privacy risks, and how these vary across different demographics. By means of our study, we also gain insight on users' expectations from defense mechanisms that can protect against such attacks. Results of our study can be used to increase awareness (about such risks) among the less-aware user demographies, and in designing effective and usable protection mechanisms as per user-expectations.**

I. Introduction

It is estimated that there are over two billion smartphone users world-wide [1]. As wearable technology is also maturing and becoming affordable, it is forecasted that approximately 322 million wearable devices (such as wrist wearables, smart glasses, etc.) will be sold by the end of 2017 [2]. These mobile devices have seemingly replaced traditional computing systems as a means for accessing common online applications and services. Pew Research Center reported that 89% of smartphone owners access the Internet from their phones for various tasks such as emailing, browsing, social networking and gaming [3]. Email, for instance, is most often read on smartphones than on a desktop or personal computer [4], [5]. As a consequence, users end up entering a variety of personal information, for example, PINs, passwords and credit card numbers, on their mobile and wearable devices. Similarly, these devices are equipped with state-of-the-art sensors capable of generating or capturing sensitive user information, such as, GPS that can precisely record users' current or past locations or cameras that can capture high-resolution images of the user or his/her surroundings. Given this plethora of highly sensitive and personal information available from users' mobile and wearable devices, they are increasingly becoming targets of sophisticated information-stealing attacks.

A majority of these threats targeted towards mobile devices originate as malware that is either embedded inside mobile apps available on popular app stores or is downloaded by users on their device through a malicious email attachment or MMS message. The primary goal of these malware is to gain elevated privileges (root exploits), enable remote code executions by installing backdoors (remote access tools or RATs), stealing personal and financial information (banking trojans and spywares) or threatening release of personal information for a ransom (ransomware). According to recent Intel Security reports [6], [7], with the exception of root exploits, most mobile threats (including, spyware and ransomware) are steadily growing and malicious apps are finding a way through the initial screening process of popular app stores. A majority of these malware operate by taking advantage of vulnerabilities in the mobile operating systems (e.g., stagefright libraries in Android), by tricking users into providing personal information (social engineering) or by gaining elevated access permissions from unsuspecting users. However, recent advancements in mobile anti-malware software can prevent most of the above attacks by observing applications for malicious activities, such as requesting elevated privileges or attempts to access restricted information [8], [9].

A new form of threat that is being observed in smartphone and wearable device malware is the inference of a target user's private data by means of on-device sensors as an information side-channel. An example of such a threat is the advertising software developer kit (SDK) called SilverPush that uses the target user's smartphone microphone to listen for near-ultrasonic sounds placed in TV, radio and Web advertisements, which could be eventually used to infer the user's preferences. In this

EuroUSEC '17, 29 April 2017, Paris, France

http://dx.doi.org/10.14722/eurousec.2017.23013

work, however, our focus is on side-channel threats that are accomplished by means of a mobile device's motion sensors. Our motivation in further studying such private information inference threats based on motion sensors is rooted in two main observations. First, malware containing such threats are difficult to detect, both by the users and the system, because access to motion sensors is generally not regulated by system or user-level access controls. In other words, all installed apps by-default have complete access to on-device motion sensors[1] and malware that misuse this motion data (say, by archiving it and covertly communicating it back to the adversary for carrying out privacy-threatening inferences) can easily avoid detection. Second, there is strong evidence (Section II) that point to the feasibility of successfully exploiting zero-permission sensors on modern smartphones and wearable devices to infer users' private information. These inference attacks can be enabled either by a malware that is unintentionally downloaded by the target user on his/her device [10], [11] or by means of an adversarial device in close physical proximity to the target user [12], [13].

Despite this, currently very little is known regarding how end-users perceive such kind of threats due to zero permission motion sensors. A chief concern is our current lack of understanding of how informed mobile and wearable device users are about the various motion sensor related threats (compared to other forms of security/privacy threats), attack modalities, and types of private data at risk. Despite significant technical advances in devising feasible attack strategies, currently there is a big knowledge gap in terms of how concerned users are visá-vis such attacks, which demographic of users are most vulnerable to such attacks and what type of actions users envision as a response to protect themselves against such attacks. It is also critical to understand whether users' usage of their mobile/wearable devices is significantly influenced or altered after learning about the existence of such privacy threats [14], [15].

There has been some progress made on the front of protection mechanisms against such attacks, however much of the proposed techniques appear to be designed in an ad hoc fashion, without really considering users' perspective, feedback or current understanding of the threat. For instance, some proposed defense mechanisms [11], [16] leverage on applications' motion sensor access patterns to detect and notify users of a potential leakage or inference threat. However, these notifications may not always be intuitive and could confuse users [17]. Moreover, an increasing number of notifications could also lead to negative effects, such as frustration and habituation [18]. This brings forth the issue of designing simple and responsive protection mechanisms and interfaces, which will not confuse or overwhelm the users [19]. Given the novelty and indirect nature of these threats, this is a non-trivial issue that has not received much attention. Our overarching goal is to arrive at an improved understanding of user concerns regarding private data inference attacks due to mobile/wearable device motion sensors in a way that would allow for an informed and effective design of future permission interfaces, access control tools and notification modalities to protect against such attacks.

In line with the above goal, we make the following specific contributions by conducting a comprehensive user-study involving a diverse group of participants:

- We first analyze the level of awareness and user perception on four well-researched motion sensor-based inference threats (Location tracking [20], [21], keystroke inference [22], [10], [23], [24], [11], [25], acoustic eavesdropping [26], [27] and device-fingerprinting [28], [29]). We also break down our analysis based on different demographics.
- We attempt to gain an in-depth perspective on user preferences for security notification modalities against potential risks and/or privacy breaches on their mobile or wearable devices. Defense mechanisms against motion sensor-based attacks [30], [16] can benefit from such an analysis by designing and delivering meaningful notifications to users.

II. Related Work

Private data inference threats that are enabled by mobile device motion sensors can be categorized based on the type of private information targeted by these threats. For example, one class of threats, known as location tracking, focuses on tracking users' location and movements by using inertial navigation models [20], [21]. Keystroke inference using mobile device motion side-channels is another highly researched threat, primarily because of the criticality associated with the information typed by the user while accessing the Internet [22], [10], [23], [24], [11], [25]. Acoustic eavesdropping using motion sensors has also received significant attention in the literature [26], [27]. Device fingerprinting attacks that enable an adversary to identify and track a user's device over time have also been proposed [28], [29]. Recently, researchers have successfully demonstrated more complex attacks using motion sensors, such as, inferring a target user's handwriting [13], factory floor secrets [31] and objects printed on nearby 3D printers [32].

On the front of protection mechanisms, it has been observed that most popular mobile operating systems do not provide any form of system or user-level access control support (say, by means of access control lists or ACLs) for on-board motion sensors primarily due to usability concerns and its impact on the quality-of-service (QoS) of applications. This leaves the mobile platform open to attacks that take advantage of this uncontrolled and unrestricted access to motion sensors. Even with an ACL in place (as was added in the most recent version of Android [33]), their effectiveness can be limited by user awareness of such a feature and motivations behind it. Recently, there have been a few additional proposals to protect users from motion sensor based inference attacks which can be broadly classified into *Design-time* and *Run-time* protection mechanisms. Design-time mechanisms [34], [35], [36] modify the static target system or interface (that is being protected) in

[1] such sensors are also referred to as zero-permission sensors

such a way that the prior or assumed knowledge of an adversary about the system or interface is no longer valid, thus rendering any side channel attack using that knowledge ineffective. One example of such an approach is to randomize the mobile keypad layout in order to prevent keystroke inference attacks [36], [35]. Runtime protection mechanisms [30], [16] propose dynamic motion sensor controls based on contextual information captured by on-device sensors. For instance, Maiti et al. [30] proposed context-aware access control on motion data, while Xu et al. [16] proposed to perturb on-device motion data by adding noise. However, none of the above proposals consider the end-users threat perception and response, concerns, requirements or feedback before designing their mechanisms and interfaces.

To maximize the outreach and impact of future/planned protection mechanisms, it is important to first assess users' perception and awareness regarding potential security/privacy threats, and then design protection mechanisms as per their understanding and expectations of these threats [37]. Similarly, several other research efforts in the literature have attempted to study user awareness of security concerns and countermeasures. For example, Felt et al. [38] conducted a survey involving 3000 participants to rank the level of user concern regarding a range of smartphone-related privacy risks and access permissions in order to guide the future selection and design of smartphone warnings. Lee et al. [39] conduct a similar large-scale survey to assess user concern regarding privacy risks in wearable devices. Another roadblock towards designing a successful protection or notification mechanism can be misaligned user perceptions regarding the design. Felt et al.'s survey on effectiveness of security indicators [19] and Harbach et al.'s survey on risk perceptions of smartphone locking behavior [40] are two instances demonstrating that design of widely used protection mechanisms can be further improved when user perception is thoroughly studied. However, it should be noted that none of these research efforts study user concerns pertaining to privacy risks associated with motion sensors, a less explicit and oblivious threat. Recently, Mehrnehad et al. [41] studied users' perception of the risk associated with numeric PIN leakage by means of a variety of mobile phone sensors. Although their survey included a scenario of PIN leakage by means of motion sensors, it was fairly constrained and restricted in terms of participant size and diversity, it was not focused on motion sensor-based privacy risks, it did not study other privacy risks (except, PIN leakage) and it did not capture users' preferences in terms of protection and notification mechanisms. In contrast, our study involves a much larger and diverse set of participants, is focused on studying a variety of side-channel privacy risks due to motion sensors onboard both smartphones and wearable devices, and also captures users' feedback on preferable protection and notification mechanisms.

III. Research Goals

The three main goals of our study include: (i) capturing the level of user-awareness regarding motion sensor-based privacy leakages ("AQ"), (ii) analyzing user-perceptions regarding such leakages ("PQ"), and (iii) understanding users' expectations vis-á-vis protection mechanisms and the associated notification interfaces and modalities ("EQ"). In this direction, we draft the following seven questions that comprehensively capture the above goals, and which we will quantitatively and qualitatively analyze with the help of our user study.

AQ1. How *aware* are people of the existing four types of mobile device motion sensor-based private data inference attacks?
AQ2. Which *demographic groups* are the *most vulnerable* to mobile device motion sensor-based private data inference attacks?
PQ3. What are *users' perceptions* of the four types of mobile device motion sensor-based private data inference attacks?
PQ4. Does *previous experience of a security attack affect users' perceptions* on an attack through use of mobile device motion sensors?
PQ5. Would *usage change after users have been educated* on mobile device motion sensor-based private data inference attacks?
PQ6. After briefly being educated on the mobile device motion sensor-based private data inference attacks, will individuals *express concern* that they will happen to them?
EQ7. What is the *preferred modality* that users expect to be notified with when a potential mobile device motion sensor-based private data inference attack is detected?
EQ8. What *other expectations* do users have towards protective mechanisms on how they should work in terms of presentation and frequency?

Awareness Question 1 (AQ1) addresses the user-awareness goal by measuring the extent (in terms of the percentage of individuals who have knowledge and the level of understanding) about this new type of privacy risk. *Awareness Question 2 (AQ2)* will be used to identify at-risk populations by investigating personal demographics (e.g., age, gender, education level, etc.), as well as, mobile technology-related experience (e.g., frequency of smartphone use, number of apps downloaded and purpose of Internet use).

In the direction of user-perception goals, *Perception Question 3 (PQ3)* attempts to gauge the overall feelings that users would exhibit in case their personal information was compromised (obviously, without their authorization) by each type of motion sensor-based attack. *Perception Question 4 (PQ4)* attempts to draw a comparison between the perceptions (related to motion sensor-based attacks) of individuals who have experienced a past security-related threat or attack and those who have not. Our aim here is to understand if past security-related experience significantly impacts future perceptions regarding this relatively newer and obscure form of security/privacy threat. *Perception Question 5 (PQ5)* attempts to study if users' mobile device usage behavior is significantly impacted after they have been educated on

motion sensor related threats. *Perception Question 6 (PQ6)* focuses on studying users' level of concern regarding this new type of attack. A higher level of concern may be indicative of users' willingness and urgency to protect their information (against such attacks), further stressing the importance of timely and appropriate user-education (about these attacks) and arriving at usable protection mechanisms.

Expectation Questions 7 and *8 (EQ7, EQ8)* focuses on further understanding users' expectations in terms of their interface with protection mechanisms, specifically, the notification information, modality (e.g. visual, auditory, tactile, or a combination), frequency and other properties of interest to the user. As the efficacy of any protection mechanism that involves users depends on how the mechanism interfaces with the users, answers to these questions will aid in the design of more effective and usable protection mechanisms (and interfaces) against such novel types of attacks.

IV. Research Methodology

In this section, we outline details of our user-study, including, participant recruitment procedures, survey details and the quantitative and qualitative metrics used to analyze our research goals.

A. Participant Recruitment

For our experiments, we recruited a diverse set of participants from a wide range of demographics by three different means, which enabled us to acquire a comprehensive and rich set of user-data for our analysis. We first recruited 156 participants through the Amazon Mechanical Turk, where each participant was compensated \$0.50 for a complete survey submission. Previous studies [42] have shown that financial gain is not the only stimulus for 'workers' on Mechanical Turk, and results obtained from such studies are generally of high-quality despite a low remuneration amount. However, the remuneration amount does impact the participation rate [42]. We additionally recruited 262 student participants from Wichita State University's psychology SONA research pool, where participating students received compensation in the form of two research credits as a course requirement. In addition to this, we reached out to individuals outside of the college campus by means of paper flyers and email/social media advertisements and were able to recruit an additional 141 participants. These participants were compensated by entering them into a drawing for a chance to win one of three \$20 gift cards. These three efforts resulted in a total participant pool size of 559. Our survey was administered by means of the Qualtrics platform [43], where participants were able to access and complete the survey online (i.e., remotely). In order to ensure meaningful, quality data and to block against potential "bot" submissions (especially, in the Mechanical Turk pool), we incorporated three attention checks throughout the survey. Similarly, we also took due care to prevent duplicate submissions. Our study procedures and survey instruments were approved by the Institutional Review Board (IRB) at Wichita State University.

B. Survey Instrument

Our survey instrument consists of 45 items (44 questions and 1 informational video). A complete copy of the instrument can be found in Appendix A. Participants required on an average 27.73 minutes ($\sigma = 203.02, median = 14.09$) to complete the survey which was also organized in a way to prevent any participant bias for questions appearing later. The survey questions (grouped into categories) appeared in the following order:

- **16 Technology Demographic Items:** Participants were first asked about their Internet habits (*"What do you typically use the Internet for?"*), length of smartphone and wearable device ownership (*"How long (in years) have you owned a smartphone?"*), and app download history (*"Approximately how many apps have you downloaded for use onto your smartphone?"* and *"Of the apps that you have downloaded, what purpose do you use them for?"*).
- **6 Privacy and Security Demographic Items:** Next, the survey focused on eliciting the types of information that participants considered private (*"Which types of personal or private information would you be concerned with unauthorized parties receiving?"*) and their past experience with security/privacy threats during technology usage (*"Have you personally experienced a security issue while using any form of computing or mobile technology?"*, *"What type of security/privacy issue did you experience?"*, *"Did any of the events above have a significant impact on your personal or professional life?"*).
- **1 Educational Video to Inform Users about Motion Sensor-based Privacy Threats:** Before proceeding with questions related to motion sensor-based privacy threats, participants are educated on what these threats are and how they are accomplished. We created a brief 83 seconds video describing each of the four types of attacks: *location tracking*, *keystroke monitoring*, *acoustic eavesdropping*, and *device fingerprinting*. To ensure that the entire video clip was watched, participants were provided a code at the end which they must enter correctly in order to continue. Survey responses with missing or incorrect codes were removed and excluded from analysis.
- **8 Items on Perceptions and Awareness of Security Risks:** Then, the survey focused on questions related to user-awareness of the motion sensor-based threats outlined in the video (*"Were you aware of any of these risks?"*) and participants' perceptions related to these threats (*"Please rate how upset you would be if motion sensor data allowed unauthorized parties to access your personal information."* and *"Please rate how upset you would be if the following recipients obtained some of your private information."*). Responses to these questions were measured on a 5-point rating or Likert scale. Additionally, the survey included an open-ended question to enable participants to subjectively explain their ratings above (*"What would you do if an app collected private information about you?"*).

- **5 Items on User Expectations on Security Notifications:** After that, participants were asked questions related to their preference in terms of notification modalities, e.g. visual, auditory, tactile, or a combination. In addition to that, the survey included several related open-ended questions on how the participants expected notifications to physically appear (based on the modality that they previously chose), at what frequency they preferred the notification to occur (e.g. every time no matter the risk, only when a specific type of risk may occur, never, etc.), and any other aspect(s) of the notification that might make it annoying for them.
- **9 Basic Demographic Items:** The survey concluded with demographic related questions, for example, age, gender and highest level of education.

C. Data Analysis

1) Qualitative Thematic Analysis: Thematic analysis is way to organize rich data sets in an operational way by identifying patterns, or themes, within the data set [44]. To identify themes, we inductively captured frequently appearing responses in relation to the specific research questions (PQ3 and EQ8). Meaning, the themes were data-driven, not pre-existing prior to sifting through the data. The lead researcher went through every response to come up with common themes in which two additional researchers independently coded each response to. Each question entry often included more than one code. PQ3 included responses from a short answer question to further elaborate why they did or did not feel upset in reaction to an application gathering private information about them without permission. Analysis for EQ8 required coding responses over three different topics: (1) expectations on how the notification would present itself (e.g. visual flashing, auditory beep, tactile vibration, etc.), (2) how frequent the notification should occur and why, and (3) what aspects might make a notification annoying. After coding was completed, we tested the inter-rater reliability to measure consistency in the coding of the two researchers.

2) Statistical Analysis: Statistical tests chosen were non-parametric measures of significance. The Chi-Square test for independence was used to test whether two categorical variables significantly differ from expected, showing whether or not the two variables are associated, or independent of each other. A Friedman Test was also conducted as a non-parametric alternative to a one-way ANOVA with repeated measures to test for differences between groups with ordinal dependent variables. The Wilcoxon Signed Rank tests were executed as a non-parametric alternative to a paired samples t-test as a post-hoc test for Friedman Test by using a Bonferroni adjusted alpha value to control for Type I error [45]. Because it is non-parametric it allows for abnormally distributed data. It assumes that the dependent variable is measured ordinally (e.g. the 5-point ranking scale) and that the independent variable is the comparison of two categorical data (e.g. pair-wise comparison between two of the four types of motion sensor attacks). All statistical analyses were conducted using IBM SPSS Statistics Version 21.

V. Results

In this section, we analyze survey responses to answer the research questions enlisted in Section III.

A. Participant Demographics

A total of 559 participants signed up for the survey. However, while screening out submissions that were incomplete and/or did not meet our minimal one year smartphone ownership requirement, we eliminated responses from 75 of those participants. Following results include responses from all the remaining 484 participants, unless specified otherwise. All survey-takers were United States residents, and their age ranged between 18 to 73 years ($\mu = 27.23, \sigma = 10.89$) with 63.6% being females. Detailed demographic background of participants can be found in Appendix B.

B. Awareness

AQ1. How *aware* are people of the existing four types of mobile device motion sensor-based private data inference attacks?

We observed that participants' risk awareness is highly dependent on the type of motion sensor attack. A Chi-Square test (Table I) indicated significantly higher awareness for location tracking, whereas they reported being generally unaware for acoustic eavesdropping, keystroke monitoring, and device fingerprinting. In addition to the above awareness rating in the five-point scale (Figure 1), we also evaluated participants' relative awareness across the four types of motion sensor attacks. The Friedman Test revealed that there was a statistically significant difference between participants' awareness of the four types of motion sensor attacks (Table II). Post-hoc testing using the Wilcoxon Signed Rank test, with a Bonferroni adjusted alpha value, was conducted to test the significance of Friedman Test and control for Type I error by comparing each of the four motion sensor attacks with each other for a total of

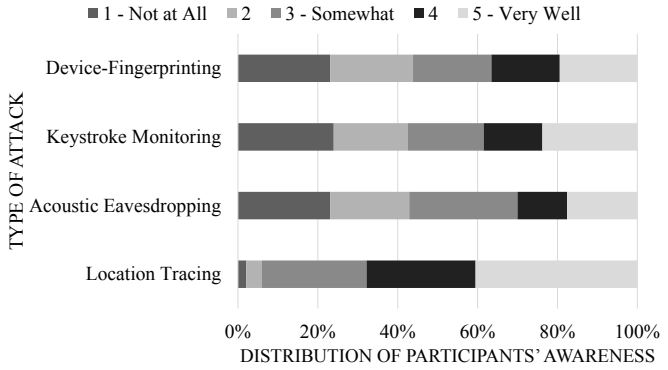

Fig. 1. Percent of awareness ratings (on a 5-point scale from 1-Not at all to 5- Yes, very well) on four classes of motions sensor attacks.

TABLE I. CHI-SQUARE TEST RESULTS FOR SELECTED RESEARCH QUESTIONS.

Chi-Square Test Values				
	LT	AE	KM	DF
AQ1 (df=4, N=484)	264.25**	29.91**	14.82*	NS
AQ2: Gender (df=1, N=484)	NS	12.70**	49.91**	10.65**
AQ2: Age (df=3, N=477)	NS	24.427**	NS	NS
AQ2: Education (df=8, N=484)	NS	NS	NS	NS
AQ2: Income (d=4, N=465)	24.56**	NS	NS	NS
PQ3: Attack Type (df=4,N=484)	367.98**	597.24**	496.89**	614.41**
PQ4 (df=1, N=484)	107.41**	208.93**	137.53**	253.10**

*p<.05, **p<.001, NS= 'not significant'

six pair-wise comparisons (Table III). Results revealed that participants' awareness for location tracking was significantly higher than for acoustic eavesdropping, keystroke monitoring, and device fingerprinting attacks. Awareness for keystroke monitoring was also statistically lower than acoustic eavesdropping. The awareness levels did not differ between device fingerprinting and acoustic eavesdropping, or device fingerprinting and keystroke monitoring. These analyses imply that participants are only significantly aware of the risks of location tracking, and are generally unaware of keystroke monitoring, acoustic eavesdropping, and device fingerprinting risks due to motion sensors. However, it is likely that participants may have confused location tracking using motion sensors with tracking by accessing on-device GPS which is much easier to access control.

AQ2. Which *demographic groups* are the *most vulnerable* to mobile device motion sensor-based private data inference attacks?

We defined groups that would be at-risk populations by identifying those who reported that they were unaware of the four motion sensor attacks. For the purpose of the Chi-Square tests in this section, the awareness rankings were re-categorized into two: aware and unaware.

Gender: A Chi-Square test for independence was conducted to compare gender against participants' awareness for each of the four motion sensor attacks. Results indicated that gender is significantly associated with the awareness level of acoustic eavesdropping, keystroke monitoring, and device fingerprinting attacks (Table I). Location tracking, however, was found to *not* have a significant association with gender. This may be explained by the overall higher awareness of location tracking. In addition, our results indicate that females were less aware, and thus more at-risk, compared to males for all four attack types.

Age: In the survey, we asked for participants' exact age, so when we tested age against awareness for the motion sensor attacks we re-categorized them into age groups: 18-25, 26-40, 41-55, and 56-75 years. We did find a significant association between age and keystroke monitoring attacks (Table I). However, location tracking, acoustic eavesdropping, and device fingerprinting were all found to not be statistically associated with age. Younger individuals (18-25 yrs), followed closely by the older age category, were found to be the most at-risk, due to their overall level of unawareness. It should be noted that some excluded cases were present here, as we allowed participants to not disclose their age.

Education Level: A Chi-Square test for independence was conducted to compare education level against participants' awareness for each of the four motion sensor attacks. Results indicated no significant association between education level and awareness for location tracking, acoustic eavesdropping, and device fingerprinting attacks. Keystroke monitoring was just over the significance level (Table I).

Income Level: We then compared participants' income level against their awareness for each of the four motion sensor attacks. Only keystroke monitoring was found to be statistically dependent on income level. Effect of income on awareness of location tracking, acoustic eavesdropping, and device fingerprinting attacks were all found to be insignificant. It should be noted again that some invalid cases were present here, as we allowed participants to not disclose their income.

TABLE II. FRIEDMAN TEST RESULTS FOR SELECTED RESEARCH QUESTIONS.

Friedman Test	
AQ1 (df=3, N=484)	334.95**
PQ3: Attack Type (df=3, N=484)	NS
PQ3: Recipient (df=4, N=484)	1277.75**
EQ7 (df=3, N=484)	147.79**

*p<.05, **p<.001, NS= 'not significant'

TABLE III. WILCOXON SIGNED RANK TEST RESULTS FOR RESEARCH QUESTION AQ1.

AQ1: Wilcoxon Signed Rank Test				
	LT	AE	KM	DF
LT	-	Z = 14.73*	Z = 12.82**	Z = 13.44**
AE	Z = 14.73*	-	Z = 2.28*	NS
KM	Z = 12.82**	Z = 2.28*	-	NS
DF	Z = 13.44**	NS	NS	-

*p<.05, **p<.001, NS= 'not significant'

C. Perception

PQ3. What are *users' perceptions* of the four types of mobile device motion sensor-based private data inference attacks?

Overall, 86.4% users rated being "upset" or "very upset" if an application collected private information without prior authorization (Figure 2). These perceptions

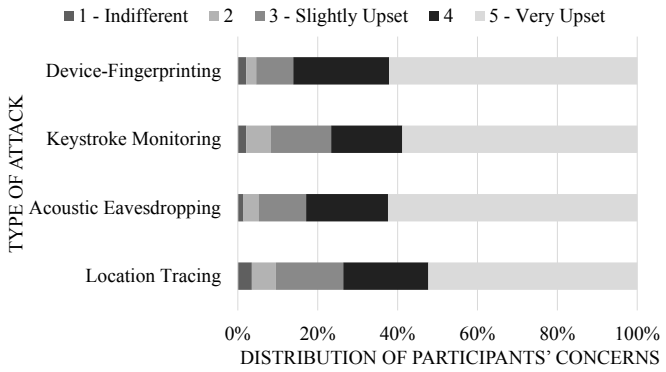

Fig. 2. Percent of user concern ratings (on a 5-point scale from 1-Indifferent to 5-Very Upset) on four classes of motions sensor attacks.

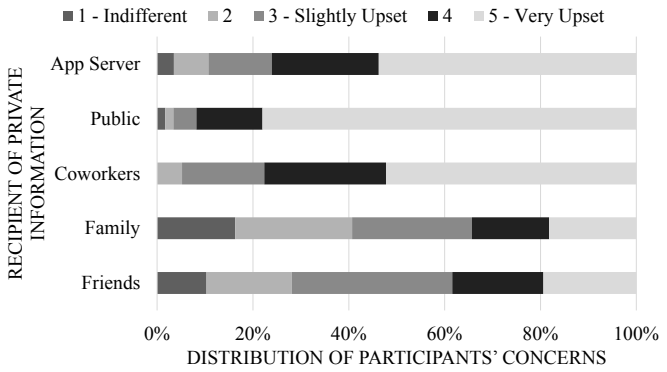

Fig. 3. Percent of user concern ratings (on a 5-point scale) based on the recipient of private information.

of being upset are found to be statistically significant. A Chi-Square test showed that participants' upset rankings are significantly different from expected for the four attack types (Table I), which was also supported by a significant Friedman Test (Table II). Further, the Friedman Test indicated that there was a statistically significant difference amongst the four types of motion sensor attacks. The Wilcoxon Signed Rank post-hoc test revealed that all six pair-wise comparisons were statistically significant except for device fingerprinting and acoustic eavesdropping pair (Table IV). Participants reported that they would be more upset to location tracking compared to acoustic eavesdropping, keystroke monitoring, and device fingerprinting. Keystroke monitoring ratings were significantly higher compared to device fingerprinting, while acoustic eavesdropping ratings were higher than keystroke monitoring.

TABLE IV. WILCOXON SIGNED RANK TEST RESULTS FOR RESEARCH QUESTION PQ3 - ATTACKS.

PQ3: Wilcoxon Signed Rank Test - Attacks				
	LT	AC	KM	DF
LT	-	Z = 5.21**	Z = 2.24*	Z = 5.90**
AC	Z = 5.21**	-	Z = 2.94*	NS
KM	Z = 2.24*	Z = 2.94*	-	Z = 3.90**
DF	Z = 5.90**	NS	Z = 3.90**	-
*p<.05, **p<.001, NS= 'not significant'				

Participants also significantly differed in their ratings in terms of the five possible recipients of their private information (Figure 3). A Chi-Square test showed that participants' upset rankings to each of the five recipients is significantly different from expected for friends, family, co-workers, the public, and an app server (Table I). Further, the Friedman Test indicated that there was a statistically significant difference amongst the five different recipients (Table II). The Wilcoxon Signed Rank post-hoc test revealed that all ten pair-wise comparisons were statistically significant except for the app's server and co-workers pair (Table V). Participants reported that they would be more upset if family, co-workers, the public, or the app's server received their private information compared to friends. Additionally, they reported that they would be more upset if their co-workers, the public, and the app's server received their private information compared to their family. There were also statistically significant differences between the public compared to co-workers and the app's server.

To delve deeper as to why users would be upset to the various motion sensor attacks, we then coded the open-ended portion of this question to ten major themes (Table VI). Some major themes that explained why users would be upset included the fact that they felt it was an invasion of privacy (36%), the application should ask the user upfront to receive particular information (42%), and that if the app didn't follow those guidelines users considered it to be very dishonest (19%). There were, however, some participants that reported reasons why they wouldn't be upset by accepting the fate of potential security attacks due to our highly technological world (4%) and their own possible user error (1%). Inter-rater reliability for the two independent raters was found to be 94.57%, $\kappa = 0.64$.

PQ4. Does *previous experience of a security attack affect users' perceptions* on an attack through use of mobile device motion sensors?

Most users have not personally experienced a security attack (62%) compared to those who have (38%) and only 11.6% have been significantly impacted by the event. We compared participants' perception rankings to their personal experience (or lack thereof) with a security attack in the past. We re-grouped the five point responses into two new categories: not upset (coded as "1") and upset (coded as "2"), and then conducted a Chi-Square test. Results showed that participants' perceptions were dependent upon their personal experience (Table I). Interestingly, those who indicated not having prior experience with a security attack/event display poorer perceptions (upset ratings closer to being upset) compared to those who have not.

PQ5. Would *usage change after users have been educated* on mobile device motion sensor-based private data inference attacks?

A majority of users (83.9%) reported that they would discontinue use of an application in order to protect

TABLE V. WILCOXON SIGNED RANK TEST RESULTS FOR RESEARCH QUESTION PQ3 - RECIPIENT.

PQ3: Wilcoxon Signed Rank Test					
	App Server	Public	co-workers	Family	Friends
App Server	-	Z = 9.74**	NS	Z = 17.42**	Z = 17.65**
Public	Z = 9.74**	-	Z = 9.82**	Z = 15.82**	Z = 16.07**
co-workers	NS	Z = 9.82**	-	Z = 18.47**	Z = 19.05**
Family	Z = 17.42**	Z = 15.82**	Z = 18.47**	-	Z = 5.93**
Friends	Z = 17.65**	Z = 16.07**	Z = 19.05**	Z = 5.93**	-
*p<.05, **p<.001, NS= 'not significant'					

TABLE VI. WHY USERS WOULD OR WOULD NOT BE UPSET IF THEIR INFORMATION WAS STOLEN WITHOUT AUTHORIZATION.

Code	Percent of Responses (PoR)
Upset	
Should ask permission	42%
Invasion of privacy	36%
Dishonest	19%
Abusive	7%
Feeling of taken advantage of	6%
Illegal	6%
Could be put in danger	4%
Not Upset	
Cost for living in a digital world	4%
For app purposes	2%
User error	1%

their private information. Most of the participants also install several applications on their smart devices ($\mu = 24.06, \sigma = 13.48$, within the interdecile range), suggesting that discontinuing particular app(s) that posed a security risk would not be that detrimental to them and their ability to use their smart device. Instead, they would more than likely delete that application and try a new one with similar functionality, but is safer.

PQ6. After briefly being educated on the mobile device motion sensor-based private data inference attacks, will individuals *express concern* that they will happen to them?

All users (100%) reported that they were concerned with motion sensor attacks occurring, which intuitively makes sense because their perceptions to such attacks were largely being upset. Amongst their open-ended responses as to why they would be upset to a motion sensor attack included reasons, some participants (4%) felt that they could be put in physical, reputational, or other forms of danger and/or taken advantage of (6%) if their private information got into the wrong hands. Many (42%) responded that they felt that they should be asked permission prior to their information being gathered, because if they were not asked they now lose their sense of control over that information. With a potential consequence of a security attack as serious as being put in danger and lack of control over their private information, it makes sense why participants expressed concern. Although this is a high level of concern, it should be noted that this concern may decay over time.

D. Expectations on Security Notifications

EQ7. What is the *preferred modality* that users expect to be notified with when a potential mobile device motion sensor-based private data inference attack is detected?

A majority of responses ranked a combination of modalities (55%) first as their preference for security notifications (Figure 4). Most preferred rankings then followed visual (26%), auditory (10%), and then tactile (9%). Consistently, the solely tactile modality method was most popularly rated as least preferable at 39%. The Friedman Test indicated that there was a statistically significant difference amongst the four modalities for a security notification (Table II). However, when participants were asked to subjectively describe their expectation on how the notifications should look like, responses were somewhat different. Coded breakdown of subjectively described user preferences on different notification methods is detailed in Table VII. The Wilcoxon Signed Rank post-hoc test revealed that all six pair-wise comparisons were statistically significant except between the combination and visual modality types (Table VIII), suggesting that users prefer some sort of visual component in combination with another modality. The other comparisons, however, were statistically different, in which visual was more preferred than audio and tactile, and tactile was the least preferred. As many might not always have their smartphones in-hand, it would make sense why a tactile vibration was not ranked higher.

EQ8. What *other expectations* do users have towards protective mechanisms on how they should work in terms of presentation and frequency?

The foremost expectation from users for security notification appearance is that it is multi-modal, particularly for the combination of auditory and visual modalities. Users had a wide range of expectations from being extremely "obnoxious" and "salient" to "subtle." The

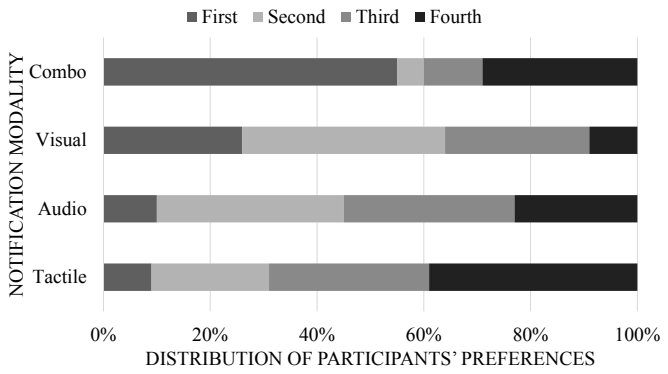

Fig. 4. Percent of user preference rankings for different notification modalities.

TABLE VII. CODED BREAKDOWN OF SUBJECTIVELY DESCRIBED USER PREFERENCES ON NOTIFICATION METHODS.

Code	PoR
Visual	
Full screen pop-up	32%
Tool bar banner	24%
Includes full details and instructions on what to do	18%
Flashing LED light	14%
Text message or email	9%
Use of emergency color scheme (e.g. red, orange)	9%
Requires acknowledgment before disappearing	7%
Similar to Amber alert warnings	6%
Authentic, not "phishy" looking	3%
Auditory	
Subtle	25%
Obnoxious	9%
Similar to Amber alert warnings	5%
Miscellaneous	
Combination of modalities	43%
Option to personalize	4%
Immediately occurs	4%

purpose of security notifications, according to users, is to not just warn them about a potential attack, but to also comprehensively instruct them what the specific issue is and how to react accordingly. For the particularly less "tech-savvy" or high-risk individuals, this is especially important. Inter-rater reliability for the two independent raters was 94.69%, $\kappa = 0.64$.

In terms of frequency, participants' preferences were quite divided. A majority (51%) preferred that they received a security notification every time there was a risk, regardless of the type of risk or the information gathered. The next most highly preferred frequency (43%) was for only when a specific attack may occur. Only a few (3.3%) preferred to receive notification after information had already been gathered, while (2.1%) preferred to receive no notifications but be able to actively check their risk at-will, and 0.4% preferred to never receive any notifications at all. Table IX and X shows participants' reasoning behind their preferred frequency to receive a security notification. Inter-rater reliability for the two independent raters was found to be 93.24%, $\kappa = 0.59$.

Despite the advantages to security notifications, aspects of the design can be seen as annoying to the user, thus detrimental to the purpose of the notification. If notifications occurred excessively, 42% of participants reported that it would make the notification annoying (Table XII in Appendix C). If the notification occurred too frequently to risks that were not viewed as a high threat, then users would consider it a false alarm, which 20% of users reported as being annoying. Inter-rater reliability for the two independent raters was 96.73%, $\kappa = 0.76$.

TABLE VIII. WILCOXON SIGNED RANK TEST RESULTS FOR RESEARCH QUESTION EQ7.

EQ7: Wilcoxon Signed Rank Test				
	Combo	Visual	Audio	Tactile
Combo	-	NS	Z = 5.73**	Z = 9.03**
Visual	NS	-	Z = 7.02**	Z = 10.70**
Audio	Z = 5.73**	Z = 7.02**	-	Z = 4.44**
Tactile	Z = 9.03**	Z = 10.70**	Z = 4.44**	-
*p<.05, **p<.001, NS= 'not significant'				

TABLE IX. USER PREFERENCES ON NOTIFICATION FREQUENCY (CLOSE-ENDED).

Notification Frequency	PoR
Every time - no matter the type of risk or information compromised	51%
Only when a specific type of risk may occur	43.20%
Only after information is gathered	3.30%
Receive no notifications, but be able to actively go check your risk at-will	2.10%
Never	0.40%

TABLE X. USER PREFERENCES ON NOTIFICATION FREQUENCY (OPEN-ENDED).

Code	PoR
Every Time	
Better safe than sorry	40%
Behavior modification	9%
Want to take immediate action	7%
Vital data on device, prevent damage	5%
Want to decide which risks to ignore	5%
At Specific Times	
Only in urgency	35%
May habituate to too many false alarms	5%

VI. DISCUSSIONS AND CONCLUSION

A. Summary

In this paper, we conducted a comprehensive user-study involving users from diverse demographic backgrounds to investigate user-awareness and perceptions related to mobile motion sensor based privacy risks, and their expectations from defense mechanisms that can protect against such threats. Results from our study have shown that users, for the most part, were unaware that this new type of motion-sensor based threat to their privacy existed. Out of the four, participants only reported being aware of location tracking. When asked for their reactions to the attacks after watching the video, users expressed genuine concern and would be very upset if these type of privacy attacks happened against them. One participant expressed concern stating, "Any information that is related to a person is his own. To take information [from] that person without asking is like identity theft, even when it was meant to be harmless [for the purposes of the app itself]." Not only would they be upset that the attack occurred, but they also expressed concern for who the possible recipient would be to that private information. Participants were found to be most upset if the public, app servers, and co-workers received their private information compared to friends and family. In their open-ended responses as to why they would be upset, participants reported that they should have been asked for permission to gather their information and they felt that it was an invasion of privacy. Interestingly, few participants said that they would not be upset because they dignified security attacks as part of the cost of living in a digital world.

We defined at-risk populations to be unaware of motion sensor based privacy threats. Our results indicate

that gender, specifically females, plays a role for being at risk for all motion sensor attacks (except for location tracking). Age was also a determining factor for being at-risk. Individuals aged 18 to 25 years, were most unaware, thus at-risk, for keystroke monitoring. Older individuals aged 56 to 75 years were very close in awareness levels compared to the youngest group. Income level also played a factor into overall awareness, indicating that individuals making less than $30,000 are more at-risk for keystroke monitoring attacks. A majority of participants (62%) had not personally experienced a security attack, although some (11.6%) have been significantly impacted by one in the past. We found that personal experience with a security attack did influence their perceptions on the motion sensor attacks suggesting that individuals without previous experience may be more sensitive and/or upset to such attacks, in general. Most users reported that they would be willing to discontinue their use of a particular application or device to secure their information. Furthermore, all participants expressed concern that a motion sensor attack could happen to them. Despite the high number, the educational video could be initially frightening to participants explaining why they all reported concern. This high proportion, however, could possibly decay with time.

A security expert's view might not always align with everyday users' needs, so it is crucial to get personalized feedback on how users expect to be notified. This is primarily why the items in regards to security notifications were mostly open-ended to prevent restrictions on their expectations. Users expect to receive some sort of notification when their information is at risk. Participants generally preferred that notifications are presented in visual form or a combination of two or more modalities. An audio-visual combination was the most frequently preferred combination while the tactile modality was least preferred. Common themes that participants reported include notifications to either appear as a full screen pop-up or as a banner consisting of the full details of the security risk and instructions on what to do in response. Preferences for the frequency of security notifications are fairly divided. A majority of the participants (51%) preferred to receive a notification every time there is a security risk no matter the type of information gathered because they would prefer to be "safe rather than sorry" and to be more proactive in protecting their private information. Other users (43.2%) preferred to only receive notifications when a specific type of risk occurs to prevent habituating to too many false alarms for less serious attacks.

Regardless of how important security notifications can be in protecting a person's private information, they can be seen as annoying. Users reported some aspects of notifications that they would find unappealing in terms of frequency (such as occurring excessively and repetitively for the same security risk), and in terms of appearance (such as being too loud, interrupts daily life or use of the device, and is uninformative). One of the participants supported this view by responding, "I wouldn't want to become oversaturated and desensitized to frequent warnings, so I would like them to trigger only after a credible threat is identified." Other participants, on the other hand, took the stance that notifications would not be annoying, regardless of how frequent it occurs or how it physically appears, because it is important that they be able to respond to the threat in a timely manner.

B. Limitations

We acknowledge that a weakness of this survey is asking users' explicit knowledge of or level of concern for motion sensor attacks. To gain true insight of their awareness, it would have been beneficial to ask them questions that brought about their knowledge and level of concern implicitly, in order to prevent over-exaggeration in their self-reports. Also, we only asked participants once if they were concerned with a motion sensor attack occurring to them, which was presented after they watched the educational video. It would have been preferable to ask them at the beginning of the survey prior to learning more about motion sensor attacks as well as a later time after they have learned about the attacks and completed the initial survey to better understand their level of concern for the security of their private information. Although input from users regarding their preferences on security notifications is important, additional testing of these protection mechanisms and interfaces may be required to evaluate their effectiveness in protecting against such attacks.

C. Recommendations and Future Directions

Users' large lack of awareness highlights the importance to create educational programs for less tech-savvy users in order to keep them abreast with the latest security/privacy vulnerabilities. Some of the classical means of security and privacy attacks have been well addressed and publicized to the user population, but newer techniques such as motion sensor side-channel based attacks have not been. To address the lack of knowledge on such attacks, we must stress the importance of how debilitating security attacks can be to users by properly educating them. One way that Suknot et al. [46] proposed is by gamifying the educational experience to teach users to be more security conscious. In reference to the design of security notifications, one user emphasized the ability to personalize and suggested, "[The design should be] optional per device. I would like to check a box to select the options [for what modality to appear]." Our study also brings attention to the importance of designing security mechanisms for these relatively unknown threats by keeping users' preferences and expectations in mind. Users will typically avoid using technology if security systems become burdensome and inconvenient, which is why it is important to first gain better insight on what the users want or expect. If security interfaces do not match these expectations (e.g., notifications occur too frequently), then users will eventually ignore them and risk a security attack [47].

Acknowledgment

This research has been supported by the US National Science Foundation (NSF) award 1523960.

REFERENCES

[1] Statista, "Number of Smartphone Users Worldwide from 2014 to 2020," https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, [Online; accessed 20-February-2017].

[2] Gartner, "Forecast: Wearable Electronic Devices, Worldwide, 2016," http://www.gartner.com/newsroom/id/3198018, [Online; accessed 20-February-2017].

[3] P. R. Center, "6 Facts About Americans and their Smartphones," http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/, [Online; accessed 20-February-2017].

[4] E. Analytics, "6 Facts About Americans and their Smartphones," https://litmus.com/email-analytics, [Online; accessed 20-February-2017].

[5] Adestra, "Top 10 Email Clients," http://www.adestra.com/resources/top-10-email-clients/, [Online; accessed 20-February-2017].

[6] McAfee, "Mobile Threat Report. What's on the Horizon for 2016," https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf, [Online; accessed 27-February-2017].

[7] ——, "Trojans, Ghosts, and More Mean Bumps Ahead for Mobile and Connected Things," https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2017.pdf, [Online; accessed 27-February-2017].

[8] V. Rastogi, Y. Chen, and X. Jiang, "Catch me if you can: Evaluating android anti-malware against transformation attacks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 99–108, 2014.

[9] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012, pp. 95–109.

[10] Z. Xu, K. Bai, and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2012, pp. 113–124.

[11] A. Maiti, M. Jadliwala, J. He, and I. Bilogrevic, "(smart) watch your taps: side-channel keystroke inference attacks using smartwatches," in *Proceedings of the 2015 ACM International Symposium on Wearable Computers*. ACM, 2015, pp. 27–30.

[12] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp)iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11, 2011, pp. 551–562.

[13] T. Yu, H. Jin, and K. Nahrstedt, "Writinghacker: Audio based eavesdropping of handwriting via mobile devices," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '16, 2016, pp. 463–473.

[14] D. Gefen, "E-commerce: the role of familiarity and trust," *Omega*, vol. 28, no. 6, pp. 725–737, 2000.

[15] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *International journal of electronic commerce*, vol. 7, no. 3, pp. 101–134, 2003.

[16] Z. Xu and S. Zhu, "Semadroid: A privacy-aware sensor management framework for smartphones," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. ACM, 2015, pp. 61–72.

[17] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, "Users' conceptions of web security: a comparative study," in *CHI'02 extended abstracts on Human factors in computing systems*. ACM, 2002, pp. 746–747.

[18] R. Böhme and J. Grossklags, "The security cost of cheap user interaction," in *Proceedings of the 2011 New Security Paradigms Workshop*, ser. NSPW '11, 2011, pp. 67–82.

[19] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking connection security indicators," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO*, 2016, pp. 1–14.

[20] J. Han, E. Owusu, L. T. Nguyen, A. Perrig, and J. Zhang, "Accomplice: Location inference using accelerometers on smartphones," in *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on*. IEEE, 2012, pp. 1–9.

[21] S. Narain, T. D. Vo-Huu, K. Block, and G. Noubir, "Inferring user routes and locations using zero-permission mobile sensors," in *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016, pp. 397–413.

[22] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "Accessory: password inference using accelerometers on smartphones," in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*. ACM, 2012, p. 9.

[23] H. Wang, T. T.-T. Lai, and R. Roy Choudhury, "Mole: Motion leaks through smartwatch sensors," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015, pp. 155–166.

[24] C. Wang, X. Guo, Y. Wang, Y. Chen, and B. Liu, "Friend or foe?: Your wearable devices reveal your personal pin," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 2016, pp. 189–200.

[25] L. Cai and H. Chen, "Touchlogger: Inferring keystrokes on touch screen from smartphone motion." *HotSec*, vol. 11, pp. 9–9, 2011.

[26] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing speech from gyroscope signals." in *USENIX Security*, 2014, pp. 1053–1067.

[27] N. Roy and R. Roy Choudhury, "Listening through a vibration motor," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2016, pp. 57–69.

[28] A. Das, N. Borisov, and M. Caesar, "Tracking mobile web users through motion sensors: Attacks and defenses," in *Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS)*, 2016.

[29] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "Accelprint: Imperfections of accelerometers make smartphones trackable." in *NDSS*, 2014.

[30] A. Maiti, O. Armbruster, M. Jadliwala, and J. He, "Smartwatch-based keystroke inference attacks and context-aware protection mechanisms," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 2016, pp. 795–806.

[31] A. Hojjati, A. Adhikari, K. Struckmann, E. Chou, T. N. Tho Nguyen, K. Madan, M. S. Winslett, C. A. Gunter, and W. P. King, "Leave your phone at the door: Side channels that reveal factory floor secrets," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 883–894.

[32] C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, and W. Xu, "My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3d printers," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 895–907.

[33] Google, "Android 7.0 nougat," [Online; accessed 27-February-2017].

[34] A. Maiti, M. Jadliwala, and C. Weber, "Preventing shoulder surfing using randomized augmented reality keyboards," in *IEEE PerCom Workshop on Security, Privacy and Trust in the Internet of Things (SPT-IoT)*. IEEE, 2017.

[35] A. Maiti, O. Crager, M. Jadliwala, and J. He, "Randompad: Usability of randomized mobile keypads for defeating inference attacks," in *Proceedings of the IEEE EuroS&P Workshop on Innovations in Mobile Privacy & Security (IMPS)*. IEEE, 2017.

[36] Software House, "Scramble Keypad SP-100," www.swhouse.com/products.

[37] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research*, vol. 20, no. 1, pp. 79–98, 2009.

[38] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns," in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ser. SPSM '12, 2012, pp. 33–44.

[39] L. Lee, J. Lee, S. Egelman, and D. Wagner, "Information disclosure concerns in the age of wearable computing," in *Usable Security (USEC)*. ISOC, 2016.

[40] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "Itsa hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *Symposium on usable privacy and security (SOUPS)*, 2014, pp. 213–230.

[41] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing pins via mobile sensors: Actual risk versus user perception," in *EuroUSEC*, 2016.

[42] M. Buhrmester, T. Kwang, and S. D. Gosling, "Amazon's mechanical turk a new source of inexpensive, yet high-quality, data?" *Perspectives on psychological science*, vol. 6, no. 1, pp. 3–5, 2011.

[43] J. Snow and M. Mann, "Qualtrics survey software: handbook for research professionals," *Qualtrics Labs, Inc*, 2013.

[44] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[45] J. Pallant, *SPSS survival manual*. McGraw-Hill Education (UK), 2013.

[46] A. Suknot, T. Chavez, N. Rackley, and P. G. Kelley, "Immaculacy: a game of privacy," in *Proceedings of the first ACM SIGCHI annual symposium on Computer-human interaction in play*. ACM, 2014, pp. 383–386.

[47] S. Breznitz, *Cry wolf: The psychology of false alarms*. Psychology Press, 2013.

APPENDIX A - SURVEY QUESTIONNAIRE

Demographics - Technology

1) How long (in months or years) have you been using the Internet?

2) How frequently do you access the web from home?

Daily	Weekly	Monthly	Never

3) How frequently do you access the web from work?

Daily	Weekly	Monthly	Never

4) How frequently do you access the web from school?

Daily	Weekly	Monthly	Never

5) How frequently do you access the web from public places?

Daily	Weekly	Monthly	Never

6) What do you typically use the Internet for? Check all that apply.

E-mail	Social media	Research	Education
Shopping	Entertainment	Navigation	Banking
Paying bills	Other (Specify)		

7) What is your primary computing platform?

Macintosh	Windows	Unix
Don't know	Other (Specify)	

8) Do you own a smartphone?

Yes	No

9) Approximately how long have you owned a smartphone? Please specify in either months or years.

10) What operating system does your smartphone device have?

iOS	Android	Windows

11) Do you own any wearable technology? Select all that apply.

Smartwatch	Fitness tracker	Clothing	Jewelry	None

12) Please list all wearable devices that you currently or previously owned. If you do not own, please type "N/A".

13) How long (in months or years) have you owned and used a wearable device? If you do not own, please type "N/A".

14) How often do you use your wearable devices?

Daily	Weekly	Monthly	Less than monthly

15) Approximately how many apps have you downloaded for use onto your smartphone?

16) Of the apps that you have downloaded, what purpose do you use them for? Select all that apply.

Social media	Work-related	Banking
News	Sports	Music
Gaming	E-mail/Communication	Event planning
Photo editing	Other (Specify)	

Demographics - Privacy & Security

17) Which types of personal or private information would you be concerned with unauthorized parties receiving? Select all that apply.

Photo	Demographic information	Passwords
Video	Financial information	Medical information
Audio		

18) Have you personally experienced a privacy or security issue while using any form of computing or mobile technology?

Yes	No

19) If yes, what type of security/privacy issue did you experience (or are experiencing)?

Computer or mobile was infected with a virus or some malicious software
Email, banking, social networking, or other personal account password was stolen and misused
Debit/credit card number, bank account number, or some other personal information was stolen and misused
Was tricked into buying or participating in a service which turned out to be a scam
Personal or private information was posted on the Internet on social network (e.g. Facebook) or online forums without your authorization or approval
Other (Specify)
None

20) Did the events above have a significant impact on your personal or professional life?

Yes	No

21) Have you heard an anecdotal story from someone else of a security issue occurring that had a significant impact on their life?

Yes	No

22) Rank the types of information (1 - most concerning, 10 - least concerning) if an unauthorized party received information about you from your mobile or wearable devices. Use your mouse to drag and drop them in your preferred order.

Photos	⇕
Videos	⇕
Audio recordings	⇕
Financial information	⇕
Medical information	⇕
Passwords	⇕
Social security number	⇕
Date of birth	⇕
Phone number	⇕
Debit / credit card number	⇕

Security

23) Please watch the video (83 seconds) below before responding to the following questions.

https://youtu.be/quBu8s3jYMQ

24) Enter the displayed code:: *[Random code displayed at the end of above video, to ensure entire video was viewed.]*

25) Were you aware of any of these risks?

	1 Not at all	2	3 Somewhat	4	5 Very well
Location tracing					
Acoustic eavesdropping					
Keystroke monitoring					
Device-fingerprinting					

26) Please rate how upset you would be if motion sensor data allowed unauthorized parties to access your personal information.

	1 Indifferent	2	3 Slightly upset	4	5 Very upset
Location tracing					
Acoustic eavesdropping					
Keystroke monitoring					
Device-fingerprinting					

27) Please rate how upset you would be if the following recipients obtained some of your private information.

	1 Indifferent	2	3 Slightly upset	4	5 Very upset
Friends					
Family					
Co-workers					
App servers					
Public					

28) How would you feel if an app gathered information about you without asking?

	1 Indifferent	2	3 Slightly upset	4	5 Very upset
Please rate					

29) Why would you feel this way? (Refer to your rating to the previous question.)

30) What would you do if an app collected private information about you? Select all that apply.

Switch to a new device	Turn off sensor
Discontinue use of device	Not sure
Deny permission to particular sensors	Nothing
Other (Specify)	Uninstall app

31) If an application that you use frequently (e.g. social media or email apps) posed a risk on your privacy, would you discontinue your usage?

Yes	No

32) Please select the first and last bubbles. *[Question to deter bots.]*

33) Given the above risks, are concerned of these attacks happening to you?

Yes	No

Expectations on Notifications

34) How would you like to be notified when you are at risk for a privacy attack? Please rank 1 (Most preferred) to 4 (Least preferred).

Audio (e.g. beep)	⇕
Visual (e.g. flashing LED light, pop-up window)	⇕
Tactile (e.g. vibration)	⇕
A combination of the above	⇕

35) Based on your answer above, please elaborate on how you would expect the notification to look like. Be as detailed as possible.

36) How frequently would you like to be notified of a potential privacy risk/breach?

Every time no matter the type of risk or information gathered
Only when a specific type of risk may occur
Only after information is gathered
Never
Receive no notifications, but be able to actively go check your risk at will

37) Why would you prefer to receive notifications at this frequency? (Refer to the question above.)

38) What would make the notification annoying?

Demographic - Personal

39) What is your age?

40) What is your gender?

Female	Male

41) What is the highest level of education you have completed?

Some high school	High school or GED
Trade, technical, or vocational training	Some college
Associate's degree	Bachelor's degree
Master's degree	Doctoral degree
Professional degree (MD, JD, etc.)	

42) How would you describe yourself?

Black or African American	Caucasian
Asian or Pacific Islander	Hispanic or Latino
Middle Eastern or Arab American	Other
Native American or American Indian	Don't wish to disclose

43) What is your marital status?

Single, never married	Separated
Married or domestic partnership	Divorced
Don't wish to disclose	Widowed

44) How much do you work?

Full-time	Part-time	Unemployed	Retired

45) What is your annual income before taxes?

< $10,000	$10,000-$19,999	$20,000-$29,999
$30,000-$39,999	$40,000-$49,999	$50,000-$59,999
$60,000-$69,999	$70,000-$79,999	$80,000-$89,999
$90,000-$99,999	$100,000-$149,999	> $150,000
Don't wish to disclose		

46) Describe where you live.

Urban	Suburban	Rural

47) Including yourself, how many people live within your household?

1	2	3	4	5	6+

APPENDIX B - PARTICIPANT DEMOGRAPHIC DETAILS

TABLE XI. PARTICIPANT DEMOGRAPHICS

	N (Total = 484)	Percent
Gender		
Female	308	63.60%
Male	176	36.40%
Race/Ethnicity		
Caucasian	322	66.50%
Asian or Pacific Islander	45	9.30%
Hispanic or Latino	36	7.40%
Black or African American	28	5.80%
Middle Eastern	8	1.70%
Native American	7	1.40%
Multi-racial	33	6.90%
Did not wish to disclose	5	1.00%
Educational Level		
High school, GED, or less	40	8.30%
Trade, technical, or vocational	9	1.90%
Some college	236	48.80%
Associate's or Bachelor's degree	162	33.40%
Graduate or professional degree	37	7.60%
Income		
Less than $19,999	84	17.40%
$20,000 - $39,999	88	18.20%
$40,000 - $99,000	85	17.60%
$100,000 - $149,000	7	1.40%
$150,000 or more	4	0.80%
Did not wish to disclose	56	11.60%
Work Status		
Part-time	207	42.80%
Full-time	183	37.80%
Unemployed	87	18.00%
Retired	7	1.40%
Marital Status		
Single	337	69.60%
Married	120	24.80%
Divorced	15	3.10%
Other or did not wish to disclose	12	2.50%
Household Size		
1	100	20.70%
2	132	27.30%
3	116	24.00%
4	83	17.10%
5+	51	10.50%
Residential Area		
Rural	67	13.80%
Suburban	217	44.80%
Urban	200	41.30%

APPENDIX C - ADDITIONAL USER PREFERENCES ON NOTIFICATIONS

TABLE XII. ASPECTS OF NOTIFICATIONS THAT CAN BE ANNOYING.

Code	PoR
Frequency	
Excessive	42%
False alarms	20%
Repetitive	11%
Inability to turn notification off	11%
Appearance	
Loud	18%
Uninformative	4%
Interrupts everyday life	4%
Blocks user from using app	2%
Phishy language, looks like a scam	1%
Too delayed	1%