Risks of Mobile Ambient Sensors and User Awareness, Concerns, and Preferences

MARYAM MEHRNEZHAD*, Royal Holloway, University of London, Egham, UK
CHRISTODOULA MAKAROUNA, Newcastle University, Newcastle upon Tyne, UK
DANTÉ GRAY, Newcastle University, Newcastle upon Tyne, UK

Abstract: Ambient sensors are being integrated within modern technologies such as mobile, smart buildings, and smart medical devices. Despite the real risks of such sensors, it is hard for users to understand and control such sensor readings since these sensors are freely accessible to mobile, website, and IoT developers without any user permission and notification. Ambient sensors have not been studied for their risks, especially from the user's point of view. We run an online user study (N=197) and evaluate user awareness, concerns, and preferences for mobile ambient sensors when accessed via apps and websites. Our findings show that users would like to have control over such sensors in a usable way and their protection actions and preferences are consistent across the two platforms (apps and websites). These findings help the sector to develop the next generation of sensor protection mechanisms more effectively.

Additional Key Words and Phrases: Mobile Ambient Sensors, Environmental Sensors, Sensor Risks

ACM Reference Format:
Maryam Mehrnezhad, Christodoula Makarouna, and Danté Gray. 2022. Risks of Mobile Ambient Sensors and User Awareness, Concerns, and Preferences. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3549015.3554171

1 INTRODUCTION

Sensors are increasing on all platforms; from mobile and wearable devices to smart home devices, smart buildings, and smart cities and farms. Sensor-enabled ("smart") devices are sensing, recording, processing and broadcasting information about people and their environment, most of the time without user permission or awareness. These smart technologies are monitoring users, including those in vulnerable groups (e.g. children and older adults), exposing them to attacks such as stealing biometric, financial and healthcare information, and inferring location. Exacerbating the very real risks this creates, is the fact that it is extremely hard for users to understand and control what these devices are monitoring. In particular, sensors on mobile devices (phones and tablets) are increasing in number and variety. Reportedly, there are more than 30 sensors on off-the-shelf mobile phones [26]. These sensors fall under different categories: biometric, communicational, motion, and ambient sensors. While the first two categories are generally better protected by mobile OSs, the latter ones are mostly left without any safeguarding measures. Only some forms of these sensors in combination with other sensors require user permission e.g. 'Physical activity' on Android which reports activities such as walking, biking, driving, step count, etc. In this paper, we

*This work was conducted when the authors were at Newcastle University, UK.

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09…$15.00
https://doi.org/10.1145/3549015.3554171

Table 1. List of ambient sensors found in off-the-shelf mobile devices.

Sensor	Unit	Data Description	Sensor	Unit	Data Description
Light	lx	Illuminance	Magnetic Field	μT	Geomagnetic field strength
Pressure	hPa/mbar	Ambient air pressure	Hall Sensor	μT	Magnetic field strength
Humidity	%	Ambient relative humidity	Air Sensor	NA	Chemical pollutants level
Ambient Temp	°C	Ambient air temperature	Proximity	cm	Distance from object
Device Temp	°C	Device temperature	Laser	cm	Depth & distance from object
Gravity	m/s^2	Force of gravity			

specifically focus on mobile ambient sensors which currently are freely accessible to developers without any permission across platforms (apps and websites). Previous research has shown that users are not generally familiar with such mobile sensors and don't realise the potential risks [15, 26, 27]. Ambient sensors, alone or in combination with other sensors, can impose serious security and privacy risks to mobile users [13, 16, 28, 38, 40, 41]. However, the research community has not studied users about their concerns and preferences in relation to the mobile ambient sensors. Accordingly, various aspects of their risks are unknown and users are less familiar with them and concerned about them in comparison to other sensors [26].

Ambient or environmental sensors are increasing, not only on mobile devices, but also on other platforms e.g. toys, smart buildings, and sometimes more than other categories of sensors. For instance, smart buildings are equipped with a wide range of ambient sensors [19]. Such sensors can introduce a wide range of risks to the users of smart environments [8, 22, 29, 34]. In addition, all previous user studies have considered sensor access through mobile apps only, and sensor access on other platforms such as websites has been understudied. Finally, while some research suggests that Machine Learning (ML) and Artificial Intelligence (AI) systems may be the solution to managing sensors in a secure way [35, 36], no user studies support such claims.

We address the above research gaps by conducting an online user study (N=197) on ambient sensors for the first time. We aim to measure user awareness, concerns, and preferences when such sensors are accessed by mobile apps as well as web applications via mobile browsers. We also ask our participants about a general 'smart system for sensor management' to handle security and privacy on their behalf. Our results show that while users may not be familiar with the risks of such sensors, they would be annoyed if their personal information is at risk via ambient sensors and would take some forms of protection actions. Such protection actions (close app/website, uninstall, deny permission, etc.) and the user preferences for permission models (permission vs. notification, install-time vs. run-time, etc.) are consistent across the two platforms (apps and websites). We also found that the majority of our participants would like a smart management system to handle sensors in a usable and secure way, while giving them control over the settings. These results are important findings since they support the industry to come up with usable solutions to protect the users against potential risks; enabling them to use smart technologies to improve their quality of life without fear or risk.

2 BACKGROUND AND RELATED WORK

We review ambient sensors, their access and risks, previous user studies and research gaps.

2.1 Ambient Sensors

The variety and types of sensors are increasing on mobile devices. There are currently more than 30 sensors in mobile devices [26]. These sensors fall under four main categories: (1) identity-related (biometric) e.g. GPS, camera, microphone, fingerprint, faceID, iris scab, heart rate, (2)

communicational e.g. WiFi, Bluetooth, and NFC, (3) motion such as gyroscope, accelerometer, and orientation, and (4) ambient (environmental) such as temperature, humidity, pressure, light, proximity, gravity, magnetic field, and hall sensor. We focus on ambient sensors on mobile devices. By going through the off-the-shelf mobile devices as well as Android [2] and iPhone developer [6] websites, we prepared a list of ambient sensors. These devices included: iPhone products (11 Pro and SE2), Google Pixel 4, Samsung Galaxy M series, Huwaei Mate series, and CAT S series. Table 1 shows a list of such sensors with their units of measurement and data description. Each of these sensors has a variety of usages in different applications. These sensors include: *Light* senses the amount of ambient light and e.g. adjust the screen brightness to it. *Pressure (Barometer)* and *Humidity* sense the atmospheric pressure, and moisture/air temperature, respectively, e.g. for weather forecasting. *Ambient Temperature* monitors the air temperature or ambient temperature on smartphones. *Device Temperature* monitors the temperature of e.g. the battery and CPU of a smartphone for performance adjustment. *Gravity* measures the acceleration effect of the earth's gravity on the device enclosing the sensor, which can be used for navigation. *Magnetic Field* is used to measure the magnetic field e.g. in a compass app. *Hall Sensor* measures the magnitude of a magnetic field; used for detecting the flip cover attached to the phone to turn the screen on and off. *Air Sensor* detects the level of the air pollutants e.g. for the quality of indoor air. *Proximity* detects nearby objects e.g. detecting accidental touch screen taps when the phone is close to the ear. *Laser* establishes the depth; calculating the distance of the phone from an object, used in e.g. construction and DIY projects.

We have included some of those applications in our survey in the Appendix. Some of these sensors may differ in units depending on the platform. For example, some proximity sensors provide only binary values representing near and far. In addition, the definition of sensors and category can vary across platforms. For example, CAT smartphones have a thermal camera that matures the thermal map of the environment. This sensor also uses the normal camera which belongs to the biometric category. In addition, certain categories such as gravity, magnetic field and proximity can belong to other sensor groups too, e.g. motion and position [2]. Such categorisation had historically been the result of considering the application of the sensor rather than its actual measurement. In this paper, however, we consider such sensors as ambient sensors since they are measuring something about the environment of the phone and the user.

2.2 Access to Ambient Sensors

Ambient sensors can be accessed in various ways including mobile apps, JavaScript code, IoT programming, and IoT search engines. Here, we explain each of these ways with examples. **Mobile app** programming is the mainstream approach to have access to mobile sensors. Android classifies a number of ambient sensors as 'Environment sensors' [2]. These sensors include ambient temperature, light, pressure, humidity, and (device) temperature. To read data from these sensors on an Android device, an instance of 'SensorManager class' should be created. Then a sensor listener should be registered and then the incoming sensor data can be handled in the 'onSensorChanged()' callback method. If the sensor value changes, it will be reported to the app with the new number, otherwise, the current value is the previously observed one. An example of a pressure sensor in an Android app is shown in Fig. 5 (Appendix). Apple Developer supports fewer ambient sensors in comparison to Android. The current ambient sensors available to iOS app developers include light, magnetometer, and altitude on the phone [6], though Apple allows access to other sensors such as home humidity via HomeKit [7]. W3C offers specifications for **browser and web developers** to define a concrete sensor interface to monitor a few ambient sensors including proximity, light and magnetometer. These specifications are developed by the Devices and Sensors (DAS) Working Group [42]. Fig. 6 shows how an ambient sensor can be observed via JavaScript code.

Another way of programming ambient sensors is via **IoT devices**. Various companies have been offering sensor solutions to developers. Examples include Bosch XDK [11] and Nordic Thingy [10]. Fig. 7 shows an example of access to a temperature sensor data via Arduino. In addition, discovering various sensor-enabled IoT devices and access to such data values are possible via IoT search engines such as shodan.io and thingful.net. Note that while our studies do not concern IoT sensors directly, most of these IoT sensors can be accessed and managed on the user's mobile phone either via an app or within a browser. Although access to ambient sensors is possible across various platforms, their definitions, categorisation, and the technical details of sensor access (e.g. when sensor value changes, or on particular frequencies) varies across platforms. This creates more complexity when it comes to managing their risks.

2.3 Risks

Mobile ambient sensors are not typically considered as the OS resources and do not require user permission on any platforms [26]. Previous research shows that mobile sensors can pose serious security and privacy threats to the users [39]. Examples include using mobile NFC for tracking user payment transactions [25], identification of mobile and IoT devices from public WiFi [44], attacking user PINs and touch actions by using motion sensors via JavaScript [27], and using mobile microphone and camera to infer PINs [37]. The research on the potential risks of ambient sensors for mobile users is relatively sparse. In [24, 28], it has been shown that the location of a user can be inferred by a combination of sensors and other mobile data even if the GPS is off. These sensors include accelerometer, magnetometer, and barometer. Additionally, it has been shown that the mobile light sensor can be used in a side-channel attack for PIN recovery [38]. W3C ambient light specification [40] recognises a number of potential privacy leaks for the light sensor including profiling, cross-device linking, cross-device communication, cross-origin leaks, and hijacking browser history, some of which has been shown in previous research [13]. This specification suggests limiting the maximum sampling frequency and reducing the accuracy of sensor readings to mitigate such threats [40]. In addition, W3C has recognised such sensor readings as a high-value target for network attackers and handles them via the permissions specification [41]. However, in practice, none of the browsers follows such recommendations, and access to such sensor data is free to the websites. According to [16], sensor APIs are accessed on around 3% of websites (of 183K), the majority of which also engage in fingerprinting.

IoT environments and devices are prone to many of these ambient sensor attacks and beyond. For example, ambient data e.g. light on wrist-wearables can be used for Keystroke inference [34]. Similarly, Air sensors (e.g. CO2) can contribute to indoor localization and occupancy monitoring [8]. Human presence and count can be detected via observing environmental parameters; ambient humidity, illumination, and sound rate [22]. In smart environments, data from multiple sources can be combined for improved recognition accuracy. For example, in [29], light, temperature and ambient motion sensor measurements are used to recognize multiple daily activities of the residents of a smart home such as grooming, cooking, eating, and watching TV. The above examples are those ambient sensors that smart environments share with mobile devices. Further types of ambient sensors are increasingly being embedded in smart devices and environments without proper safeguarding; putting the security and privacy, and safety of the users at risk [22]. We also predict that with the advances in AI and sensor processing, more attacks will be introduced based on ambient sensors in all sensing contexts and it is important to study such sensors separately.

By following the relevant related work on security and privacy risks of ambient sensors, we recognise the following as potential risks: **Location Tracking**: using sensor readings to physically locate the device (instead of using GPS directly) [28]. **Eavesdropping**: eavesdropping on user activity with the phone e.g. recovering speech (user speaking or talking on the phone) or screen

content (game, movie, etc.) from sensor readings [13]. **Keystroke Monitoring**: inferring user input on a touchpad (e.g. PINs, passwords, and lock patterns) from sensor readings [34, 38]. **User (activities) Identifying**: inferring individual's patterns and activities (e.g. sitting, running, using a train, and taking a phone call) [8, 29]. **Device Fingerprinting**: uniquely identifying a device and profiling users for purposes such as targeted advertising [16, 40].

2.4 User Studies

It is known that users are not generally familiar with most mobile sensors, and that there is a disparity between the actual and perceived risk levels of sensors [15, 27]. It has also been shown that teaching the users (via general sensor description and working with sensor apps) does not immediately correct the user risk perception, and other factors such as the user's prior general knowledge have a stronger impact [26]. While there are many user studies on biometric sensors (e.g. [1]) and some on communicational (e.g. [32] on contact tracing apps) and motion sensors (e.g. [15]), mobile ambient sensors have not been studied via user studies. There is limited user studies on ambient sensors in other contexts such as smart buildings [19] where the results show that users are not generally familiar with the application of smart buildings' ambient sensors such as temperature, CO2, humidity, occupancy and brightness. In addition, users are concerned about their privacy in such smart environments and would like to have more transparency and control regarding such data. There has been an ongoing conversation in the industry (e.g. [41]) about the usability of some of the proposed safeguarding methods for mobile sensors including install vs. run-time, individual vs. group permissions, one-time vs. continuous monitoring, explicit vs. implicit, opt-in vs. opt-out consent, limiting sampling rate and adding noise, global and pre-origin access control, visual indicators, etc. However, it is not clear if and how these methods have been evaluated from the user point of view. In addition and on the next level, there are some academic efforts to use ML and AI algorithms in order to manage sensors automatically e.g. [35, 36], however, none of them include users as co-designers.

3 METHODOLOGY

In this Section, we explain the design of our online survey, data collection and analysis.

3.1 Questionnaire Design

For designing this survey, we prepared a list of ambient sensors and potential risks by a comprehensive literature review as explained in Section 2. While most ambient sensors are named after their functionality and are self-explanatory, for measuring user concerns for specific risks associated with each sensor, we gave description and application examples for each sensor before asking the related questions. To make sure that the user knows about sensors and potential risks and to avoid response bias, we only provided a general description of sensors and attacks without highlighting that ambient sensors can contribute to such attacks specifically. This is consistent with the methodology in [15, 26] where similar level of description of sensors and risks was presented to the participants in a video. We chose to give written descriptions about sensors and their potential risks as opposed to providing videos [15] and asking the participants to work with sensor apps [26] for three reasons. First, within the current permission models of mobile apps and browsers, none of these sensors can be controlled by users. Hence we did not need to educate the users about protection mechanisms to observe the real-world practices and preferences of the users. Second, since the study was online and there was no observation by the researchers, we did not want to confuse our users by asking them to move between the survey page and other web applications. Third, previous research [26] has shown that working with sensor-enabled apps wouldn't immediately improve the user perception of risks around sensors, and other factors such as their prior

knowledge have a more significant impact. Our survey consisted of 8 sections (full questionnaire in the Appendix).

1. Mobile ambient sensors: After a brief description of the study, we ask our participants to what extent they are familiar with each sensor and how concerned are they about these sensors in relation to their general privacy and security? In this section, we do not give a description of sensors to measure the prior knowledge and concern of our participants about sensors. Given that the majority of these sensors are named after their functionality, our participants in the pilot study did not report any difficulty in answering these questions.

2-3. Tech demographics and general security and privacy: Next, we ask our participants how familiar they are with mobile technology. We also ask them general questions about their security and privacy concerns and experiences. We provide a list of personal and private information (e.g. photo, medical records, and user activities) and ask them about their concern on these items if accessed by unauthorised parties.

4. Protection preferences: At this stage, we provide a list of sensors with a brief example of their application. Then we ask if and how our participants want to be informed about apps and websites having access to these sensors. Here, we study two platforms (apps and websites), two general safeguarding methods (asking for permission with user direct input and notifying user without user interference), as well as how frequently the user wish to be asked for permission/notification (never, install time, run time, each visit, regularly).

5. Risks: Next, we ask our participants to read the sensor descriptions again, and briefly mention that some of the mobile sensors (not specifically ambient) may have some potential risks as listed in Section 2. We provide brief explanations about these risks; giving the chance to all participants to familiarise themselves with such risks. Next, we ask if they previously knew about these risks and whether they think each ambient sensor may contribute to such risks. We measure their feelings and protection actions (deny permission, using other apps/websites, uninstall app, close website, etc.) if an app/website gathered information about them via sensors without any permission/notification.

6-7. Protection and notification preferences: In this section, we ask our participants to think about their protection preferences again (similar to section 4). This is to put their knowledge and concern into context. Note that at this stage, the participants have already been provided with the description of sensors, example of their applications and a range of risks that mobile sensors might contribute to. In addition, we ask them if they would prefer a smart management system to handle sensor access and permission on their behalf. We ask for further comments in open-text questions about their reasons. Here, we only study the general understanding of users about potential smart sensor management systems to gain a broad picture. In our future study, we would like to focus on features and users' feedback on such a smart system. Finally, we present our participants with a list of notification models (audio, visual, tactile, combination, none) and ask for their preferences and their reasons.

8. Demographics and consent: We also ask some questions about the demographics of our participants and their consent. In addition to this explicit consent, we also explained to our participants in our email invitations that taking part in this study is completely voluntary and they can drop out at any stage. They also were provided with email addresses to share their ideas and concerns about the study. We finish our survey by thanking the participants and offering them to enter a competition to win a £50 Amazon voucher.

3.2 Data Collection and Analysis

The questionnaire was created using 'onlinesurveys.ac.uk'. We conducted a pilot study with 10 acquaintances of the authors to check the flow of the survey and its data collection processes. We fixed the minor typos and made a few structural changes accordingly. Then we sent the link

to potential participants via email lists, messaging apps, and social media. This research had full approval from Newcastle University's Ethics Committee before the research commenced. Participation in this study was completely voluntary and anonymous and our participants could drop out of it at any stage as they were advised in the invitation email/message. The participants were provided with the contact details to communicate their comments and concerns. Our survey was completed by 197 participants across several EU countries occupying different jobs ranging from student, teacher, auditor, HR, accountant, engineer, to farmer, personal assistant, and not working. 50% of our participants were female, 49.5% were male, and 0.5% chose other. The age range covered from 18 to 63 years old (average: 31, STD: 10.8).

Our method of processing the collected data is a mix of quantitative and qualitative analysis. The results for some of the questions are presented by stacked bar figures. For our free-text style questions, we run thematic analysis; taking an inductive approach and allow the data to determine our themes. We facilitated a conventional line-by-line coding [18] of all the responses. Three researchers (two of the paper's authors and an independent researcher) contributed to our thematic analysis. Two of these researchers performed the coding and extracted the key themes independently. For more complex and lengthy comments, we assigned multiple themes to them. The researchers discussed these themes to agree on potential inconsistencies and also chose the user comments that represent such themes for inclusion in the paper. We acknowledge that these comments may include more insight than the extracted themes and that a focused study (e.g. semi-structured interviews) is required to uncover such insights, which we leave as future work.

3.3 Limitations

We took a comprehensive approach and included multiple questions in our survey, which might have caused survey fatigue. However, the response to the open-text questions suggests that the participants stayed engaged with the study until the end. This also suggests that while we did not randomise the order of the sensors and risks in the survey (since the platform did not allow), it is unlikely that the questions were answered randomly. We analysed the effect of random answers for each participant and did not find any visible patterns. The majority of the participants said they are either students in different disciplines or associated with the university at different levels (researchers, faculty members, or admins). Hence, we acknowledge that our study results are only based on mostly university-level educated participants.

When we want to introduce sensor risks to the participants, we highlight that "*If mobile sensors (e.g. Bluetooth, GPS, Motion and Ambient sensors) are not used responsibly by apps and websites, some of them can impose some levels of risks to user security and privacy*". Hence, by choosing their preference, the participants aim to protect themselves from the potential harms caused by malicious programs. We assumed that the participants would know that denying access to sensors might affect the application of a legitimate program. This is in line with the approach adopted by [15, 26, 27]. In practice, there could be a dilemma for the user to decide whether an app/website needs such sensor access or not. Although we did not factor that in, we did include a section on user's opinions on a general smart sensor management system. We aim to study such factors in user perception and practice in managing sensors both manually and via a smart system in the future. This study relies on self-reports, which is widely employed for eliciting user responses in user studies and the insights can translate to real-world settings [33]. Working from home might have impacted the number of attendees, as well as their concerns and preferences in various ways.

4 RESULTS

197 participants completed our questionnaire. Except for one, all the participants said they own a smartphone/tablet; the majority for more than five years (84.1%). 66.3% had an Android device, 32%

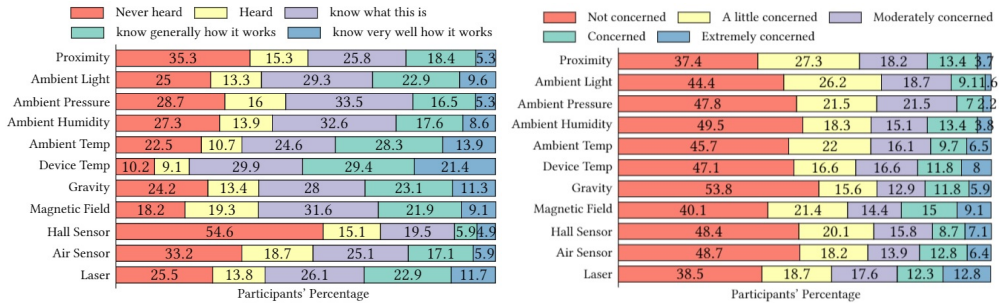

Fig. 1. Left: Participants' awareness (x labels are shortened here), Right: concern levels about ambient sensors.

iOS, and 2.1% Windows devices. On average, our participants had 42 (self-)installed apps (from 1 to 450 apps, STD: 52). The apps varied across categories (in descending order): social media, banking, email/communication, music, work-related, news, gaming, photo-editing, sports, event planning, and other (e.g. shopping, learning, and medical). Our participants said that they normally visit a website on their mobile (64.4%), PC/laptop (29.3%), tablet (4.8%), and via other means (1.6%). 65.6% of the participants said they visit less than 10 websites in a day, while the rest said they would visit more than 10 websites.

4.1 Awareness and Concern

In the beginning of our survey, we asked if the participants know these sensors and to what extent they are concerned about each sensor. Fig. 1 demonstrates user familiarity and concern levels for ambient sensors. Most of our participants chose either *Never heard of it*, or *Heard of it, but don't know what this is*, or *I know what this is, but I don't know how it works*; among which the Hall sensor is the least known one, and Device Temperature is the most familiar one. Fig. 1 also shows that most participants are either *Not concerned* or *A little concerned* about these sensors in relation to their general privacy and security, and there are no significant differences across the sensors. While it may look like that most users know these sensors at some level, these results are consistent with [26, 27] where the authors concluded that such awareness level is far from those of other sensor categories such as biometric and communicational.

When we asked about their general privacy and security views, over 80% of the participants were concerned about their photos and videos, passwords financial information to be accessed by unauthorised parties. This was followed by over 60% of out participants being concerned about their conversations, audios, location, and activities/identification. Over 50% of the participants showed concern for their medical info, device unique info, and touchpad input. Only 40% were concerned about their demographic info (e.g. DoB). In addition, 63% of participants said that they have not personally experienced any privacy/security issues related to computing or mobile tech, while the rest said they have. Such incidents included a virus, stolen passwords, compromised bank info, and scamming. Around 18% of our participants said that such an experience had significantly impacted their personal/professional life, and 55% said that they have heard a story on such a significant impact on someone else's life.

4.2 Protection Preferences

At this point, we presented a list of ambient sensors with a short description and example in our questionnaire. Over 70% of our participants (strongly) agreed that they will be annoyed if an app/website has access to their mobile ambient sensors without their permission and without

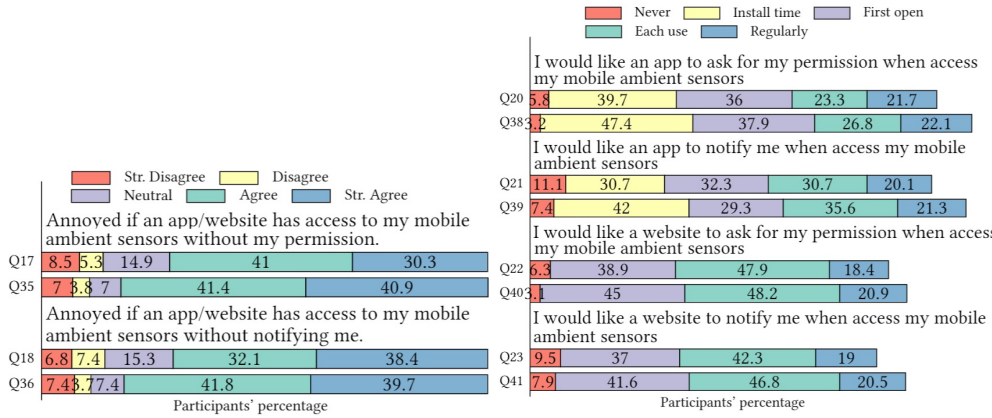

Fig. 2. Left: Participants' annoyance about app/website access to sensors before (Qs17-18) and after being introduced to risks (Qs35-36). Right: Views on sensors permission models before (Qs20-23) and after being introduced to risks (Qs38-41).

notifying them (Fig. 2). When directly asked if they think a service (app and website) should ask for their permission before having access to ambient sensors on their mobile device, more than 80% of our participants (strongly) agreed with such a statement.

As shown in Fig. 2, our participants mostly preferred the app to ask for permission when installing it, then when they open it for the first time (to use), on each use and regularly. A few participants chose 'Never'. A similar trend was observed for being notified about such sensor access. In the case of websites, our participants preferred to be asked for permission as well as notified on each visit, followed by when opened for the first time, and then regularly. Very few people said 'Never'. Note that in these forms of questions, multiple choices were allowed. We acknowledge some of the questions (e.g."access x without permission", Fig. 2) might have a negative connotation and induce protective behavior from users. However, the results from the follow-up questions, with a more positive tone confirm such findings. Upon asking for extra comments, a few participants were surprised and annoyed about websites accessing such sensors (as opposed to app access). Some expressed unpleasant feelings about the current management of sensors e.g. annoyance for 'take it or leave it' approach and expected explanation about the usage of these sensors by apps. Some said they generally preferred to opt-in instead of opt-out. Some of the participants had concerns over the combination of such sensor streams and potential privacy implications. Only a few participants said they do not recognise these sensors as sensitive. Some users expected the OS to handle sensor access automatically in a trustworthy way, and some commented that they prefer notification over permission. We will discuss such preferences at more length later.

4.3 Risk Awareness and Feelings

When asked about the risks of mobile sensors (Fig. 3), they expressed different levels of familiarly with these risks. Location tracking and device fingerprinting were more known to the participants and user (activity) identifying, eavesdropping and keystroke monitoring were less known to them. Fig. 3 demonstrates that our participants mostly think that all of these sensors can contribute to location tracking. User (activities) identifying came second, followed by other risk categories. Proximity sensor was chosen to contribute to all the risk types more than other sensors. Note that at this point of the study, our participants were provided with information about sensors and risks in order to have a consistent reference for the following questions.

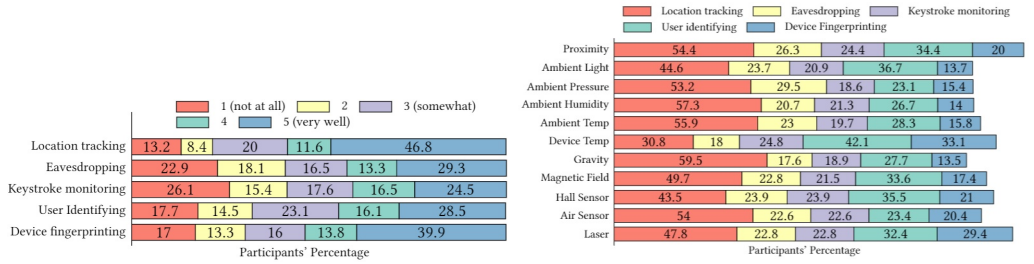

Fig. 3. Left: Participants' familiarity levels with the risks. Right: Participants choosing if ambient sensors contribute to the risks.

We highlight that the user perceived risks may or may not be consistent with the actual risks of such sensors. For instance, 42.1% of the participants feel that the device temperature helps to reveal user identification, and 54.4% believe that proximity sensor readings can contribute to location tracking. To the best of our knowledge, there is no concrete research on whether device temperature and proximity sensors can cause any threats to user identification or location leakage yet. Finding out the disparity between such perceived risks and the actual risks is an important research topic that is left as future work.

When our participants were asked about their feelings in the case of unauthorised access to personal information via these sensors, the majority of them (around or more than 80%) said they will be (very) upset about it. Similarly, more than 80% of our participants said they will be (very) upset if an app/website gathered information about them via ambient sensors without any permission or notification. When asked why would they feel like that in a free-text question, our participants stated various points. Through a thematic analysis of 108 comments, we recognised the following themes (Table 2): Around 30% (60 comments) of our participants expressed that it is not desirable to share their personal data **without consent**. For example, a participant said: "*I must have the right to refuse access to any sensor which collects data about me*". Another comment included: "*I don't want any kind of information to be gathered with no permission or saved*". Another participant said: "*It is none of their businesses to gather any of that information. It violates my right to privacy (unless I have explicitly said it's okay)– which I believe should be a human right.*" Around 23% (46 comments) of our participants said they felt this way since it is a **violation of their privacy**. For example, a comment included: "*I see it as a massive invasion of privacy*". Another participant said: "*Its an invasion of my privacy and a risk to the safety of my child and myself* ". Another concern of our participants, shared by 13% (25 comments), was the illegitimate and **malicious usage** of such sensor data and whether or not it will bring them any form of harm. For example, a participant commented: "*My privacy would be violated and accessed by third-parties, which might use my information to conduct malicious intentions e.g. access my bank or social media account.*" Another one said: "*The information could be used to cause me financial, mental or physical damage*". Our participants also asked for more transparency in sensor data collection e.g. saying "*Apps and websites should be upfront about the sensor data they are collecting.*" Other form of feelings such as '*exploited*', '*insecure*', '*monitored*', '*spied on*', '*creepy*', and '*tracked*' were also observed in the comments.

Table 2. Participants' reasons for unpleasant feelings about unauthorised access of ambient sensors.

Theme	Lack of Consent	Violation of Privacy	Malicious Usage	Others (e.g. Transparency)
no. (%)	60 (30%)	46 (23%)	25 (13%)	25 (13%)

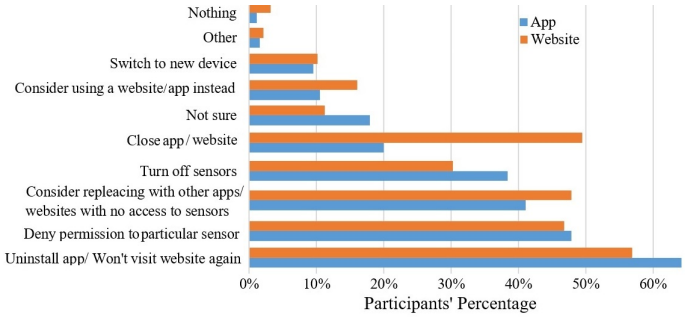

Fig. 4. Potential actions taken by participants in case of senor leakage in Apps and Websites.

4.4 Protection Actions

As shown in Fig. 4, our participants chose multiple actions as a protective method in case an app or a website imposes any risk via ambient sensors. Uninstalling the app and not visiting the website again were chosen by more than 50% of our participants. The participants also chose other items including denying permission, using other services, and closing the app/website. The popularity of these actions was pretty much the same across apps and websites with one exception. This suggests that users have a consistent preference when it comes to their protection actions for sensors regardless of the platform. The only exception was closing the app/website which was only chosen by 20% of the participants for apps, vs. 49% for websites. This disparity is, of course, due to the differences in the nature of these platforms which make them not directly comparable. Closing a website and not visiting it again could be considered as the equivalent of uninstalling an app. However, closing an app means that it can still be on the user's device and it may continue collecting data in the background. This is an interesting finding for the web community since the results suggest that users might feel more in control of a webpage regarding sensor access in comparison to an app that goes through a vetting process before being available on the app market. Further studies are required to discover the reasons behind this finding.

In the comment section, some of the participants mentioned other forms of Privacy Enhancing Technologies (PETs) for protecting themselves against sensor leakage including using tracker blockers and/or extensions (STRANDS, privacy badger, GoogleDontTrackMe, etc.), and complaining about not having a choice but using the services due to e.g. work reasons or lack of alternatives. When our participants were asked directly if they would discontinue the usage of a service (app or website) if it poses risks to their privacy, more than half of them said yes, 10% said no and the rest were not sure. Similarly, more than half of the participants said they would be concerned about such risks happening to them, while 20% said they are not concerned, and the rest were not sure.

4.5 Protection Preferences (Revisited)

After being informed about the risks of sensors, some participants felt more cautious. Fig. 2 shows a shift in the expressed annoyance level in the case of a sensor access without a permission or notification. When directly asked if a service should ask for permission, the same percentage (over 80%) of the participants agreed, with more moving from Agree to Strongly agree. This may indicate that regardless of being informed about sensor risks, the users are indeed demanding to have more control on ambient sensors which may not be perceived as risky as other sensors (e.g. GPS or mic). Similarly, there was a shift in the number of times that various permission models were chosen in the revisited questions. As shown in Fig. 2, there is a decrease in 'Never', and all the other items

Table 3. Extracted themes form user comments on features of a smart sensor management system.

General Features	no. (%)	**Preferred Risk Notification**	no. (%)	**Annoying Risk Notification**	no. (%)
Control	30 (15%)	Distinguishable	36 (19%)	Repetitive	52 (26%)
Security & Privacy	20 (10%)	Communication Channel	10 (%5)	Poor User Interface	25 (13%)
Usability	25 (12%)	Including Details	24 (11%)	No Control/Customisation	14 (7%)
		Simple	18 (8%)	False Alert	13 (7%)
		Requiring User Action	14 (7%)		

were chosen more than before. The only exception is being notified about sensor access on apps when installed vs. opened for the first time where the former has increased more significantly, and the latter has slightly decreased. This is despite the fact that install-time permission model has been retired by Android, which will be discussed later.

4.6 Smart Sensor Management System

We asked if our participants would prefer a smart management system to handle sensor permissions. More than half of our participants (strongly) agreed to that questions and 30% were neutral and the rest (strongly) disagreed. Through thematic analysis of 60 comments (Table 3), we extracted the following themes for reasons of such preference: Around 15% (30 comments) commented that such a smart system would enable them to be more **in control** of sensor data via turning sensors on and off, handling permissions, being notified, auditing apps and sensor access, etc. For instance, a comment included: "*Check and confirm that ambient sensors are used only with my permission, and if not to notify me immediately.*" Other examples include: "*Giving you control whenever you want to check the use of your device and sensors*", and "*specify why an app needs access to these and ask for approval*". Around 12% commented that the **usability** of such as mart system will be convenient in many ways. For example, one said: "*It would be easier to manage permissions; especially, with a feature for grouping similar apps to manage their access permissions as a group rather than once for each app*". Another one said: "*It should allow me to easily revoke sensor access and re-enable it when an app absolutely needs it.*" Around 10% believed that such a smart system would protect their **privacy and security** more efficiently than managing app permission manually. One comment said: "*It [smart system] should respond to news about leaks to apps and automatically restrict the app or containerize it with fake sensor data.*" Another one said: "*[such a system would] protect [the] privacy and keep users safe while running in [the] background of [the] device.*" Other themes include the ability of the smart system to learn the user behaviour in permissioning, automatic analysis of apps/websites to distinguish benign services from malicious ones, embedded with the OS and low-performance impact. For example, a comment included: ' '*Comfort. It [smart system] would have to be manually configured at first, so that when I install apps later, it would manage their privileges and permissions as I would see fit, without me having to do it myself every time*". Another participant said: " *..., I would like such a smart system in my OS to be able to tell if an app or website should or should not be given access to certain sensors on my device*". Another one said: "*Such a system should be able to identify characteristics of the sensors on an app/website and alert the user prior to use in order to receive a confirmation about proceeding to either download the app or enter the website.*"

Out of the 22 comments left by those who did not like a smart system, they mostly indicated that trusting such a system is not easy since it may be hacked and/or does not work effectively. One participant said: "*3rd parties may hack this system and use it to control all sensors and my privacy would still get violated.*" Another one said: "*Can't guarantee the smart system will make the correct choices for the permissions. My opinion on whether I want them used or not may change*". They also indicated that they prefer to handle their privacy manually rather than relying on a system e.g.,:

"*I want to give permission myself and to be reminded of issues/risks to be aware*". In the comments of this section, we observed that some of the participants may have not speculated that a smart system would take their input and would be fully automatic and take the control away from them. Since we did not give any description of a specific smart system for sensor management, such confusion was anticipated.

4.7 Risk Notification Preferences

We asked our participants about the ways that they would like to be notified about risks. Visual indicators category (e.g. LED light and pup-up windows) was the (most) preferred one, followed by Tactile (e.g. vibration) and then Audio (e.g. beep). A combination of such methods was, of course, the most preferred category. We also asked our participants to elaborate on how they would expect the notification to look like. This free-text question had a significant response from our participants (98 comments). We observed some interesting themes: Around 19% of our participants (36 out of 98 comments) described a desirable notification to be as **distinguishable** as possible, using words such as '*bold*', '*specific*', '*characteristic*', '*like an alarm*', '*flashing*', '*very alerting*', '*bold letters*', etc. with one participant commenting: "*Flash, vibration and light in 'police' type siren*". Our participants highlighted various reasons for these preferences e.g.: "*Flashing and vibrating would be good - my phone makes enough beeping noises already, so would be difficult to assign this to a specific notification*", and "*There are plenty of fake security windows pop-ups so a way to distinguish between the fake and real ones would be a must.*" Some of the participants (5%) thought that such risk notification should be communicated with them via **other channels** such as '*text message*', '*email*', and even a '*phone call*'. Such comments include: "*Email with a precise description of the attack, time, source of the attack, and possible countermeasures.*" and "*... a call ringing so I can notice the risk immediately.*" 11% of our participants said they expect such risk notifications to **include details** about the threat and the countermeasures, for example, "*A pop-up window describing the risk and how to prevent the risk and protect myself.*" and "*preferably a pop-up which notified me. This should contain details of the issue and options for mitigation*". Around 8% of our participants described a desirable notification to be ***'simple'***, '*straight to the point*', '*clear*', '*regular*', '*plain*', and potentially managed by the mobile OS to look '*professional*' and '*official*', such as a '*simple Android notification*' and an '*iOS warning*'. For example, a participant said: "*A regular pop-up Android notification. On a computer, a plugin for a browser, a small discreet pop-up on the side can work well.*" Though, some of the expected features in this theme such as '*small*' notification and icon conflicted the previous theme (including details). Some comments (14 comments) included content expecting a risk notification to require **user action** e.g. by "*asking for approval*", "*A pop-up message with a Yes/No*", "*The system says at risk for a privacy attack, please review your preferences*", and " *I want the notification to stop the app until I have intervened, ...*" Other comments expected such notification to be presented to the user before using the service stating e.g. "*before you go onto a website you should be able to see a pop-up preventing you from doing anything else apart from Accept/deny the permissions of the website. Similar to how cookies on websites are handled*". Some expected the notification to remember the user's previous behaviour e.g.: "*..., it should be a small notification that can be yes or no allowed upon request, it should remember my previous option so I can one click the button with the knowledge that the decision had already been thought out by myself, ...*". A few users believed that communicating the risks depend on "*how configured on a user basis, available in the settings*" as well as the risk level e.g. someone said: "*It depends on the ratio of the risk. For high risks: a pop-up, a vibration and a beep. For medium risks: a pop-up, and vibration. For low risks: a pop-up.*"

When asked how **frequently** would they like to be notified of a potential privacy risk/breach, 47% of the participants chose 'Every time no matter the type of risk or information gathered', 43% chose 'Only when a specific type of risk may occur', 5% selected 'Only after information is gathered',

2.5% chose 'Receive no notifications, but be able to actively go check your risk at will', and 1.5% chose 'Never'. When we asked the participants why they would prefer to receive notifications at this frequency in a free-text question, the reasons varied from '*to have as much information as possible*', '*to be extra safe*' and '*to be better informed*' to '*don't want to be hassled*', and '*getting a notification every time may be excessive*'. We ran a quick text analysis on the data and realised that those who would like to receive notification all the time, would like to '*be in control*' and '*aware*' of any data leakage, and highlighted, '*privacy*', '*security*', and '*safety*' is important to them. On the other hand, those who chose to be notified for specific risk types, said that only '*very risky*' incidents mattered to them and the '*usability*' of the system is an important factor.

When asked what form of notification would annoy them, the following themes were observed: More than half of the comments (out of 101) included words such as **'*repetitive*'**, '*intrusive*', '*frequent*' and '*prolonged*'; stating that such practice would impact the '*usability*'. For example, someone said: "*It can get very annoying to receive messages all the time no matter the type of risk.*" A quarter of the comments were concerned about the a **poor user interface** of the notification saying that a '*loud*', '*high-pitched*', '*obtrusive*', and '*noisy*' and '*excessive*' alarm and in some cases light and vibration, as well as those that visually look '*unofficial*', and those which could not be easily '*off*' and '*dismissed*' would bother them. For example, a participant said: "*Constant flashing, ringing and vibration for a long time e.g. longer than 30 seconds.*" 14 of our participants said it would be bothering if the notification did not give them **'*control/customisation*'** over their preferences. For example, one said: "*If it is constant with no way to adapt it, e.g. if it believes google maps is tracking me and there's no way to set it as 'allowed'*". Others said: "*if it did not contain information and/or pathway to mitigation - just knowing without being able to do anything*", "*if there no way to prevent the notifications appearing again", and "If it's unnecessary and constant when precious approval has been given.*" Some of our participants (13 comments) said that it would be bothering to get a notification which is a **'*false alert*'** without a reason and/or for '*small risks*', or something they already know. For instance, someone who wished to be notified on all risks, said: "*[it would bother me] if the warning is for not important issue/risk*". Another comment included: "*Repeated notifications for something I already know [is bothering]. For example, my Android phone sometimes notifies me that "Snapchat is using the camera", whilst I'm taking a photo.*" Other comments said it would bothered them if there was '*no notification*' for risks, if there was '*not enough information*', and/or it was a '*late notification*' after the harm was done.

5 DISCUSSION

Here, we discuss our results, real-world practices, and provide some recommendations for industrial practices and areas for future work.

5.1 Results across Demographics

Our statistical analysis shows that our male participants expressed more *knowledge* about sensors and the potential risks associated with sensors (e.g. location tracking, eavesdropping, keystroke monitoring) in comparison to our female participants. However, our female participants expressed more *concerns* in relation to their general privacy and security being at risk via these sensors as well as the potential contribution of such sensors to the known risks. The same results across gender were concluded in regards to the risks associated with mobile motion sensors in [15]. We did not find any significant difference between men and women in their feelings about their personal information being accessed by unauthorised parties via ambient sensors and without their consent (Fig. 2). In terms of protection preferences (Fig. 2), the same pattern was found among male and female participants. Our results from analysing Q33 on users' potential actions about a malicious website/app across the two genders (Table 4) highlights that women are less decisive on

Table 4. Participants' answers to Q33 (If an app or website that you use frequently (e.g. news, social media, etc.) posed a risk on your privacy, would you discontinue your usage?) across gender and mobile OS.

Action	Male	Female	Android	iOS
Yes	62%	51%	56%	57%
Not sure	31%	36%	33.5%	33%
No	7%	13%	10.5%	10%

terminating the use of the app/website. These results support previous research concluding that women tend to be more sensitive and concerned about their privacy than men [14], though they might be less involved in taking protective [12, 30] and technical actions [14, 23, 31]. We also found out that there are different patterns across preferences in different age groups. The younger the participants are, the less they prefer to involve in permission controlling. Our younger participants chose '*When opening the app/website for the first time*' and '*when installing the app*' more often than older participants. This may be due to various factors such as usability as mentioned by the participants themselves too. We did not observe any significant differences across the age ranges for their protective actions when they are at risk via these sensors.

We investigated whether or not the type of the user mobile OS has an impact on their preferences about receiving risk notification (Q48). We did not find any significant differences across the OSs and Android and iOS users both chose *'Every time no matter the type of risk or information gathered'* and *'Only when a specific type of risk may occur'* categories much more often than other categories as their preferred frequency of such a risk notice. Similar results appeared for Android and iOS users for questions related to protection actions (e.g. Q33, Table 4) where 56-57% of the participants said they will stop using a popular website/app if it poses a risk, 10% said they won't stop their usage, and 33% were not sure about their decision. These findings are only indicating that such differences across demographics exist and further research is required for a more in-depth investigation.

5.2 Real-world Practices

We found out that although more than 60% of our participants are either not or a little concerned about ambient sensors, more than 70% of them will be annoyed if an app or a website has an access to them without their consent and control. The current practices on mobile OSs and browsers would not enable the users to have control over such data. It seems that such a fact has been realised by users as well e.g. a final comment included: "*We just have to learn to live with the idea that everything we do is trackable and is being recorded*". Additionally, the link between the data protection regulations (e.g. GDPR) and sensor specifications e.g., W3C [42] and the implementation of sensor APIs by mobile OSs and browsers (e.g. Apple, Google, Firefox, etc.) is not clear. Although a commission of many privacy and data protection authorities stated that sensor and IoT data should be treated as personal data [21], in practice, access to sensor data on various platforms is still unregulated. Finally, sensors' definitions and applications, technical implementations as well as their safeguarding approaches are not consistent across platforms (e.g. Android, iOS, various browsers, IoT). This leads to more complexity in the user understanding and protective behaviour. Our results show that regardless of the platform, there are certain themes around user concerns and preferences that can be reflected in real-world practices to improve security and usability.

5.3 User-centric Solutions

Regulating sensors in a usable and secure way is complicated. On one hand, asking for user consent (e.g. explicit permission) can improve security. On the other hand, it will suffer from usability issues. Interestingly, some of the common practices by the mobile industry are not the user

preferred protection method. For example, Android changed its install-time permissions to run-time permissions in 2018 [3] for security reasons. However, our participants, similar to [26], showed an interest in install-time permissions. In the context of opting-out from app tracking, Apple has incorporated a new privacy notification with control options; App Tracking Transparency (ATT) policy [5], on iOS 14.5 (2021). Although, previous research has shown that users normally ignore permission prompts [17, 20], some reports show that 96% of US users opt-out of app tracking [9]. This indicates that user security and privacy behaviour may change over time and safeguarding approaches should be updated too.

The inconsistency between safeguarding approaches across platforms and the regular updates would make it even harder for the users. Android 11 (2020) introduced one-time permissions within its apps [3]. In this model, whenever an app requests permission related to location, microphone, or camera, the user-facing permissions dialogue contains an option called '*Only this time*'. Additionally, on Oxygen OS 10 (OnePlus) a *'Privacy Alert Slider'* [43] has been added and every time that resources such as camera or microphone are being used by 3rd party apps, the user is continuously being notified. Some of our participants complained that this privacy alert is annoying since such information is already known. Furthermore, if an app targets Android 12 (2021) or higher, the system places a limit on the refresh rate of data from certain motion sensors and will ask for user permission for higher rates. This is to protect potentially sensitive information about users [4]. Another feature is the Android Privacy Dashboard (Android 12) [3] where in the system settings, users can access separate screens that show when apps access location, camera, and microphone information and developers can provide a rationale for users to help them understand why their app needs such access. Though such safeguarding measures are not present for environmental sensors yet, further studies can help to include user feedback on these new features and put them in comparison with those found in this paper.

Due to the fast progress in sensing and smart technologies, it is essential to plan for the next generation of safeguarding solutions for sensors. There exists some research proposing ML and AI systems as potential solutions to manage sensors in a secure way [35, 36]. However, no user studies support such approaches. In this paper, we explored user preferences for smart sensor management systems and concluded that various features are desired by our participants. Such systems should be usable, safe and allow the users to be in control. For example, one of our participants commented: "*A smart system which is designed in a centralised way to restrict access to sensor data would be very good for people less aware of what might be collected about them and protect them from security risks/attacks*". We believe that it is essential to include the users as co-designers of security and privacy features in modern technologies. This is specifically important in sensing technologies since they vary in range, application, and user groups e.g. smart toys and medical devices.

6 CONCLUSION

This paper studied user concerns and preferences in relation to mobile ambient sensors on apps and websites for the first time. Our results demonstrate that the majority of the participants are not or only a little concerned about ambient sensors. However, they would be (strongly) annoyed if a service has access to these sensors without their consent. Participants' views on permission models (permission vs. notification, install-time vs. run-time, first visit and regular reminders, etc.) as well as the protection actions (nothing, close app/website, uninstall, deny permission, etc.) were consistent across platforms (app and website). And finally, Our participants generally preferred a smart management system to handle sensors on their behalf with a wide range of features including giving them control, being usable, secure, and safe. These results are extendable to other contexts such as IoT and support industry to develop the next generation of solutions to protect the users against sensor risks.

ACKNOWLEDGMENTS

We would like to thank W3C Devices and Sensors (DAS) working group for their continuous and constructive feedback on this research. We thank all the participants of this survey.

REFERENCES

[1] I. Ahmad, R. Farzan, A. Kapadia, and A. J. Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *ACM on Human-Computer Interaction*, 4(CSCW2):1–28, 2020.
[2] Android. *Environment sensors*, 2022. Available at: "developer.android.com/guide/topics/sensors/sensors_environment".
[3] Android. *Permissions on Android*, 2022. Available at: "developer.android.com/guide/topics/permissions/overview".
[4] Android. *Sensors Overview*, 2022. Available at: "https://developer.android.com/guide/topics/sensors/sensors_overview".
[5] Apple. *App Tracking Transparency*, 2021. Available at: "https://developer.apple.com/documentation/apptrackingtransparency".
[6] Apple. *SensorKit*, 2021. Available at: "developer.apple.com/documentation/sensorkit".
[7] Apple. *HomeKit*, 2022. Available at: "developer.apple.com/documentation/homekit".
[8] I. B. Arief-Ang, F. D. Salim, and M. Hamilton. Cd-hoc: indoor human occupancy counting using carbon dioxide sensor data. *arXiv preprint arXiv:1706.05286*, 2017.
[9] ArsTechnica. *96% of US users opt out of app tracking in iOS 14.5, analytics find*, 2021. Available at: "https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/".
[10] Bosch. *Nordic Thingy: 91*, 2021. Available at: "nordicsemi.com/Software-and-tools/Prototyping-platforms/Nordic-Thingy-91".
[11] Bosch. *Bosch XDK*, 2022. Available at: "bosch-connectivity.com/products/cross-domain/cross-domain-developement-kit/".
[12] M. Büchi, N. Just, and M. Latzer. Caring is not enough: the importance of internet skills for online privacy protection. *Information, Communication & Society*, 20(8):1261–1278, 2017.
[13] S. Chakraborty, W. Ouyang, and M. Srivastava. Lightspy: Optical eavesdropping on displays using light sensors on mobile devices. In *International Conference on Big Data*, pages 2980–2989. IEEE, 2017.
[14] K. P. Coopamootoo, M. Mehrnezhad, and E. Toreini. " i feel invaded, annoyed, anxious and i may protect myself": Individuals' feelings about online tracking and their protective behaviour across gender and country. *USENIX Security*, 2022.
[15] K. Crager, A. Maiti, M. Jadliwala, and J. He. Information leakage through mobile motion sensors: User awareness and concerns. In *European Workshop on Usable Security*, 2017.
[16] M. Diamantaris, F. Marcantoni, S. Ioannidis, and J. Polakis. The seven deadly sins of the html5 webapi: A large-scale study on the risks of mobile sensor-based attacks. *ACM Transactions on Privacy and Security (TOPS)*, 23(4):1–31, 2020.
[17] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *Symposium on Usable Privacy and Security*, pages 1–14, 2012.
[18] T. Groß. Why privacy is all but forgotten. *Privacy Enhancing Technologies*, 2017(4):97–118, 2017.
[19] S. Harper, M. Mehrnezhad, and J. Mace. User privacy concerns of commercial smart buildings. In *Workshop on Socio-Technical Aspects in Security and Trust*, pages 40–52, 2020.
[20] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall. A conundrum of permissions: installing applications on an android smartphone. In *Financial cryptography and data security*, pages 68–79. Springer, 2012.
[21] J. Kohnstamm and D. Madhub. Mauritius declaration on the internet of things. https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf, 2014.
[22] J. Kroger. Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In *IFIP International Internet of Things Conference*, pages 147–159. Springer, 2018.
[23] E. T. Maryam Mehrnezhad, Kovila Coopamootoo. How can and would people protect from online tracking? In *Privacy Enhancing Technologies*, pages 1–12, 2022.
[24] S. Mazilu and G. Tröster. A study on using ambient sensors from smartphones for indoor location detection. In *Proceedings of 12th Workshop On positioning, navigation and communication (WPNC). IEEE*, 2015.
[25] M. Mehrnezhad, M. A. Ali, F. Hao, and A. van Moorsel. Nfc payment spy: a privacy attack on contactless payments. In *Research in Security Standardisation*, pages 92–111. Springer, 2016.
[26] M. Mehrnezhad and E. Toreini. What is this sensor and does this app need access to it? In *Informatics*, volume 6, page 7. Multidisciplinary Digital Publishing Institute, 2019.
[27] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao. Stealing pins via mobile sensors: actual risk versus user perception. *International Journal of Information Security*, 17(3):291–313, 2018.
[28] A. Mosenia, X. Dai, P. Mittal, and N. K. Jha. Pinme: Tracking a smartphone user around the world. *IEEE Transactions on Multi-Scale Computing Systems*, 4(3):420–435, 2017.

[29] T. Nef and et al. Evaluation of three state-of-the-art classifiers for recognition of activities of daily living from smart home ambient data. 2015.
[30] I. Oomen and R. Leenes. Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management*, pages 121–138. Springer, 2008.
[31] Y. J. Park. Do men and women differ in privacy? gendered privacy and (in) equality in the internet. *Computers in Human Behavior*, 50:252–258, 2015.
[32] E. M. Redmiles. User concerns & tradeoffs in technology-facilitated contact tracing. *arXiv preprint arXiv:2004.13219*, 2020.
[33] E. M. Redmiles, Z. Zhu, S. Kross, D. Kuchhal, T. Dumitras, and M. L. Mazurek. Asking for a friend: Evaluating response biases in security user studies. In *ACM SIGSAC Conference on Computer and Communications Security*, pages 1238–1255, 2018.
[34] M. Sabra, A. Maiti, and M. Jadliwala. Keystroke inference using ambient light sensor on wrist-wearables: a feasibility study. In *ACM Workshop on Wearable Systems and Applications*, pages 21–26, 2018.
[35] A. K. Sikder, H. Aksu, and A. S. Uluagac. A context-aware framework for detecting sensor-based threats on smart devices. *IEEE Transactions on Mobile Computing*, 19(2):245–261, 2019.
[36] A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac. Aegis: a context-aware security framework for smart home systems. In *Annual Computer Security Applications Conference*, pages 28–41, 2019.
[37] L. Simon and R. Anderson. Pin skimmer: inferring pins through the camera and microphone. In *ACM workshop on Security and privacy in smartphones & mobile devices*, pages 67–78, 2013.
[38] R. Spreitzer. Pin skimming: exploiting the ambient-light sensor in mobile devices. In *ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, pages 51–62, 2014.
[39] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Communications Surveys & Tutorials*, 20(1):465–488, 2017.
[40] W3C. *Ambient Light Sensor*, 2021. Available at: "https://www.w3.org/TR/ambient-light/".
[41] W3C. *Permissions*, 2021. Available at: "w3c.github.io/permissions".
[42] W3C. *Devices and Sensors Working Group*, 2022. Available at: "developer.android.com/guide/topics/sensors/sensors_environment".
[43] xda developers. *OxygenOS 10.3.1 (Privacy Alert)*, 2021. Available at: "forum.xda-developers.com/tags/privacy-alert/".
[44] L. Yu, B. Luo, J. Ma, Z. Zhou, and Q. Liu. You are what you broadcast: Identification of mobile and iot devices from (public) wifi. In *USENIX Security Symposium*, pages 55–72, 2020.

A SENSOR PROGRAMMING EXAMPLES

```
...
private SensorManager sensorManager;
private Sensor pressure;
...
sensorManager = (SensorManager) getSystemService(Context.SENSOR_SERVICE);
pressure = sensorManager.getDefaultSensor(Sensor.TYPE_PRESSURE);
public final void onSensorChanged(SensorEvent event) {
float millibarsOfPressure = event.values[0];
// Do something with this sensor data
protected void onResume() {
super.onResume();
sensorManager.registerListener(this, pressure,SensorManager.SENSOR_DELAY_NORMAL);
} ...}
```

Fig. 5. Example of a pressure sensor being registered and used in an Android app.

```
const sensor = new AmbientLightSensor();
sensor.onreading = () => console.log(sensor.illuminance);
sensor.onerror = event =>
console.log(event.error.name,event.error.message);
sensor.start();
```

Fig. 6. Example of a js code; ambient light sensor is created with default configuration and printed to the console.

```
int sensorPin = A0; // Arduino Pin to read sensor output
int sensorInput;
double temp;
void setup() {
Serial.begin(9600); //Start Serial Port as default
}
sensorInput = analogRead(sensorPin); //Read analog sensor
temp = (((((double)sensorInput/ 1024)* 5)- 0.5)* 100);
// Convert voltage to degrees Celsius
Serial.println(temp);
```

Fig. 7. Example of a C code using a TMP36 Temperature sensor with Arduino. It converts the analog sensor reading to degrees Celsius and prints it.

B QUESTIONNAIRE TEMPLATE: SURVEY ON MOBILE ENVIRONMENTAL SENSORS

B.1 Mobile Ambient Sensors

[General Description]

1. How well do you know these sensors? [a Table with a list of sensors in the rows and familiarity level in the columns (I've Never heard of it, I've Heard of it but don't know what this is, I know what this is, but don't know how it works, I know generally how it works, I know very well hos it works) was presented.]

2. How concerned are you about these sensors in relation to your general privacy and security (e.g. if an app or website has access to these sensors, how would you feel)? [a Table with a list of sensors in the rows and concern level (Not concerned, A little concerned, Moderately concerned, Concerned, Extremely concerned) in the columns was presented.]

B.2 Technology Use

[Qs3-10 on the duration of having a smartphone/tablet, type of OS, type and number of apps, type and number of websites and ways of access (mobile, tablet, PC)]

B.3 General Privacy & Security

11. Which types of personal or private information would you be concerned if unauthorised parties have access to? Select all that apply. -Photo -Videos -Audio -Demographic information -Financial information -Passwords -Medical information -Location -Conversations -Touchpad input -User activities/identification -Device unique information

12. Have you personally experienced a privacy or security issue while using any form of computing or mobile technology? -Yes -No

13. 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 authorisation or approval.

-None

-Other

14. Did the events above have a significant impact on your personal or professional life? -Yes -No

15. Have you heard of an anecdotal story from someone else of a security issue occurring that had a significant impact on their life? -Yes -No

16. Rank the types of information and the level of your concern (1-Least concerning, 5-Most concerning) if an unauthorised party received information about you from your mobile devices. [a Table with a list of different types of information (Photos, Videos, Audio recording, Medical information, Passwords, DoB, Phone no., Debit/Credit card number, Location, Conversations, Touchpad input, User activities/identification, Device unique information) in the rows and concern level (1 to 5) in the columns was presented.]

B.4 Protection Preferences

Please read the sensor descriptions before completing this section.

[List of ambient sensors and their functionality in the form of an example was presented here.]

For each of the following questions, choose the option which describes your opinion the best.

17. I will be annoyed if an app or website has access to ambient sensors on my mobile device without my permission (i.e. without explicit input from me). -Strongly disagree -Disagree -Neutral -Agree -Strongly agree

18. I will be annoyed if an app or website has access to ambient sensors on my mobile device without notifying me (i.e. without showing me a message). -Strongly disagree -Disagree -Neutral -Agree -Strongly agree

19. I think every app and website should ask for my permission before having access to ambient sensors on my mobile device. -Strongly disagree -Disagree -Neutral -Agree -Strongly agree

20. I would like **an app** to ask for **my permission** (with explicit input from me) when it has access to the ambient sensors on my mobile device: (Choose as many as apply) [Options:] -Never, -When installing the app, -When opening the app for the first time only, -Each time using the app, -Regular permission requests when using the app

21. I would like **an app** to **notify me only** (without requiring my input) when it has access to the ambient sensors on my mobile device: (Choose as many as apply) [Options:] -Never, -When installing the app, -When opening the app for the first time only, -Each time using the app, -Regular permission requests when using the app

22. I would like **a website** to ask for **my permission** (with explicit input from me) when it has access to the ambient sensors on my mobile device: (Choose as many as apply) [Options:] -Never, -When opening for the first time only, -Each time visiting the website, -Regular permission requests while on the website

23. I would like **a website** to **notify me only** (without requiring my input) when it has access to the ambient sensors on my mobile device: (Choose as many as apply) [Options:] -Never, -When opening for the first time only, -Each time visiting the website, -Regular permission requests while on the website

24. Do you have any more comments about permissions to mobile sensors?

B.5 Mobile Sensors Risks

Please read the sensor descriptions before completing this section.

[The same list of sensors was presented here.]

If mobile sensors (e.g. Bluetooth, GPS, Motion and Ambient sensors) are not used responsibly by apps and websites, some of them can impose some levels of risks to user security and privacy e.g.:

- Location Tracking: using sensor readings to physically locate the device, (instead of using GPS directly).
- Eavesdropping: e.g. recovering speech (when you are speaking, or talking on the phone, etc.) from sensor readings.
- Keystroke Monitoring: inferring user input on a touchpad from sensor reading (e.g.: PINs, passwords, lock patterns).
- User Identifying: inferring individual's patterns and activities e.g. sitting, running, using a train, taking a phone call, etc.
- Device fingerprinting: uniquely identifying a device and profiling users for purposes such as targeted advertising.

For each of the following questions, choose the option which describes your opinion the best.

25. Were you aware of any of these risks? [a Table with a list of risk types in the rows and user prior knowledge of them 1 (not at all), 2, 3 (somewhat), 4, 5 (very well) in the columns was presented.]

26. If chose other, please elaborate:

27. Do you think ambient sensors can contribute to each of the above risks? Choose as many as you think. [a Table with a list of sensors in the rows and a list of risk types in the columns was presented.]

28. Please rate how upset you would be if an ambient sensor data allowed unauthorised parties to access your personal information. [a Table with a list of risk types in the rows and a user feeling levels (1 (Not upset), 2, 3, 4, (Very upset)) in the columns was presented.]

29. How would you feel if an app/website gathered information about you via ambient sensors without asking for permission or showing a notification? Please rate: -1 (Not Upset), -2 -3 -4 -5 (Very upset)

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

31. What would you do if **an app** collected private information about you via ambient sensors? Select all that apply. [Options:] -Switch to a new device, -Turn off sensors, -Not sure, -Deny permission to particular sensor, -Nothing, -Close app, -Uninstall app, -Consider replacing with other apps with no access to sensors, -Consider using a website instead, -Other

32. What would you do if **a website** collected private information about you? Select all that apply: [Options:] -Switch to a new device, -Turn of sensors, -Not sure, -Deny permission to particular sensors, -Nothing, -Close website, -Won't visit website again, -Consider other websites with no access to sensors, -Consider using an app instead, -Other

33. If an app or website that you use frequently (e.g. news, social media, etc.) posed a risk on your privacy, would you discontinue your usage? -Yes -No -Not sure

34. Given the above risks, are concerned of these attacks happening to you? -Yes -No -Not sure

B.6 Protection Preferences (revisited)

Now that you know about ambient sensors and their potential risks, we ask you to answer the questions of page 4 (Protection Preferences) again. As a reminder, sensor descriptions and potential risks are provided here again.

[The same lists of sensors and their risks as A5 were presented here.]

35-41. [Questions 17-23 were asked again]

42. I would prefer a smart management system to handle permissions to sensors on my mobile device. -Strongly disagree -Disagree -Neutral -Agree -Strongly agree

43. If agree, why and what would be the features of such a smart system?

44. If disagree, why?

45. Do you have any more comments about permissions to mobile sensors?

B.7 Expectations on notifications

46. How would you like to be notified when you are at risk for a privacy attack? Please rank 1 (Least preferred) to 5 (Most preferred). [a Table with a list of notification methods (Audio, Visual, Tactile, A combination, and None) in the rows and user preference levels (1 (Least preferred), 2, 3, 4, 5 (Most preferred)) was presented.]

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

48. 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.

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

50. What would make the notification annoying?

B.8 Demographics and Thank you