Article

On Transparency and Accountability of Smart Assistants in Smart Cities

Haroon Elahi, Guojun Wang ^{*} , Tao Peng and Jianer Chen

School of Computer Science, Guangzhou University, Guangzhou 510006, China;
haroon.elahi@e.gzhu.edu.cn (H.E.); pengtao_work@163.com (T.P.); jianer@gzhu.edu.cn (J.C.)

* Correspondence: csgjwang@gzhu.edu.cn

Received: 1 November 2019; Accepted: 4 December 2019; Published: 6 December 2019

Abstract: Smart Assistants have rapidly emerged in smartphones, vehicles, and many smart home devices. Establishing comfortable personal spaces in smart cities requires that these smart assistants are transparent in design and implementation—a fundamental trait required for their validation and accountability. In this article, we take the case of Google Assistant (GA), a state-of-the-art smart assistant, and perform its diagnostic analysis from the transparency and accountability perspectives. We compare our discoveries from the analysis of GA with those of four leading smart assistants. We use two online user studies (N = 100 and N = 210) conducted with students from four universities in three countries (China, Italy, and Pakistan) to learn whether risk communication in GA is transparent to its potential users and how it affects them. Our research discovered that GA has unusual permission requirements and sensitive Application Programming Interface (API) usage, and its privacy requirements are not transparent to smartphone users. The findings suggest that this lack of transparency makes the risk assessment and accountability of GA difficult posing risks to establishing private and secure personal spaces in a smart city. Following the separation of concerns principle, we suggest that autonomous bodies should develop standards for the design and development of smart city products and services.

Keywords: smart city; smart assistants; transparency; accountability; privacy; security

1. Introduction

Transparency and traceability of modern computing systems have emerged as the top strategic trends due to the rapid spread of complex smart city technologies, and the issues that they are introducing [1]. This will become even more serious when Artificial Intelligence (AI) based smart solutions involve in all aspects of life in the smart city. Transparency of a smart city system is associated with an appropriate record of its objectives and subsequent implementation and validation [2]. The level of transparency in the design and implementation of such a system can affect developers, end-users, society, experts/regulators, and deployers [3]. It enables end-users to understand the working of the system and thus builds their trust in technology. Developers of a transparent system can find its errors and fix them. Transparency promotes the social acceptability of technology and helps experts and regulators to make sure that the system works as claimed and that it complies with the regulatory frameworks. Finally, deployers of a transparent smart city system have confidence in its fairness and legality. Transparency makes the working of these systems explainable, which is a basic condition for ensuring their accountability [4]. Therefore, transparency errors in the design and implementation of smart city systems and their potential harms to individuals or society need to be identified.

Accountability is the possibility of making someone accountable for what they have done. For example, the privacy and security decisions of users can be influenced, or their data can be

collected stealthily [5,6]. It is accountability that forces those in the data business to operate within the boundaries of regulatory frameworks. Different regulatory frameworks include provisions in this regard. For example, the thus far most comprehensible data protection regulation, the European Union's General Data Protection Regulation (GDPR) lays the principles of "lawfulness, fairness and transparency", "purpose limitation", "data minimization", "accuracy", "storage limitation", and "integrity and confidentiality" and holds data controllers (entities involved in data collection, processing, storage, and use) accountable for demonstrating the compliance with these principles [7]. Data controllers are obliged to set up technical and organizational measures for data and privacy protection of data subjects and may be held accountable for failing to do so. Data controllers are also responsible for demonstrating the effectiveness of such measures.

Transparency and accountability of smart systems play a vital role in the privacy protection of smart city inhabitants. The competing interests of different systems and service providers can motivate them to over-collect user and device data with possibly a severe impact on the privacy of data subjects and the security of smart city systems in a world where "if you torture the data long enough, it will confess to anything" [8,9]. Transparency of these systems and the accountability mechanisms ensure that their users are not tricked, cheated, and violated. Making the details of a computing system transparent to its users lets them make informed privacy and security decisions while choosing the systems and interacting with it [10]. The fear of punitive actions bind system and service providers to comply with the requirements [11–13].

The GDPR particularly emphasizes the transparency and accountability of data collection and processing systems [7]. Recitals 39 and 58 set lawfulness and fairness of data collection and processing conditional to the transparency of data collection, usage, consultation, or otherwise processing (immediate or future) and the extent of processing to the data subjects. GDPR requires that any information and communication relating to the processing of personal data collection should be easily accessible and easy to understand, and conveyed using concise, clear, and understandable language. Even visualization aids should be used, if necessary. According to recital 78 of GDPR, such ease of access, enhanced understanding, and the use of visualization aids is of particular importance "where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising". Recital 100 provides that the purpose of setting such conditions of transparency is to help data subjects "quickly assess the level of data protection of relevant products and services". Article 5 of the GDPR associates transparency with accountability.

Smart Assistants have rapidly emerged in smartphones, vehicles, and many smart home devices. From serving people with special needs in smart homes to solving problems in the classrooms and from assisting in finding directions to entertaining people, they have a variety of uses [14–17]. The most common form of these smart assistants has emerged in smartphones. Hundreds of millions of smartphone devices have been shipped with these smart assistants [18]. It is estimated that, by 2023, there will be 8 billion smart assistants in the world [19]. These smart assistants are taking diverse roles and positions in our lives. Google Assistant (GA) is embedding in phones, speakers, smart display, cars, TVs, laptops, smartwatches, and many more devices [20]. Amazon wants its smart assistant, Alexa, to perceive the lives of people and shape them [21]. The potential impact of smart assistants on the lives of smart city inhabitants reflects in findings of a recent report published by the United Nations Educational, Scientific and Cultural Organization (UNESCO), which says that AI and the digital assistants that it powers are ushering humanity into an era that portends changes as deep, expansive, personal, and long-lasting as those that grew out of the industrial revolution [22].

The modus operandi of these smart assistants, that is, collecting, analyzing, and using data of their users and the nature of assignments that they perform, makes them sensitive from privacy and security point of view. It is the responsibility of developers of these smart assistants to consider the requirements of establishing private and secure user spaces in smart cities. However, recent research discovers

numerous privacy and security issues in these smart assistants, and their design flaws are introducing unforeseen problems in daily life. Vulnerabilities in their underlying mechanisms are found to put the privacy of their users and security of the devices at stake, and their mysterious behaviors are raising trust issues [23–26]. One of the key solutions to addressing these issues can be introducing transparency in data collection behaviors and operations of these smart assistants [27]. However, recent reports question the transparency of how some of these smart assistants work [28]. Nevertheless, there is not much work that investigates transparency issues in smart assistants and studies their impact on the privacy protections of users and the accountability of these systems. Our recent work finds transparency issues in Google Assistant (GA) [29]. However, the primary focus of that work is on identifying privacy and security issues in Android smartphones due to the integration of AI in these devices, where it uses smart assistants as a case study. Therefore, its findings of transparency issues in smart assistants are only secondary.

This work extends our previous research in [29] with the purpose to demonstrate the importance of the role of transparency in the design of smart assistants and find its impact on their accountability and privacy protection of smart city citizens. For this purpose, we take the case of GA, a state-of-the-art smart assistant, and perform its diagnostic analysis to assess the transparency of its risk communication to its potential users and implementation. We use description-to-permissions fidelity and functions-to-API-usage fidelity, two traits important from the transparency and accountability perspectives [30,31]. Further, we use two online user studies to verify how does the transparency of GA affect the privacy protection of its users. We focus on seeking answers to the following questions.

1. *Is GA transparent in its risk communication and implementation?*
2. *How does the transparency of GA affect its accountability?*
3. *How does the transparency of GA affect the privacy protection of its users?*

To get the answers to the first two questions, we performed a diagnostic analysis of GA, and, to find the answer to the third question, we conducted two online user studies (N = 100 and N = 210) with students of four universities in three countries (China, Italy, and Pakistan). The first user study assessed the ability of potential users of GA to understand data access behavior of GA. This understandability is critical for its risk assessment [32]. The second user study focused on investigating the transparency of risk communication by GA to its potential users.

With the purpose to demonstrate the importance of the role of transparency in the design of smart assistants and find its impact on their accountability and privacy protection of smart city citizens, this work makes the following contributions.

1. We performed a diagnostic analysis of GA. We assessed description-to-permissions fidelity and functions-to-API-usage fidelity in GA and compared its discovered traits with those of four leading smart assistants. Our research discovered that GA has unusual permission requirements and sensitive API usage, and its risk communication to potential users and underlying implementation are not transparent, which can affect its potential users and experts in a smart city.
2. We demonstrate that the lack of transparency in GA's implementation makes its risk assessment and validation difficult for experts. It fails many state-of-the-art risk evaluation and malware detection methods and poses threats to check-and-balance and accountability mechanisms in smart cities.
3. We conducted two online user studies (N = 100 and N = 210) with students of four universities in three countries (China, Italy, and Pakistan) to verify whether risk communication in GA is transparent to its potential users, and how it affects their privacy protection. The results of these studies suggest that a lack of transparency in GA's design makes its risk assessment difficult for its potential users. This can adversely affect the privacy protection of these users and may hinder establishing private and secure personal spaces in smart cities.

The rest of this paper organizes as follows. Section 2 contains the related research. Section 3 presents the diagnostic analysis of GA. Section 4 provides details of the two user studies. Section 5 provides the results of this research. Section 6 discusses the different implications of this research. Section 7 discusses different limitations of this work. Section 8 concludes this paper.

2. Related Work

Different researchers have studied the transparency and accountability issues in smart cities and smart city technologies. Privacy and security issues in smart assistants have also been investigated in some studies. This section presents the recent related research.

2.1. Transparency and Accountability in Smart Cities

Recent research identifies that a lack of transparency in the infrastructure facilities and applications in smart cities can introduce security, privacy, and trust issues. Cohen and Money [33] identified eight areas for the implementation of smart city projects. Transparency is one of those eight areas. They proposed that there was an immediate need for establishing transparency standards for smart city products and services. Ferretti et al. [34] proposed that, with the increasing role of Internet of Things (IoT) in smart cities, it was necessary that the working of trusted third parties engaged in the authorization of resources be made transparent for their accountability. Steijn and Niezen [35] proposed that accountability was needed to reduce the barriers to the adoption of cloud-based services. They conducted an online user experiment whose results suggest that accountability was a desired trait, and potential users of cloud services were even ready to pay for accountability tools. Brauneis and Goodman [2] evaluated six predictive algorithms used by public sector organizations. Their evaluation was focused on finding whether citizens could discover what policy judgments selected programs embodied and assess their utility and fairness. They found that all these programs failed to provide meaningful transparency to their end-users, that is, the citizens. Zouave and Marquenie [36] assessed to what extent regulatory frameworks addressed the challenges of transparency and accountability in the systems used by law enforcement agencies for the profiling of criminals in smart cities. They discovered that a lack of shared awareness among authorities, developers, and police users introduced gaps that could affect the judgments made by these systems.

2.2. Transparency and Accountability in Android Apps

In this research, we focus on the Android version of Google Assistant. Therefore, this section introduces the transparency and accountability traits from the perspective of Android apps. Android apps are published mainly through app stores. In the app stores, app providers describe the functions of the app and specify its requirements to access user data and critical device features (in the form of required permissions). Other metadata such as app version, number of downloads, details of the app provider, and user feedback are also shown to app users. Users can compare an app's functions and permissions (Android's tool to protect user data privacy and device security [37]) to assess its benefits and risks and decide whether they should install the app or not [38]. If the app providers are not transparent in communicating app descriptions and data and device feature requirements, they can lure users into installing the apps and affect their privacy and device security.

Different methods are used to validate the working and behaviors of Android apps to prevent them from misbehaving or risking user privacy and device security. Misalignments in their descriptions and permission requirements, unnecessary use of Android permissions and sensitive Application Programming Interfaces (APIs), app collusions, and use of framing effect are some of the known indicators for intrusive apps [31,39–47]. Apps should also put adequate privacy protection and security controls in place [48]. They should fairly use permissions to gain informed user consent and should be transparent in doing so. Failures to demonstrate that a mechanism for obtaining informed user consent is in place, and adequate measures for privacy protection and security are provided can hold the app providers accountable, as provided in GDPR [7].

2.3. Privacy and Security Issues in Smart Assistants

Lau et al. [26] studied the factors affecting people's adoption or rejection of smart speakers, their related privacy concerns, and privacy-seeking behaviors around these devices. They found that a lack of trust towards smart speaker companies was one of the main reasons for non-adoption among non-users. They also found that users of these devices did not understand their privacy risks, rarely used their privacy controls, and the privacy controls in these devices were not well-aligned with user's needs.

Alepis and Patsakis [49] demonstrated that voice-controlled assistants could be easily manipulated while bypassing Android's security mechanisms. They proposed that, while an AI base of these assistants makes them more extensible, it also makes comprehending their full risks difficult. Zhang et al. [50] manipulated skills of Amazon Alexa and Google Home by launching remote, large-scale attacks. They carried out these attacks remotely by publishing attach skills and stole user data and eavesdropped on their conversations. Zhang et al. [51] demonstrated how smart assistants could be exploited to collect user data without their knowledge. They developed a spyware app and disguised it as a popular microphone controller game app. They stealthily recorded incoming and outgoing calls and synthesized Google Assistants keywords. They used Google Smart Assistant to collect environment light and noisy data by exploiting accelerometer, ambient light sensor, and the microphone without being detected by the antivirus systems.

Seymour [52] identified a lack of choice for users and the lack of control over data collections by existing smart assistants as their two main problems. They suggested that not only could these devices collect data from their direct surroundings but also other smart devices in their vicinity. This was demonstrated by Chung et al. [24], who collected data from Amazon Alexa and its enabled devices to characterize the lifestyles and living patterns of its users successfully. Elahi et al. [29] presented a risk analysis of Google Assistant to identify security and privacy concerns of integrating artificial intelligence in Android smartphones. They raised concerns about the transparency in its permission use, and validation.

Despite their wide-scale use and potential role in smart cities, the number of studies addressing privacy and security issues in smart assistants is small. Most of these studies focus on exploiting the abilities of different smart assistants [24,49–51]. Likewise, other studies motivate to further investigate issues in the privacy controls of smart assistants and explore related risks [26,29,52].

3. Diagnostic Analysis of GA

In this section, we present a diagnostic analysis of Google Assistant (GA) from a transparency and accountability point of view. GA is an AI-enabled app available in smartphones, laptops, wearable devices, vehicles, and smart home devices such as smart speakers, smart TVs, and smart displays. Google expects that GA will soon be installed on a billion devices [53]. Indeed, it will appear in most of the smart devices in the smart city [54]. GA engages in two-way communication with its users, senses, or collects data and voice commands and can perform several functions for its users without explicit intervention. The wide-scale support and use of GA and its features make it an exciting product and an attractive case to study. Diagnostic analysis of smart assistants can reveal their vulnerabilities and lead to more trustworthy systems [25].

3.1. Method

To evaluate its design vulnerabilities, we performed a diagnostic analysis of the GA app. The first analysis of apps is performed by the app users who must evaluate apps by reading their descriptions, looking at their data and device feature requirements, and other metadata such as user reviews before installation. After that come the experts, who may consider additional factors such as sensitive API usage by an app in their analyses; therefore, we used description-to-permission fidelity,

description-to-API-usage fidelity, and compared the permission and sensitive API usage of GA with four leading smart assistants, including Alexa, Cortana, Dragon, and Lyra Virtual Assistant.

3.1.1. Description-To-Permissions Fidelity

Description-to-permissions fidelity is an established method to learn an app's behavior. Gorla et al. [30] introduced this method to validate whether the functions of an app conform to its claims. From a user's point of view, whose only chances of evaluating the risks of an app depend on the app information provided on an app store; this method is critical and representative. Such information includes its functional description, rating, reviews, information of the developers, number of downloads, and its permission requirements. However, for this research, we only use app description and its permission requirements as required by the selected method.

3.1.2. Functions-to-API-Usage Fidelity

Android Sensitive APIs are a subset of Android APIs that are governed by the respective Android permissions [30,55]. Thus, they represent the actual implementation and behavior of an app as reflected by its code. Sensitive APIs, as their name suggests, access sensitive information and critical device features in a smartphone. Thus, they can be used to depict the critical behaviors of an app [31,46,56]. We used functions-to-API-usage fidelity to verify transparency of code implementation against the functions of the GA.

3.1.3. Comparison with Leading Smart Assistants

Comparing app behaviors has mainly been used by security researchers to find abnormal or malicious behaviors of Android apps. For example, many works use machine learning algorithms to learn permission use patterns, or the API usage patterns among benign and malicious apps to predict the behavior of new apps [56,57]. We selected four leading smart assistants from the Google Play store for this purpose. A comparison of permission and API usage among these smart assistants with those in GSA would help us identify abnormal behaviors.

3.2. Procedure

We acquired the APK file of GA (version 0.1.187945513) from www.apkpure.com and its description from the Google Play store. We searched for leading smart assistants in the Google Play store and selected Alexa (version 2.2.241878.0), Cortana (version 3.0.0.2376-enus-release), Dragon (version 5.9.2—build 278), and Lyra Virtual Assistant (version 1.2.4). To extract their permissions and verify sensitive API usage, we used Androguard (version 3.1.1), an open source reverse engineering tool [58]. We used Python to write custom scripts for this purpose. To identify the app functions from their descriptions, we used open and axial coding. Coding is the process of manually deciphering and naming interesting concepts found in the data [59]. In open coding, we read the descriptions, obtained from Google Play store, of all the five smart assistants, line-by-line, and assigned functional names to these texts. These functional names constituted open codes. Axial coding serves to refine and differentiate open codes and lends them the status of categories. Thus, we compared the open codes defined in descriptions of all smart assistants and finalized the function names, which are provided in Table 1.

3.3. Findings

In this section, we present the findings of our diagnostic analysis of GA.

Table 1. Functions of the examined smart assistants discovered in their descriptions.

Function	Alexa	Cortana	Dragon	GSA	Lyra
Across Devices	✓	✓	-	✓	✓
Listen Music	✓	-	-	✓	✓
Shopping	✓	-	-	-	-
News Updates	✓	-	-	-	✓
Voice Recognition	✓	✓	✓	✓	✓
Personalization	✓	✓	✓	✓	✓
Calendar Management	✓	✓	✓	✓	-
Calls and Messaging	✓	-	✓	✓	-
Intercom	✓	-	-	-	-
Smart Home Device Mgmt.	✓	-	-	✓	-
Online search	-	✓	✓	✓	✓
Reminders	✓	✓	✓	✓	✓
Notes taking	-	✓	✓	-	✓
Social Media Posts	-	-	✓	-	✓
Send emails	-	-	✓	✓	-
Event Planning	-	-	-	✓	-
Get Directions	-	-	-	✓	✓
Play YouTube Videos	-	-	-	✓	✓
Translation	-	-	-	-	✓
Launch Apps	-	✓	✓	✓	-
Physical Activity Tracking	-	-	-	✓	-

✓ means the presence of the function in a given smart assistant and - shows its absence.

3.4. Description-To-Permissions Fidelity

Performing open and axial coding led us to discover fifteen main functions in the description of GA. These functions are shown in Table 1. These functions show that GA can operate across devices and synchronizes its data for this purpose. Users can ask it to play music, make calls, send messages, send emails, event planning, sending reminders, getting directions, playing YouTube videos, launch different apps, and tracking their physical activities. Further, it can be used to manage smart home devices. It uses voice recognition, calendar events, and across devices to achieve many of these tasks. As given on the play store, it requires only one permission to perform these functions, namely Read Google Services (READ_GSERVICES). Our extraction and review of its permissions from its package file confirmed the same.

3.4.1. Functions-To-API-Usage Fidelity

As shown in Table 1, we discovered fifteen functions from the description of GA, as provided on the Google Play store. We used Androguard reverse engineering tool to discover the usage of related API usage in GA [58]. We searched for APIs used for learning device identity, making calls, text messaging, network information collection, location-based services, streaming services, synchronization, network connectivity, and speech recognition. As shown in Table 2, our experiment discovered the use of only one out of twenty-five targeted APIs. We repeated this test using Ninja Droid 2.0 [60] and ProGuard [61], two Android reverse engineering tools, and found the same results.

Table 2. A comparative overview of API usage in the examined smart assistants

API	Alexa	Cortana	Dragon	GSA	Lyra
getDeviceId	✓	✓	✓	-	-
getSubscriberId	-	-	-	-	-
getCallState	✓	-	-	-	-
getNetworkCountry	-	-	-	-	-
sendTextMessage	-	-	-	-	-
getRequestBody	-	✓	-	-	-
getNetworkInfo	✓	-	-	-	✓
getLastKnownLocation	✓	✓	-	-	-
getLatitude	✓	✓	✓	-	✓
getLongitude	✓	✓	✓	-	✓
getOutputStream	✓	✓	-	-	-
openStream	-	-	-	-	-
sendDataMessage	-	-	-	-	-
setPlaybackStat	✓	-	✓	-	✓
setCallback	✓	✓	✓	-	✓
getAssets	✓	✓	✓	✓	✓
getHost	✓	✓	✓	-	✓
requestSync	-	✓	-	-	-
startSync	-	-	-	-	-
stopSync	-	-	-	-	-
loadUrl	-	✓	✓	-	-
connect	✓	✓	✓	-	✓
getLanguage	✓	✓	✓	-	✓
speak	✓	✓	✓	-	✓
shutdown	✓	✓	✓	-	✓

✓ indicates the usage of a given API by a smart assistant, and - means the absence of its use.

3.4.2. Comparison with Leading Smart Assistants

As apparent from the list of functions provided in Table 1, most of the functions discovered in GA's description are also discovered in the descriptions of other smart assistants. For example, similar to GA, Alexa, Cortana, and Lyra Virtual Assistant operate across devices, and all four evaluated smart assistants use voice recognition and offer personalized services to their users. Similar to GA, users can ask Lyra Virtual Assistant to find directions for them, and it can play YouTube videos for them. Cortana and Dragon can launch apps, and Dragon can send emails, similar to GA. Only physical activity tracking and event planning are additional app features in GA. Nevertheless, there are functions that other smart assistants offer to their users, and GA does not. For example, online shopping, news updates, intercom service, note-taking, social media posting, and translation are functions that one smart assistant offers or another, but GA.

However, as given in Table 3, when we look at the permission requirements of these five smart assistants, GA offers an exceptional case. While Alexa, Cortana, Dragon, and Lyra Virtual assistant require a large number of normal, dangerous, and system or signature permissions that match the functions claimed to be offered by these smart assistants, GA required only one system or signature permission. Likewise, Table 4 provides the Dangerous Permissions required by Alexa, Cortana, Dragon, and Lyra smart assistants to perform functions given in Table 1. GA does not require any Dangerous Permission.

Table 3. A comparison of permission requirements of the selected smart assistants.

App	Normal	Dangerous	System or Signature	Total
Alexa	21	9	26	56
Cortana	29	18	14	61
Dragon	20	18	6	44
GA	0	0	1	1
Lyra	10	16	2	28

Table 4. Dangerous permissions in Alexa, Cortana, Dragon, and Lyra.

App	Dangerous Permissions
Alexa	RECORD_AUDIO, ACCESS_FINE_LOCATION, CAMERA, WRITE_EXTERNAL_STORAGE, READ_EXTERNAL_STORAGE, READ_CONTACTS, CALL_PHONE, SEND_SMS, READ_PHONE_STATE
Cortana	RECORD_AUDIO, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, CALL_PHONE, READ_PHONE_STATE, PROCESS_OUTGOING_CALLS, READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE, CAMERA, SEND_SMS, READ_CONTACTS, WRITE_CALENDAR, READ_CALENDAR, READ_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_MMS, ACCESS_LOCATION_EXTRA_COMMANDS
Dragon	RECORD_AUDIO, READ_PHONE_STATE, WRITE_EXTERNAL_STORAGE, CALL_PHONE, READ_CONTACTS, READ_SMS, SEND_SMS, WRITE_SMS, READ_CALENDAR, WRITE_CALENDAR, RITE_CONTACTS, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_LOCATION_EXTRA_COMMANDS, RECEIVE_SMS, READ_EXTERNAL_STORAGE, READ_CALL_LOG, WRITE_CALL_LOG
Lyra	CALL_PHONE, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, RECORD_AUDIO, READ_PHONE_STATE, READ_CONTACTS, WRITE_CONTACTS, READ_CALENDAR, WRITE_CALENDAR, SEND_SMS, RECEIVE_SMS, READ_SMS, WRITE_SMS, CAMERA, READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE

Table 2 shows the comparative findings of API usage for learning device identity, making calls, text messaging, network information collection, location-based services, streaming services, synchronization, network connectivity, and speech recognition. Again, we find an unusual pattern in GA. Apart from getAssets API use, which provides access to an app's assets, GA does not use any of the standard APIs mentioned in Table 2 and corresponding to functions listed in its description on Google Play store.

4. User Studies

The findings of our diagnostic analysis of GA indicated a lack of transparency. Opinion 02/2013 on apps on smart devices by Article 29 Data Protection Working Party identifies “the lack of transparency and awareness of the types of processing an app may undertake combined with a lack of meaningful consent from end-users before that processing takes place” as the key risks to the data protection of users of smart devices [62]. This indicates that the lack of transparency in risk communication and implementation of GA discovered in our diagnostic analysis could affect the privacy protection of its potential users. Therefore, we conducted two online user studies with students from four universities in three countries. The purpose of conducting these user studies was to know how this lack of transparency would affect the privacy protection of its potential users. Underneath, we provide the details of two user studies, including their design, methods, procedure, and findings.

4.1. User Study 1

Understandability of a system by its users is critical for its risk assessment [32]. For example, risk assessment affects the privacy management decisions of smartphone users [44]. Understandability of an Android app by its users can be reflected in their understanding of its functions and data access requirements [30]. Therefore, assessing the ability of smartphone users to understand and relate GA description and permission requirements would reveal whether the information provided on the

Play Store could help them determine whether to install this app or not. Accordingly, the first user study intended to verify whether potential GA users could understand its description and permission requirements, as provided on the Google Play Store, and relate them.

4.1.1. Design

Android Applications are typically distributed through app stores, and users download them to meet different needs [63]. The responsibility of assessing an app's risk lies in the users [44]. At this stage, app stores present app descriptions and their permission requirements to potential app users. These users are supposed to read and understand the descriptions of an app and review its permission requirements to decide whether to select and install a particular app or not [64]. Users install an app only when its perceived benefits exceed perceived risks [65]. Thus, the download stage becomes the first line of defense for users to protect their privacy by weeding out privacy-intrusive apps [66].

Since manipulation of information presented to app users in app stores can affect user privacy and device security, regulations such as GDPR require app providers to take into consideration user expectations [7]. Therefore, we can reasonably assume that a privacy respecting app provider shall take into consideration user expectations. Such behaviors of app providers can be assessed by determining whether app behaviors are within user expectations. Moreover, user expectations can be assessed via their perception in combination with their judgment while reading app descriptions and reviewing its permission requirements for making choices at the download stage [67,68]. A gap between users' expectations and actual data access by an app indicates the possibility of misuse of access to sensitive data [69].

Therefore, we designed an online user experiment to measure the users' expectations regarding the data access needs of GA by reviewing its description. We compared user expectations with actual GA permission requirements to determine the gap in expected versus actual data access requirements (permissions). The first user study was conducted to seek an answer to the following question.

1. *Do GA permission requirements match user expectations?*

We designed an online user survey to collect data from smartphone users. We collected these data anonymously. The purpose of data collection was clearly conveyed to the data subjects. Participation in the study was voluntary. Since no sensitive data collections were involved in this study, and all the potential participants were adults, the study did not need ethical approval.

4.1.2. Method

In this section, we provide the details of the survey content, the method to disseminate the survey, and the sample information.

Survey Content

We collected GA description from the Google Play Store and anonymized it by replacing "Google Assistant" with "smart app". No other changes were made in the description. Further, we prepared a list of permissions by considering the functions in GA description and consulting Android online documentation [37]. We also looked at the permission requirements of the four smart assistants that offer similar functions and whom we used for comparison with GA. Participants were asked to read the description of the app and select the permissions that they perceived could be required to perform the functions given in the description. The details are provided in Appendix A.1.

In demographic information, we asked respondents for their age, gender, smartphone type, and the number of apps that they had installed on their smartphones. The number of app installations was asked to confirm that they had gone through the process involved in app selection, that is, reviewing app descriptions and their permission requirements.

Survey Method

We used Google Forms to set up an online survey questionnaire. We shared it in the WeChat group of international and exchange students at Guangzhou University. WeChat is a popular social media app widely used in China that allows setting up user groups for social interactions and information exchange. Guangzhou University has set up a WeChat group of international and exchange students that was used to circulate the questionnaire. The group had 187 members at the time of conducting this study. Due to the slow response, we needed to send multiple reminders to the group members.

Sample Information

The sample of this study consisted of 187 adult smartphone users. Since we intended to target the users of Google's products and services, we did not collect data from locals. Rather we circulated this survey among the international and exchange students at Guangzhou University. These students included bachelor, master, and Ph.D. students at Guangzhou University and exchange students from Padua University, Italy.

4.1.3. Results

In this section, we present the results of this user study.

Demographics

We received 100 responses. There were 34 female and 66 male respondents. The average age of the respondents was 28.2 years ranging between 18 and 61 years of age and with a standard deviation value of 7.7. Participants hailed from 10 different countries. There were 73 Android users, 23 iPhone users, and 4 users of other smartphones. Forty percent of the respondents had installed between 10 and 20 apps on their smartphones, 30 percent had installed between 20 and 30 apps, and another 30 percent had installed more than 30 apps.

Findings

The purpose of conducting this study was to verify whether respondents could understand GA's description and permission requirements and relate them. The responses showed that none of the respondents could relate the description with the actual permission requirements of GA.

4.1.4. Analysis

The purpose of data collection was to observe user decisions for learning their permission expectations against given functions. These data would help us determine the gap among user expectations and the actual permission requirements of GA. We determined this gap by analyzing the responses to learn their similarities with the permission requirements of GA. To achieve this, we calculated Jaccard similarity among the responses and the actual permission requirements of GA. Jaccard similarity has been used in research addressing decision-making issues, and discovering harmful behaviors of Android apps [70–72]. Measuring the Jaccard similarity coefficient j between two datasets A and B is the result of the division between the number of features that are common to all divided by the total number of properties [73]. The values of the Jaccard Similarity Index lie between one and zero. A value of one depicts maximum similarity, and zero depicts an absence of similarity. Figure 1 shows the distribution of the Jaccard Similarity Index values for the responses of 73 Android users. It can be seen that the permission requirement expectations of about 40% of the respondents mismatch the actual requirements of the GA. For the rest of the respondents, there is a partial similarity. However, this similarity is negligible.

$$j(A, B) = \frac{A \cap B}{A \cup B}$$

A better view of the results can be understood by calculating the dissimilarity. The dissimilarity can be calculated as follows. The values of the Jaccard Dissimilarity Index lie between one and zero. One depicts maximum dissimilarity, and zero depicts no dissimilarity.

$$\text{Jaccard dissimilarity} = 1 - j(A, B)$$

Figure 2 shows the dissimilarity of user choices from the actual GA permission requirements. It shows an obvious gap between user expectations and actual GA permission requirements.

Figure 1. Distribution of Jaccard Similarity Index values for responses of 73 Android users.

Figure 2. Jaccard Dissimilarity Index values for responses of 73 Android users show an obvious gap between expected and actual permission requirements of GA.

We also calculated Jaccard similarity and dissimilarity index values for the responses of iPhone and other smartphone users to see whether there was any difference among the responses of Android

users and non-users. Figure 3 shows the distribution of Jaccard Dissimilarity Index values, and Figure 4 shows that there is an obvious gap between the expected and actual permission requirements of GA even in the case of Android non-users.

Figure 3. Distribution of Jaccard Similarity Index values for responses of 27 non-Android users.

Figure 4. Jaccard Dissimilarity Index values for responses of 27 non-Android users show an obvious gap between expected and actual permission requirements of GA.

We performed a paired-sample t-test to verify whether there was a significant difference among the responses of Android users and non-users. At 95% Confidence Interval of the difference, we got a significance value of 0.110, which means that there was no significant difference among the responses of Android users and non-users. The same test was performed for the responses of male and female respondents. At 95% Confidence Interval of the difference, we obtained a significance value of 0.7, which means that there was no significant difference among the responses of male and female smartphone

users. Further, we calculated correlation among the age and the similarity of responses to the actual permission requirements of GA, which returned a value of -0.087 that shows an absence of correlation among age and the responses.

4.2. User Study 2

The use of permissions in Android applications is the means to obtain the consent of app users before these apps access user data and sensitive device features. A lack of transparency is closely related to a lack of informed consent [62]. To meet the requirements of informed consent, it is the responsibility of app providers (in this case, Google) to convey the risks of their apps to potential users in an unambiguous manner. GDPR makes it mandatory for data controllers to use plain and understandable language in communication of risks to app users [7]. Therefore, we conducted a second user study to learn whether Android users could perceive the risks of GA through its permission requirements.

4.2.1. Design

Risks in Android smartphones emerge mainly from an app's requirement to access user data in and critical device features, which can, in turn, generate sensitive data. Android uses a permission mechanism to protect user data and device security [37]. These permissions have different sensitivity levels according to the nature of data or device features that they protect. App permissions are central to many risk evaluation models. For example, the authors of [39,44–46] used app permissions to determine its access to sensitive user data and critical device features for calculating app risks. As Android uses a privacy self-management model and users grant or deny different permissions to an app after evaluating the costs and benefits of a function that the app is offering, users are supposed to be familiar with the sensitivity of different permissions [64].

As mentioned above, it is the responsibility of app providers to convey the risks of apps to their potential users. Since permissions provide the basis for risk evaluation of apps and informed consent, we wanted to know whether Google has done its job in the case of GA or not. We designed an online user study to seek an answer to the following question.

1. *Does Google transparently convey the risks of GA to its potential users?*

We collected the data anonymously. The purpose of data collection was clearly conveyed to the data subjects. The participation in the study was voluntary, and users were free to leave the study if they desired to do so. Since no sensitive data collections were involved in this study, and all the potential participants were adults, the study did not need ethical approval.

4.2.2. Method

In this section, we provide the details of the survey content, the method to disseminate the survey, and the sample information.

Survey Content

The purpose of conducting this user study was to learn whether Google clearly conveys the risks of GA to its potential users. It can be learned by assessing whether Android users are aware of the sensitive nature of the permission used by GA. As mentioned above, Android defines different sensitivity levels for the permissions according to the nature of data and device resources that they protect. Consequently, there are four levels of sensitivity. Normal permissions are considered harmless for user privacy and device security. App developers use signature permissions for protecting Inter-component communication. Dangerous permissions protect private user data and critical device resources. The survey content is provided in Appendix A.2.

Furthermore, users can have different perceptions of sensitivity associated with different types of data and resources [60]. Their privacy decisions can be affected by their sensitivity perceptions

regarding different permissions. We selected six sensitive permissions, namely Authenticate Accounts, Camera, Read Contacts, Read Google Services, Read SMS, and Send SMS, and asked respondents to select the most sensitive permission. Previous research shows that users perceive app access to the camera, contact list, and SMS sensitive [74]. We added Authenticate Accounts and Read Google Services, two less obviously dangerous permissions in this list. We also gave them an option “I do not know”, in case if they did not understand Android permissions.

Method

We used Google forms to set up an online questionnaire. The survey was circulated in four different master and bachelor classes in two public sector universities in Pakistan.

Sample Information

The sample of this study consisted of 212 adult smartphone users. Since we intended to target the users of Google’s products and services, we did not collect data in China. The sample of this study included 140 undergraduate and 72 graduate students from two public sector universities in Pakistan. There were 72 students of MSc. physics, 100 (50 + 50) computer science students, and 40 electrical engineering students.

4.2.3. Results

In this section, we provide the findings of our study based on our data collection.

Demographics

A total of 210 respondents participated in this study. There were 131 females and 78 males. One respondent preferred not to reveal their gender. The ages of the participants ranged between 19 and 37, with an average age of 22 years and a standard deviation value of 2.5. Out of 210 respondents, 193 were Android phone users and 17 respondents used iPhones or other smartphones. On average, respondents have been using smartphones for two and a half years with a standard deviation value of 2.2.

4.2.4. Findings

We had asked users to select the most sensitive permission among the given dangerous permissions. Respondents also had an option to select “I do not know” option in case they did not know the answer to the question asked. Figure 5 shows a distribution of responses by 193 Android users who took part in our study.

Figure 5. Distribution of responses of 193 Android users.

4.2.5. Analysis

The purpose of this study was to find whether smartphone users were aware of the risks of the permission used by Google Assistant, that is, Read Google Services. Because this permission is specific to Android applications, we only considered the responses of Android users. As our findings show, only 6% of the respondents chose Read Google Services as the most sensitive permission among the given dangerous permissions. As shown in Table 5, 3% percent of female and 10% of male respondents considered the permission used by GA as the most sensitive permission. It means that 97% of female and 90% of male respondents to our study do not treat it as a sensitive permission when compared with other permissions offered to them. Therefore, we can infer that most of the respondents of this study were not aware of the risks of this permission. However, at the same time, an alarming finding was that 42% (46% of females and 31% of males) of the respondents chose “I do not know”, which indicates that these respondents were not aware of the risks associated with the given Android permissions.

Table 5. Percentage Response Distributions for Female and Male Respondents

Choice	Female	Male
Authenticate Accounts	31	28
Camera	10	12
Read Contacts	1	9
Read Google Services	3	10
Read SMS	3	6
Send SMS	3	3
I Don't Know	46	31
No Response	3	1

Figure 6 shows the percentage distribution of responses according to the educational background of 193 Android users who participated in the second user study. The distribution of responses shows that 9% of computer science students chose Read Google Services as the most sensitive permission. This fell to 4% for physics students, and 0% of the engineering students selected it as the most sensitive permission. At the same time, 47% of physics students acknowledged that they did not know which permission was the most sensitive one, while 42% of computer science and 30% of engineering students acknowledged the same.

Figure 6. Percentage distribution of responses according to educational background of 193 Android users.

5. Results

With the purpose to demonstrate the importance of the role of transparency in the design of smart assistants and find its impact on their accountability and privacy protection of smart city citizens, this research was conducted to find answers to the following questions.

1. *Is GA transparent in its risk communication and implementation?*
2. *How does the transparency of GA affect its accountability?*
3. *How does the transparency of GA affect the privacy protection of its users?*

In this section, we report the answers to these questions in light of the findings of our research.

Question 1: Is GA transparent in its risk communication and implementation?

Answer: Looking at the findings of our diagnostic analysis of the GA app for verifying its description-to-permissions fidelity and description-to-API-usage fidelity, it is discovered that GA does not conform to both these tests. Neither do its permission requirements correspond to its description shown to its users in the Google Play store nor does its API usage reflects its functions discovered in its description. Table 4 shows the dangerous permissions in Alexa, Cortana, Dragon, and Lyra Virtual Assistant. It is easy to map their demands for dangerous permissions with their functions given in Table 1. This is the transparency that is expected from permission use in Android apps. However, in the case of GA, its permission demands cannot be mapped with its functions.

Question 2: How does the transparency of GA affect its accountability?

Answer: Transparency of a system provides explainability, which is particularly important for its validation and, therefore, accountability [4]. The lack of transparency makes the assessment of the harmful effects of a system difficult [32]. As mentioned in the Introduction, there are many state-of-the-art risk evaluation models that use an app's description, its permissions, and API usage to assess its risks. However, as the results of our analysis show, a lack of transparency in the design and implementation of GA leads to an absence of explainability, which makes many risk evaluation models ineffective and affects its validation. This form of design can severely affect the check and balance system in smart cities.

Question 3: How does the transparency of GA affect the privacy protection of its users?

Answer: Our two user studies verified that the nonconformance of description-to-permissions fidelity could affect its potential users from knowing its risks. The first user study confirmed a gap between the expected and actual permission requirements of GA, and the results of the second user study suggested that users did not know the sensitive nature of this particular permission. These results suggest that Google Assistant does not convey its risks to its potential users transparently, which can make its risk evaluation difficult for its potential users.

6. Discussion

In smart cities, whose architectural technologies will be involved in collecting, analyzing, and using data for their operations, new privacy and security challenges will arise [75–78]. Transparency in the design, implementation, and operations of smart city products can ensure establishing private and secure personal spaces for the citizens by enabling their validation and accountability. This becomes especially sensitive when the products in question serve the needs of hundreds of millions of users across borders and even of those who are vulnerable.

Previous research identifies a lack in the transparency of operations of predictive algorithms used in some smart city infrastructures [2,36]. However, their impact is limited to the cities where these systems operate. Likewise, different works identify security and privacy issues in smart assistants [26,27,50,51]. Nevertheless, previous works on the privacy and security of smart assistants focus on vulnerabilities in their implementation. Current work contributes to the research on the transparency of smart city products and smart assistants. It identifies a lack of transparency in the risk communication of a state-of-the-art smart assistant and its implementation through diagnostic analysis. It explains the implications of this lack of transparency from an accountability perspective

and for the privacy protection of its potential users, i.e., the smart city inhabitants, through two user studies conducted with students of four universities in three countries.

The findings of this research become particularly important since the use of smart assistants is on the rise in smart cities [18,19]. In addition to general-purpose smart assistants, special-purpose smart assistants are increasingly being designed to be used by people with special needs, in the classrooms, and for the elderly [14,15]. Moreover, the number of minors using smartphones is increasing and introducing different issues [79,80]. Because most of the popular smart assistants have smartphone versions, we can imply that minors will use a large number of generic (e.g., GA) and special-purpose smart assistants (e.g., educational smart assistants). Consequently, the responsibility of risk assessment and management of these products falls on experts, designers, developers, and regulatory bodies.

Towards this end, as mentioned in above, GDPR requires data controllers to transparently communicate the risks of their products and services to users. Considering the case of GA, Google has provided a list of permissions and described their role in data and feature protection in Android phones; Read Google Service (READ_GSERVICES) is not on that list [37]. The only information available on this permission says that it lets an app read the configuration of Google services [81]. However, this explanation comes from an unofficial source and sheds no light on the nature and scope of this permission. We infer that Google has failed to transparently communicate the risks of this particular permission to the users of GA. The lack of transparency in risk communication is supposed to affect the privacy protection of the users of this smart assistant. The results of our user studies confirm that the respondents failed to perceive the risks of GA, which validates a failure on the part to Google to convey risks of this product effectively to its potential users. Since risk communication is a fundamental condition for informed consent [82], a question mark can be put on the validity of consent gained using means such as the undocumented permission in GA. The legality and fairness of operations of this smart assistant should also be assessed. However, we leave this to legal experts and researchers.

As the results of this research suggest, a lack of transparency in the implementation of GA leads to the lack of explainability and therefore affects its validation and accountability. We observe that many risk evaluation models turn ineffective in this regard. For example, one recently published work [44] proposes a risk evaluation model for Android apps that calculates a threat score for the app based on its requested permissions. It calculates the different types of threat scores, including privacy, systems, and financial threat scores. All these scores are based on the requested permissions. For example, for calculating privacy threat score, it assigns limited threat to permissions such as ACCESS_COARSE_LOCATION, a significant threat to permissions with serious privacy consequences (e.g., WRITE_SOCIAL_STREAM), the relevant threat to permissions such as ACCESS_FINE_LOCATION, and the maximum threat to permissions which may have an effect on the privacy of device and its user. System and financial threats are also calculated using different permissions. If we use this model to evaluate the risks of GA, it will generate entirely inaccurate threat scores. The same is true for other risk evaluation models using app permissions or API usage. The same goes for tools such as MalPat [56] and DASAPA [83], and the approaches proposed in [84,85]. This is an alarming situation and seeks immediate attention from the research community and regulatory bodies.

Further, GDPR requires that the implementation of privacy controls should be technology-neutral. However, the results of our research show that, in the case of GA, both its permission requirements and its underlying implementation turn it into a black box for end-users and experts, affecting its risk assessment and validation and, therefore, accountability. We understand that, despite the limited AI features of GA, the current set of Android permissions did not serve its operational requirements, which led Google to use more powerful permission. This demonstrates that current Android permissions will not serve the privacy protection and security needs of Android users in the smart city. This offers new challenges for privacy protection tools in Android. We propose that other privacy protection mechanisms should also be evaluated to verify whether they serve the needs of technologies that will prevail in smart cities.

Overall, we believe that smart assistants will assume important roles in the lives of smart city inhabitants. Many other smart city products with similar capabilities will emerge, and transparency in their data collection behaviors will be a trait needed for ensuring the privacy protection of smart city citizens [27]. This research shows how deviation from de facto app design and permission use in GA introduced transparency and validation issues affecting the privacy protection of smart city citizens and the accountability of this smart assistant. We understand Google's ability to make such drastic changes is associated with its role in controlling Android that allows it to do things that no other stakeholders can do. Previous instances confirm this tendency. For example, Google can collect user data while bypassing the apparent security and privacy architecture in Android [86]. Google is also known to influence Android phone manufacturers for including its browser app in their devices for its advantage [12]. There are also cases in which Google denied providing timely fixes after learning vulnerabilities in the Android security mechanism [87]. Therefore, we understand that the security and privacy of smart city products and citizens cannot be left to the entities whose interests conflict with those of data subjects, especially when they are known to have an urge to change the current privacy architecture [9,88].

Congruent with the recommendations of Ferretti et al. [34], we suggest that product developers in the smart city should be made accountable for issues such as a lack of transparency in their products. Further, Cohen and Money [33] identified the need to establish standard specifications for smart city infrastructure at a broader level. Notably, product level standards and specifications are mostly missing. We believe that there is an urgent need to develop standards for designing all smart city products, including smart assistants. A failure to do so will result in encountering issues more severe than those identified in [2,17], and this work. We insist that these standards should be developed by autonomous bodies and not by the entities whose interests lie in the related business. Moreover, as suggested by Zouave and Marquenie [36] and Dilawar et al. [77], all stakeholders of the smart city products should be involved while developing these standards.

7. Limitations

In this paper, we focus on transparency issues in smart assistants and explore their impact on the privacy protection of smart city inhabitants and the accountability of these products. In this regard, we take the example of GA—a state-of-the-art smart assistant and perform its diagnostic analysis. We followed the standard method to learn the expectations of Android users and compared them with the actual permission requirements of GA and also recorded their related risk perceptions. The decisions and choices of Android users while evaluating an app are influenced by the information offered to them and their privacy awareness and skills [62]. However, the role of the offered information cannot be ignored [64]. Moreover, it is known that user decisions while reading app descriptions and reviewing its permission requirements for making choices at the download stage represent their expectations [67,68].

It is also important to note that our analysis does not evaluate the post-installation behaviors of GA. Future research can assess the post-installation behaviors and operations of GA from a transparency point of view. Moreover, transparency of risk communication also influences trust [62]. The impact of the lack of transparency in risk communication by GA to its potential users on their trust can also be an interesting area for future research.

Moreover, we assessed the Android Sensitive API usage in GA for its validation and accountability, treating it as an independent app. Using Android Sensitive APIs to evaluate underlying implementations of an app is a widely-used approach [46,56,89]. However, its more thorough analysis can reveal its behaviors such as whether it colludes with other apps installed on Android smartphones. If it colludes with other apps installed on an Android smartphone, its ethical implications need to be assessed. Its behavior on devices other than smartphones should also be investigated. Finally, transparency issues in other smart assistants and their impact on the lives of smart city inhabitants also need to be assessed.

In the case of user studies, we used web-based surveys, which are believed to be cost-effective and speedy and can generate large samples [90]. However, User Study 1 had a lower response rate (53%). We believe that it was due to two reasons. (1) The access to Google Forms was restricted (based on our observation, we had assumed that international students had means to access Google Forms). (2) It asked a difficult question, that is, relating app description to the required permissions. A need to consider app description and given permissions concurrently to establish a relationship makes it difficult from a problem-solving perspective [91]. However, this is exactly what is expected from a smartphone user in the privacy self-management model followed in Android devices [38,92]. In User Study 2, we followed a controlled approach and obtained a better response rate (99%). Likewise, such studies cannot create a user experience equivalent to the real situations encountered by users while installing apps. However, they are a useful tool to measure estimates. Our results can help developers of smart city products who “end up designing applications either based on their assumptions on user privacy expectations or relating to their own expectations of privacy as a user” [93].

Further, the participants in this study were university students, and their ages varied, particularly in the first user study. Previous research shows that younger users of technology are comparatively more privacy-aware, and university education also increases privacy concerns [94]. Thus, the sample of this study could have introduced a bias in the research where increased privacy awareness and skills of the participants would lead to positive results. However, our findings indicate no correlation between age and responses in the first user study. Likewise, despite having higher education, the participants failed to generate responses that could be considered favoring the results of this research. Overall, all of them were smartphone users and therefore constituted a representative sample.

8. Conclusions

Smart assistants are emerging at a fast pace and assuming different roles in the lives of smart city citizens. Similar to other smart city products and services, they collect, analyze, process, and use data, including personal data of smart city citizens for their operations. Making sure that these products do not threaten the privacy and security of their users becomes the responsibility of those designing and developing these smart assistants and putting them to work. It is the transparency in their design, implementation, and operations that enables their risk assessment, validation, and accountability. However, this research shows that those supposedly responsible for ensuring the privacy and security of smart city citizens and products may violate conditions such as transparency for their interests. Our diagnostic analysis of GA discovered a lack of transparency in its risk communication to its potential users and its sensitive API usage. Our two user studies (N = 100 and N = 210), conducted with students of four universities in three countries, verified a negative impact of the lack of risk communication on the privacy protection ability of its potential users. Further, we explained how its lack of transparency in risk communication and implementation makes its accountability difficult, making many risk assessment models and malicious application detection systems ineffective. These findings endorse the importance of transparency in the design and implementation of smart city products and indicate a need to set up standards and specifications for smart city products, which should be developed by autonomous bodies with the participation of all stakeholders.

Author Contributions: Conceptualization, H.E.; methodology, H.E.; validation, G.W. and J.C.; formal analysis, H.E.; investigation, H.E.; resources, G.W.; data curation, H.E.; writing—original draft preparation, H.E.; writing—review and editing, G.W. and T.P.; supervision, G.W.; project administration, J.C.; and funding acquisition, G.W., T.P., and J.C.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grants 61632009, 61802076 and 61872097; in part by the Guangdong Provincial Natural Science Foundation under Grant 2017A030308006; and in part by the High-Level Talents Program of Higher Education in Guangdong Province under Grant 2016ZJ01.

Acknowledgments: We want to thank M. Naeem Shehzad (Assistant Professor, E.E., COMSATS University Islamabad, Lahore Campus, Lahore, Pakistan) and Saqib Ali (Assistant Professor C.S., University of Agriculture, Faisalabad, Pakistan) for their support in collecting data for our User Study 2.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Appendix A.1

Introduction: We install new Apps on our smartphones for improved experience and for making the best use of our smartphone devices. While installing Apps, we are informed of the permissions that an application needs to perform its functions smoothly. These permissions determine the data and resources on our device that this application will be able to access and utilize. Thus it directly affects our privacy. In this survey, we offer you a smart assistant application and mention the permissions that it may require. Please look at the functions that we offer you, review given permissions, and select the permissions that you think are necessary for these functions.

(Note: This survey is solely for research purposes, and we sincerely thank you for sparing time and for your participation).

Demographics and Background

Gender

1. *Male*
2. *Female*
3. *Prefer not to say*

Age (in years)

Smartphone type

1. *Android*
2. *iPhone*
3. *Other*

Country

Smart Assistant Description Smart Assistant Functions—Make us do it for you. Your Intelligent Assistant can help with the little things like setting an alarm or playing your favourite music, or the big things like planning a special occasion. Just ask your Assistant and make us do it. You can easily access your Intelligent Assistant by holding the Home button on your phone or by simply saying, “Ok Boy”. Your Intelligent Assistant also syncs to your other devices including Smart Home devices like smart TVs, laptops, and more. Get things done easily The Intelligent Assistant is your personal assistant and time management tool. Quickly check your inbox, keep track of your to-do lists, and set reminders and alarms. Make calendar events (“Add dinner with Charlie tomorrow at 7 p.m. to my calendar.”)? Set reminders (“Remind me to buy a birthday gift for Jane”)? Set alarms (“Set an alarm for 7 a.m.”) Do more with your commute Whether you’re driving, biking, or walking, use your Google Assistant to navigate and stay in touch. Make hands-free phone calls (“Call Mum”)? Send text messages (“Text Sara I am running late”)? Get directions (“Navigate to Hyde Park by tube”) Stay in the know Love news, arts, and culture? Your Intelligent Assistant can keep you updated on the latest headlines and sports scores, or offer translations in over 100 languages. Receive the latest news updates (“Tell me today’s news”)? Get the local weather forecast (“Do I need an umbrella today”)? Get answers (“Translate ‘where is the nearest bus stop’ in Spanish”) Control your phone and home hands-free Play music, watch your favourite shows, dim your lights, and more. Google Assistant syncs with your Smart Home, Chromecast, and other devices. Play music (“Play my Relaxed Morning playlist”)? Enjoy your favourite entertainment at home (“Play trending YouTube videos on my TV”)? Adjust your home to the way you like it (“Dim the lights in the living room”)

Table A1. List of possibly needed permissions.

Access Bluetooth Settings	Draw Over Other Apps	Read your Contacts
Access Precise Location	Find Accounts on the Device	Receive Data from Internet
Add or Remove Accounts	Find Contacts on the Device	Record Audio
Approximate Location	Full Network Access	Retrieve Running Apps
Change Network Connectivity	Interact Across Users	Run at Startup
Change Your Audio Settings	Modify or Delete the Contents of Your USB Storage	Send SMS Messages
Connect and Disconnect from Wi-Fi	Pair with Bluetooth Devices	Take Pictures and Videos
Control Vibration	Power Device On or Off	Use Accounts on the Device
Create Accounts and Set Passwords	Prevent Device from Sleeping	View Network Connections
Device & App History	Read Google Services	View Wi-Fi Connections
Directly Call Phone Numbers	Read Phone Status and Identity	
Disable Your Screen Lock	Read the Contents of Your USB Storage	

Appendix A.2

Introduction: Thanks for taking part in this user survey. The purpose of conducting this survey is purely academic and the collected data will only be used for academic research. This participation is consensual and you are free to quit if you do not want to share your opinion.

Demographics and Background

Gender

1. *Male*
2. *Female*
3. *Prefer not to say*

Age (in years)

Smartphone type

1. *Android*
2. *iPhone*
3. *Other*

How long have you been using smartphone (in years)?

Question: Android Permissions help us control the access of different apps to our data and critical device resources. Please go through the following Permissions and select the most sensitive Permission.

1. *Authenticate Accounts*
2. *Camera*
3. *Read Contacts*
4. *Read Google Services*
5. *Read SMS*
6. *Send SMS*
7. *I Don't Know*
8. *No Response*

References

1. Panetta, K. Gartner Top 10 Strategic Technology Trends for 2020. Gartner.com. 2019. Available online: <https://tinyurl.com/y3meckzs> (accessed on 22 October 2019).
2. Brauneis, R.; Goodman, E.P. Algorithmic Transparency for the Smart City. *SSRN Electron. J.* **2017**, *103*, 103–176. [CrossRef]
3. Felzmann, H.; Fosch-Villaronga, E.; Lutz, C.; Tamo-Larrieux, A. Robots and Transparency: The Multiple Dimensions of Transparency in the Context of Robot Technologies. *IEEE Robot. Autom. Mag.* **2019**, *26*, 71–78. [CrossRef]

4. Association for Computing Machinery US Public Policy Council (USACM). *Statement on Algorithmic Transparency and Accountability*; USACM Press: Washington, DC, USA, 2017; pp. 1–2.
5. Adjerd, I.; Acquisti, A.; Brandimarte, L.; Loewenstein, G. Sleights of privacy. In Proceedings of the Ninth Symposium on Usable Privacy and Security—SOUPS '13, Newcastle, UK, 24–26 July 2013; p. 1.
6. Gibbs, S. Google has been tracking Android users even with location services turned off. *The Guardian*, 22 November 2017.
7. The European Parliament and the Council of the European Union, Regulation (EU) 2016/679 (GDPR). *Off. J. Eur. Union* **2016**, L119, 1–88.
8. Kathuria, V. Greed for data and exclusionary conduct in data-driven markets. *Comput. Law Secur. Rev.* **2019**, *35*, 89–102. [CrossRef]
9. Zuboff, S. Big other: Surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* **2015**, *30*, 75–89. [CrossRef]
10. Rode, J.; Johansson, C.; DiGioia, P.; Silva Filho, R.; Nies, K.; Nguyen, D.; Ren, J.; Dourish, P.; Redmiles, D. Seeing further: Extending visualization as a basis for usable security. In Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 12–14 July 2006; pp. 145–155.
11. Hern, A. Google fined Record £44m by French Data Protection Watchdog. *The Guardian* (International Edition), 2019. Available online: <https://tinyurl.com/ybbgojxg> (accessed on 23 January 2019).
12. Antitrust: Commission fines Google 4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine. Press Release, 2018. Available online: http://europa.eu/rapid/press-release_IP-18-4581_en.htm (accessed on 5 August 2018).
13. Jee, C. *Facebook Is Set to Pay a Multibillion-Dollar Fine to Settle a US Privacy Probe*; MIT Press: Cambridge, MA, USA, 2019.
14. De Oliveira, G.A.A.; Bettio, R.W.D.; Freire, A.P. Accessibility of the smart home for users with visual disabilities. In Proceedings of the 15th Brazilian Symposium on Human Factors in Computer Systems—IHC '16, São Paulo, Brazil, 4–7 October 2016; Volume Part F1280, pp. 1–10.
15. Winkler, R.; Söllner, M.; Neuweiler, M.L.; Rossini, F.C.; Leimeister, J.M. Alexa, Can You Help Us Solve This Problem? In Proceedings of the Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems—CHI EA '19, Glasgow, Scotland, 4–9 May 2019; pp. 1–6.
16. Bentley, F.; Luvogt, C.; Silverman, M.; Wirasinghe, R.; White, B.; Lottridge, D. Understanding the Long-Term Use of Smart Speaker Assistants. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 1–24. [CrossRef]
17. Macfarlane, J. When apps rule the road: The proliferation of navigation apps is causing traffic chaos. It's time to restore order. *IEEE Spectr.* **2019**, *56*, 22–27. [CrossRef]
18. Udin, E. China's Smart Assistant Will Reach 5.8 Billion Units in 2023. 2019. Available online: <https://tinyurl.com/yy5z68t2> (accessed on 20 October 2019).
19. Sarah, P. Report: Voice Assistants in Use to Triple to 8 Billion by 2023. 2019. Available online: <https://tinyurl.com/y2takllq> (accessed on 27 November 2019).
20. Google Assistant. 2019. Available online: <https://assistant.google.com> (accessed on 27 November 2019).
21. Karen, H. Inside Amazon's Plan for Alexa to Run Your Entire Life. MIT Technology Review, November 2019. Available online: <https://tinyurl.com/yytqpb2n> (accessed on 5 November 2019).
22. UNESCO and EQUALS Skills Coalition. *I'd Blush If I Could: Closing Gender Divides in Digital Skills through Education*; United Nations Educational, Scientific and Cultural Organization: London, UK, 2019; Available online: <https://en.unesco.org/Id-blush-if-I-could> (accessed on 10 June 2019).
23. Politou, E.; Alepis, E.; Patsakis, C. A survey on mobile affective computing. *Comput. Sci. Rev.* **2017**, *25*, 79–100. [CrossRef]
24. Chung, H.; Lee, S. *Intelligent Virtual Assistant knows Your Life*. *arXiv* **2018**, arXiv:1803.00466.2018.
25. Chung, H.; Iorga, M.; Voas, J.; Lee, S. 'Alexa, Can I Trust You?' *Computer* **2017**, *50*, 100–104. [CrossRef]
26. Lau, J.; Zimmerman, B.; Schaub, F. Alexa, Are You Listening? *Proc. ACM Human-Comp. Interact.* **2018**, *2*, 1–31. [CrossRef]
27. Flikkema, P.G.; Cambou, B. When things are sensors for cloud AI: Protecting privacy through data collection transparency in the age of digital assistants. In Proceedings of the 2017 Global Internet of Things Summit (GloTS), Geneva, Switzerland, 6–9 June 2017, pp. 1–4.

28. Wong, J.C. 'A white-collar sweatshop': Google Assistant contractors allege wage theft. *The Guardian*, 25 June 2019.
29. Elahi, H.; Wang, G.; Peng, T.; Chen, J. AI and its Risks in Android Smartphones: A Case of Google Smart Assistant. In Proceedings of the 5th International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DependSys 2019), Guangzhou, China, 12–15 November 2019; pp. 1–15.
30. Gorla, A.; Tavecchia, I.; Gross, F.; Zeller, A. Checking app behavior against app descriptions. In Proceedings of the 36th International Conference on Software Engineering—ICSE 2014, Hyderabad, India, 31 May–7 June, 2014; pp. 1025–1035.
31. Yu, L.; Luo, X.; Qian, C.; Wang, S.; Leung, H.K.N. Enhancing the Description-to-Behavior Fidelity in Android Apps with Privacy Policy. *IEEE Trans. Softw. Eng.* **2018**, *44*, 834–854. [CrossRef]
32. Slovic, P. Perception of risk. *Science* **1987**, *236*, 280–285. [CrossRef] [PubMed]
33. Cohen, S.; Money, W. Establishing Smart City Technical Standards and Guidance. In Proceedings of the 26th International Conference on World Wide Web Companion—WWW '17 Companion, Perth, Australia, 3–7 April 2017; pp. 1161–1166.
34. Ferretti, L.; Longo, F.; Colajanni, M.; Merlino, G.; Tapas, N. Authorization Transparency for Accountable Access to IoT Services. In Proceedings of the 2019 IEEE International Congress on Internet of Things (ICIOT), San Diego, CA, USA, 5–30 June 2019; pp. 91–99.
35. Steijn, W.M.P.; Niezen, M.G.H. The Value of Accountability in the Cloud: Individual Willingness to Pay for Transparency. *IEEE Technol. Soc. Mag.* **2015**, *34*, 74–82. [CrossRef]
36. Zouave, E.T.; Marquenie, T. An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling. In Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 11–13 September 2017; pp. 17–23.
37. Permissions Overview. Android Developer Documentation. Available online: <https://bit.ly/2HcAcyce> (accessed on 25 June 2019).
38. Zhou, Y.; Piekarska, M.; Raake, A.; Xu, T.; Wu, X.; Dong, B. Control yourself: On user control of privacy settings using personalization and privacy panel on smartphones. *Procedia Comput. Sci.* **2017**, *109*, 100–107. [CrossRef]
39. Bal, G.; Rannenbergh, K.; Hong, J.I. Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns. *Comput. Secur.* **2015**, *53*, 187–202. [CrossRef]
40. Kim, K.J.; Shin, D.H.; Yoon, H. Information tailoring and framing in wearable health communication. *Inf. Process. Manag.* **2017**, *53*, 351–358. [CrossRef]
41. Bao, L.; Lo, D.; Xia, X.; Li, S. What permissions should this android app request? In Proceedings of the 2016 International Conference on Software Analysis, Testing and Evolution, SATE 2016, Kunming, China, 3–4 November 2016; pp. 36–41.
42. Sun, L.; Li, Z.; Yan, Q.; Srisa-an, W.; Pan, Y. SigPID: Significant permission identification for android malware detection. In Proceedings of the 2016 11th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, Puerto Rico, 18–22 October 2016; pp. 59–66.
43. Dao, T.A.; Singh, I.; Madhyastha, H.V.; Krishnamurthy, S.V.; Cao, G.; Mohapatra, P. TIDE: A user-centric tool for identifying energy hungry applications on smartphones. *IEEE/ACM Trans. Netw.* **2017**, *25*, 1459–1474. [CrossRef]
44. Dini, G.; Martinelli, F.; Matteucci, I.; Petrocchi, M.; Saracino, A.; Sgandurra, D. Risk analysis of Android applications: A user-centric solution. *Futur. Gener. Comput. Syst.* **2018**, *80*, 505–518. [CrossRef]
45. Rashidi, B.; Fung, C.; Bertino, E. Android resource usage risk assessment using hidden Markov model and online learning. *Comput. Secur.* **2017**, *65*, 90–107. [CrossRef]
46. Jing, Y.; Ahn, G.-J.; Zhao, Z.; Hu, H. RiskMon: Continuous and Automated Risk Assessment of Mobile Applications. In Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, CODASPY 2014, San Antonio, TX, USA, 3–5 March 2014; pp. 99–110.
47. Bhandari, S.; Jaballah, W.B.; Jain, V.; Laxmi, V.; Zemmari, A.; Gaur, M.S.; Mosbah, M.; Conti, M. Android inter-app communication threats and detection techniques. *Comput. Secur.* **2017**, *70*, 392–421. [CrossRef]
48. Zafir, G. Forgetting About Consent. Why The Focus Should Be On 'Suitable Safeguards' in Data Protection Law. In *Reloading Data Protection*; Springer: Dordrecht, The Netherlands, 2014; pp. 237–257.
49. Alepis, E.; Patsakis, C. Monkey Says, Monkey Does: Security and Privacy on Voice Assistants. *IEEE Access* **2017**, *5*, 17841–17851. [CrossRef]

50. Zhang, N.; Mi, X.; Feng, X.; Wang, X.; Tian, Y.; Qian, F. Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home. *arXiv* **2018**, arXiv:1805.01525.
51. Zhang, R.; Chen, X.; Lu, J.; Wen, S.; Nepal, S.; Xiang, Y. Using AI to Hack IA: A New Stealthy Spyware Against Voice Assistance Functions in Smart Phones. *arXiv* **2018**, arXiv:1805.06187.
52. Seymour, W. How loyal is your Alexa? In Proceedings of the Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems—CHI '18, Montreal, QC, Canada, 21–26 April 2018; pp. 1–6.
53. Porter, J. The Biggest Google Assistant Products from CES 2019. The Verge. 2019. Available online: <https://tinyurl.com/ycasf9j4> (accessed on 20 April 2019).
54. Amadeo, R. The Google Assistant SDK Will Let You Run the Assistant on Anything. Arstechnica.com. 2017. Available online: <https://tinyurl.com/k3at2vw> (accessed on 29 January 2019).
55. Felt, A.P.; Chin, E.; Hanna, S.; Song, D.; Wagner, D. Android Permissions Demystified. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 627–638.
56. Tao, G.; Zheng, Z.; Guo, Z.; Lyu, M.R. MalPat: Mining Patterns of Malicious and Benign Android Apps via Permission-Related APIs. *IEEE Trans. Reliab.* **2018**, *67*, 355–369. [CrossRef]
57. Fang, Z.; Han, W.; Li, D.; Guo, Z.; Guo, D.; Wang, X.; Qian, Z.; Chen, H. revDroid: Code Analysis of the Side Effects after Dynamic Permission Revocation of Android Apps. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security—ASIA CCS '16, Xi'an, China, 30 May–3 June 2016; pp. 747–758.
58. Desnos, A. Androguard: Reverse Engineering, Malware and Goodware Analysis of Android Applications. 2013. Available online: <https://github.com/androguard> (accessed on 6 June 2018).
59. Bohm, A. Theoretical Coding: Text Analysis in Grounded Theory. In *A Companion to Qualitative Research*; Flick, U., von Kardoff, E., Stein, I., Eds.; SAGE Publications: London, UK, 2004; pp. 270–275.
60. Rovelli, P. Ninja Droid. GitHub. Available online: <https://github.com/rovellipaolo/NinjaDroid> (accessed on 6 December 2019).
61. ProGuarg. Available online: <https://tinyurl.com/y6qzlmdb> (accessed on 5 March 2019).
62. Article 29 Data Protection Working Party. Opinion 02/2013 on Apps on Smart Devices (wp202). Available online: <https://tinyurl.com/r7kb8dx> (accessed on 5 June 2019).
63. Google, Publish Your App. Android Developers. 2019. Available online: <https://tinyurl.com/y6krwplm> (accessed on 25 November 2019).
64. Chong, I.; Ge, H.; Li, N.; Proctor, R.W. Influence of privacy priming and security framing on mobile app selection. *Comput. Secur.* **2018**, *78*, 143–154. [CrossRef]
65. Harris, M.A.; Brookshire, R.; Chin, A.G. Identifying factors influencing consumers' intent to install mobile applications. *Int. J. Inf. Manag.* **2016**, *36*, 441–450. [CrossRef]
66. Gu, J.; Xu, Y.; Xu, H.; Zhang, C.; Ling, H. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decis. Support Syst.* **2017**, *94*, 19–28. [CrossRef]
67. Yang, W.; Xiao, X.; Pandita, R.; Enck, W.; Xie, T. Improving mobile application security via bridging user expectations and application behaviors. In Proceedings of the 2014 Symposium and Bootcamp on the Science of Security—HotSoS '14, Raleigh, NC, USA, 8–9 April 2014; pp. 1–2.
68. Manski, C.F. Measuring Expectations. *Econometrica* **2014**, *72*, 1329–1376. [CrossRef]
69. Neumann, P.G. Expectations of security and privacy. *Commun. ACM* **1994**, *37*, 138 [CrossRef]
70. Xu, X.; Zhang, L.; Wan, Q. A Variation Coefficient Similarity Measure and Its Application in Emergency Group Decision-making. *Syst. Eng. Procedia* **2012**, *5*, 119–124. [CrossRef]
71. Chen, K. Wang, X.; Chen, Y.; Wang, P.; Lee, Y.; Wang, X.; Ma, B.; Wang, A.; Zhang, Y.; Zou, W. Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS. In Proceedings of the 2016 IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, 23–25 May 2016; pp. 357–376.
72. Li, L.; Bissyande, T.F.; Klein, J. Rebooting Research on Detecting Repackaged Android Apps: Literature Review and Benchmark. *IEEE Trans. Softw. Eng.* **2019**, 5589. [CrossRef]
73. Jaccard, P. Etude Comparative de la Distribution Florale Dans Une Portion Des Alpes et du Jura. *Bull. Societ Vaudoise Sci. Nat.* **1901**, *35*, 547–579.

74. Elahi, H.; Wang, G.; Xie, D. Assessing privacy behaviors of smartphone users in the context of data over-collection problem: An exploratory study. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017, pp. 1–8.
75. Peng, T.; Liu, Q.; Wang, G.; Xiang, Y.; Chen, S. Multidimensional privacy preservation in location-based services. *Futur. Gener. Comput. Syst.* **2019**, *93*, 312–326. [\[CrossRef\]](#)
76. Zhang, S.; Wang, G.; Bhuiyan, M.Z.A.; Liu, Q. A Dual Privacy Preserving Scheme in Continuous Location-Based Services. *IEEE Internet Things J.* **2018**, *5*, 4191–4200. [\[CrossRef\]](#)
77. Dilawar, N.; Majeed, H.; Beg, M.O.; Ejaz, N.; Muhammad, K.; Mehmood, I.; Nam, Y. Understanding citizen issues through reviews: A step towards data informed planning in Smart Cities. *Appl. Sci.* **2018**, *8*, 1589. [\[CrossRef\]](#)
78. Pasolini, G.; Toppan, P.; Zabini, F.; Castro, C.D.; Andrisano, O. Design, Deployment and Evolution of Heterogeneous Smart Public Lighting Systems. *Appl. Sci.* **2019**, *9*, 3281. [\[CrossRef\]](#)
79. Chang, F.C.; Chiu, C.; Chen, P.; Chiang, J.; Miao, N.; Chuang, H.; Liu, S. Children's use of mobile devices, smartphone addiction and parental mediation in Taiwan. *Comput. Hum. Behav.* **2019**, *93*, 25–32. [\[CrossRef\]](#)
80. Fischer-Grote, L.; Kothgassner, O.D.; Felnhofer, A. Risk factors for problematic smartphone use in children and adolescents: A review of existing literature. *Neuropsychiatrie* **2019**. [\[CrossRef\]](#)
81. READ_GSERVICE. 2019. Available online: <https://tinyurl.com/y27dz3we> (accessed on 25 June 2019).
82. Horner, R.; Rimmer, C. Consent: Assessing and communicating risk. *Surgery* **2019**, *37*, 431–434. [\[CrossRef\]](#)
83. Fan, M.; Liu, J.; Wang, W.; Li, H.; Tian, Z.; Liu, T. DAPASA: Detecting Android Piggybacked Apps Through Sensitive Subgraph Analysis. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1772–1785. [\[CrossRef\]](#)
84. Xu, Y.; Wang, G.; Ren, J.; Zhang, Y. An adaptive and configurable protection framework against android privilege escalation threats. *Futur. Gener. Comput. Syst.* **2019**, *92*, 210–224. [\[CrossRef\]](#)
85. Li, J.; Sun, L.; Yan, Q.; Li, Z.; Srisa-an, W.; Ye, H. Significant Permission Identification for Machine-Learning-Based Android Malware Detection. *IEEE Trans. Ind. Informatics* **2018**, *14*, 3216–3225. [\[CrossRef\]](#)
86. Collins, K. Google Collects Android Users' Locations Even When Location Services Are Disabled. 2017. Available online: <https://tinyurl.com/y93eadtp> (accessed on 23 May 2018).
87. Ng, A. More Than 1,000 Android Apps Harvest Data Even after you Deny Permissions. CNET, July 2019. Available online: <https://tinyurl.com/y5dxluf5> (accessed on 10 July 2019).
88. Varian, H.R. *Beyond Big Data*; Berkeley School of Information: San Francisco, CA, USA, 2013.
89. Rasthofer, S.; Arzt, S.; Bodden, E. A Machine-learning Approach for Classifying and Categorizing Android Sources and Sinks. In Proceedings of the 2014 Network and Distributed System Security Symposium, San Diego, CA, USA, 23–26 February 2014; pp. 23–26.
90. Fabo, B.; Kahanec, M. Can a voluntary web survey be useful beyond explorative research? *Int. J. Soc. Res. Methodol.* **2018**, *21*, 591–601. [\[CrossRef\]](#)
91. Sweller, J.; Ayres, P.; Kalyuga, S. Intrinsic and Extraneous Cognitive Load. In *Cognitive Load Theory*; Springer: New York, NY, USA, 2011; pp. 57–69.
92. Solove, D.J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Rev.* **2013**, *126*, 1880.
93. Senarath, A.R.; Arachchilage, N.A.G. Understanding user privacy expectations: A software developer's perspective. *Telemat. Inform.* **2018**, *35*, 1845–1862. [\[CrossRef\]](#)
94. Wang, Z.; Yu, Q. Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Comput. Law Secur. Rev.* **2015**, *31*, 782–792. [\[CrossRef\]](#)