bbbb

by Patience Hyat

Submission date: 11-Aug-2022 04:36AM (UTC+0800)
Submission ID: 1878426375
File name: MOBILE_PRIVACY_AWARENESS_1.docx (395.15K)
Word count: 7495
Character count: 42122

TRANSFORMTIKA, Vol.15, No.1, Juli 2017, pp. 1 - xxx
ISSN: 1693-3656,
journals.usm.ac.id/index.php/transformatika

MOBILE PRIVACY AWARENESS OF HIGHER EDUCATION STUDENTS IN PLATEAU STATE NIGERIA

(Left, Bold, Arial 16, max **10 words** in English)

First Autor[1], Second Author[2], Third Author[3]
[1]Institution/affiliation
addres, telp/fax of institution/affiliation, e-mail: xxxx@xxxx.xxx
[2]Institution/affiliation
addres, telp/fax of institution/affiliation, e-mail: xxxx@xxxx.xxx

ARTICLE INFO

Article history:

Received 30 December 2010
Received in revised form 30 April 2011
Accepted 26 September 2012
Available online 8 October 2012

ABSTRACT

The ubiquitous nature of mobile devices and wide array of applications (and services) they offer make them useful in virtually all areas of human endeavours. Owners of mobile devices store large amounts of vital and sensitive personal information on their devices. Unauthorized access to such information by third parties can violate the privacy of users and expose individuals and businesses to huge financial loses and damage to reputation. This makes it imperative for owners of technology service providers and owners of mobile devices to take proactive steps that prevent privacy violation. One of such critical steps is privacy awareness, which is the knowledge and consciousness of the need for privacy, an understanding of actions that promote or compromise privacy and the consequences of irresponsible online behaviour. The aim of this study is to assess the level of awareness of tertiary institution students with respect to privacy issues associated with the use of mobile communication devices. The research uses questionnaires to obtain data on the privacy awareness of users of mobile devices in some tertiary institutions in Plateau State. The paper investigates the current status of mobile privacy issues and awareness of users in these tertiary institutions. It also attempts to expose the gaps in privacy awareness of mobile device users, the factors responsible for limited privacy awareness and strategies for addressing the low level of privacy awareness of mobile device users. The results from this study show that high level of literacy does not necessarily imply high-level privacy awareness. Many respondents who are privacy aware do not possess the necessary skills or knowledge to ensure data and user privacy on their mobile devices. Others who possess this knowledge are will to engage in practices that compromise privacy in exchange for financial gain. Overall, the study exposes the actual level of privacy awareness and defeat the assumption that high level of education automatically results in high-level privacy awareness. It also contradicts the assumption that being privacy-aware guarantees responsible online behaviour and adherence to practices that promote online privacy.

KEYWORDS: Mobile Devices; Online Privacy; Privacy Awareness; Privacy Risks; Smartphones

1. Introduction

The term “mobile devices” is generally used to refer to a category of handheld gadgets (computers and telephones) that can easily be carried about and operated in the hand. These devices use wireless technologies (Bluetooth, near field communication, cellular networks and Wi-Fi) to provide and support communication and data transmission. A mobile device cannot function without an operating system which provides a platform for other system and application programs

Received February 23, 2014; Revised May 29, 2014; Accepted June 12, 2014

to execute. Mobile devices have small memory size and low processing power compared to desktop computers and servers. Hence the operating systems as well as system and application programs used by mobile devices are usually in small-sized and low-scaled versions due to the low memory size and limited processing power of these devices. Mobile devices are used for personal and business purposes including phone calls, text messaging, electronic mail, mobile/internet banking, electronic commerce, educational purposes, online meetings and business collaborations. The fast, easy and seamless communication provided by mobile technology enables business organization and their workers to enjoy better productivity and almost interrupted business operations. The ubiquitous nature and widespread use of mobile technology encourage organizations to deploy mobile systems and applications to support their businesses and enhance the growth of their corporations. The ease with which consumers can access and download mobile applications enhances their adaptation to mobile technology and provides rapid support for business organizations which use this valuable technology.

Privacy is "the state of being alone and not watched or disturbed by anyone" [1]. Privacy enables us to protect our dignity and set barriers which prevents unnecessary interference. This gives an individual the right to decide who has access to his data, information and communication. In the context of information technology, privacy can be defined as the right to protection of personally identifiable information and the use of such information in accordance with relevant laws and regulations. That is, how much and to what extent a user's personal data can be made available to third parties online [2]. Privacy awareness refers to the knowledge and consciousness of the right to one's privacy. That is, being knowledgeable and conscious enough to set barriers, provides limits and determine accessibility to personal space, belongings, data, information and communication. Mobile device privacy awareness is a situation whereby a mobile device user is knowledgeable about privacy risks associated with the use of mobile devices and making conscious effort to ensure the protection of his personal data and the usage (transmission, sharing or modification) of such data in line with agreement(s) between him (data owner) and data collectors and based on approved laws and regulations. Mobile gadgets use wireless technology for communication and data transmission. Many owners of mobile devices store sensitive personal information on their devices. They also use such devices for highly sensitive activities involving their health and financial information. The ubiquitous nature of wireless technology makes it more difficult to secure wireless transmissions compared to their wired counterparts. Mobile devices are easily movable and are thus exposed to theft or loss. The movable nature of mobile devices and their use in public expose the information stored in them to prying eyes of unwanted persons. Common privacy attacks are eavesdropping and shoulder surfing. Many young people share huge amounts of sensitive personal information online resulting in abuses and unpleasant circumstances such as cyberbullying, identity theft, and cyber stalking, school expulsions and reputation damage [3]. Privacy violations compromise the confidentiality, integrity and availability of sensitive information stored in and transmitted by mobile devices and by extension violate the privacy of users. Cybercriminals who gain access to private information such as mobile phone numbers, email addresses and credentials, credit card numbers, working IP addresses, and online gaming account details can offer them to third parties in exchange for financial rewards and without the knowledge or consent of the owners [4]. Hence, users are advised evaluate the likely consequences before divulging sensitive information to third parties online. It is also important to change account settings of applications used for social media, online gaming, electronic commerce and online banking from the default mode to "privacy conscious" mode. This is to minimize the likelihood of data exfiltration via these platforms. Another suggestion is for users to delete or remove sensitive personal information from online accounts they rarely use. Users should update their apps regularly, limit the use of social media accounts in signing to other applications and avoid carrying out sensitive transactions when connected to public Wi-Fi. Adequate online privacy is necessary to prevent third parties from collecting, analyzing and sharing of personally identifying information

(such as name, date of birth, address and social security number) and non-personally identifying information (which includes browsing history, online shopping history and social media profiles) [5].

Mobile device users are increasingly becoming aware of their right to privacy. For example, Brazilian Internet users are increasingly becoming privacy aware as indicated by their desire to decide how owners and operators of online platforms handle data provided to them [6]. A study by Kaspersky and reported by [6] shows that 74% of Brazilian Internet users have attempted to remove their personal data from websites and social media platforms. However, about a quarter (24%) of the users do not have the required knowledge for removing sensitive personal data from online platforms. However, privacy awareness and concerns about privacy do not necessarily translate into online behaviours and attitudes that promote privacy. A survey to explore the relationship between privacy awareness and concern revealed that a large number (75%) of Americans have high online privacy concerns, but their actual online behaviours do not correlate with such high level of concerns [7]. Many users are unaware of their responsibilities or lack the capacity (in terms of knowledge and skills) to ensure the privacy of data and information. They are also not conscious of the implications of their actions and inactions on the user privacy. The increase in the level of privacy awareness makes many smartphone users place privacy concerns above the features of their devices [8]. About 80% percent of the smartphone users surveyed by the study in [8] download only app applications they trust. Majority of the users are also not favourably disposed to location and activity tracking by mobile applications. A high level of privacy awareness among data owners can expose data collectors to avoidable litigations and claims for damages in the event of privacy violations. Hence it is imperative for data collectors to conform with privacy agreements (usually signed at the point of data collection) and laws and regulations governing data privacy. They should also educate data owners on their roles and responsibilities towards the achievement of mobile data privacy.

Our knowledge, experience and observation show that students of tertiary institutions are among the most educated or literate members of any society. They also represent a significant chunk of mobile devices users in any country. There is a wrong assumption of the correlation between the high literacy of these group of mobile device users and their level of security awareness. Previous studies have shown that many students lack the knowledge, consciousness and motivation for security and privacy [9, 10]. Mobile device security is a growing area within the information security domain, but mobile data privacy is still at its infancy. Mobile device manufacturers consider security and privacy of users very important, but access to and use of large number of downloadable applications from the internet makes it very complex and difficult to handle threats and vulnerabilities associated with the privacy of users. A number of studies (see Section 2 – related works) have been carried out on privacy awareness of mobile device users. However, none of these studies assessed the privacy awareness level of tertiary education students who own and use mobile devices. To the best of our knowledge, this is the first study to evaluate the level of mobile privacy awareness of students of tertiary institutions in Nigeria.

2. Related Work

Smartphone users are affected by two main dimensions of privacy namely, human-centric privacy and technology-centric privacy [11]. The essence of human-centric privacy is to strike balance between provision of sensitive data to mobile applications and platforms for better user experience and the need to prevent exposure of personally identifiable information due to privacy concerns. The study identified awareness, expectation and authorization as the issues associated with human-centric privacy. Expectation deals with how users expected their data to be used by

mobile applications and the need for mobile platforms to meet such expectation. In other words, users' data should be used only for the purpose for which they have been collected. Awareness explores the correlation between the level of privacy awareness of smartphone users and their actual online behaviours. Authorization states that all operations on users' data must be carried out by users themselves and not the mobile application owner or a third party. Technology-centric privacy, on the other hand, uses technologies such as algorithms, tools and privacy enhancing solutions in systems and applications to protect users against privacy violations. The paper identified sensitivity and anonymity as the two main dimensions of technology-centric privacy. Sensitivity refers to the provision of high-level protection for sensitive information (such as location, voice and image data, biometric data and environment context) stored in mobile devices, whose disclosure can result in compromise of user privacy. Anonymity is the possibility of data to remain protected in the event of unauthorized disclosure. This is necessary because of the lack of a completely fool proof defence against privacy attacks.

A number of studies have been carried out to access privacy awareness of mobile device users based on human-centric and technology-centric aspects of privacy. These studies identify the factors which influence users' level of privacy awareness and suggest measures (and/or propose tools) to enhance privacy awareness of mobile device users. One of such is a concept known as "Profile for the Information Privacy Aware User" consisting of the main attributes of a user who is knowledgeable about and conscious of his online privacy [12]. The profile is aimed at promoting privacy awareness among internet users and internet providers. It also intends to simplify the jobs of professionals who develop technologies for improving privacy awareness. A related work explored the roles of privacy concerns, trust, and user awareness on the willingness of social media users to share personal information online [13]. The research used online survey (via questionnaire) to obtain data from 340 social-media users. It also performed reliability and validity analyses to prove validity of the structural model applied in the study, while using structural equation model (SEM) analysis to determine relationships among constructs in the model. Analysis results reveal a positive relationship between user awareness, trust, and privacy concerns and the willingness of social media users to share personal information online. In other words, a high level of awareness of privacy risks and concerns about the implications of privacy attacks make users more careful about sharing personal data on social media sites. On the other hand, users who have high level of awareness and legitimate privacy concerns would still go ahead to share personal information on social media sites they trust. The study suggests that business corporations and government agencies apply strict guidelines in the form of Standard Operating Procedures (SOPs) to limit the quantum of sensitive information stored in social-media accounts. This will prevent deliberate or accidental leakage of personal or corporate data by workers through social-media accounts. Social media companies are advised to provide users with mechanisms to enable them make informed decision about the nature and volume of personal information to make available online. Users should be careful in their daily activities and engagements on the Internet generally and social media specifically. They should avoid sharing sensitive information such as location data and untagged photos downloaded by people they do not know. An attempt to assess the impact of factors, particularly privacy awareness on the willingness of social media users to disclose or protect their information during online interaction focused on user's behaviour as it relates to privacy protection and information disclosure [16]. The results of an empirical study based on a survey of 210 Facebook users revealed that many active users of Facebook disclose a lot of personal information. This is due to their ignorance of the public nature of any information shared online and the ability of third parties to access such information. The users do not possess adequate knowledge and understanding of the privacy policy and terms of use of Facebook. A survey to determine the level of privacy awareness and adherence to behaviour and practices that prevent privacy violations revealed a very low level of security and privacy awareness of many smartphone users [15]. Hence the study developed an easy-to-use approach for determining the 'level of

awareness (LOA)' of smartphone users. This will enable the users to evaluate their level of privacy awareness from time to time and take actions that will enhance their privacy. A slightly different approach to privacy awareness is a model that factored in the peculiarities in the attitudes of different users towards privacy and the privacy preferences of individual users [16]. This enables the proposed model to make appropriate decisions about the privacy needs of users and minimize the individual user's exposure to privacy risks. The study used a survey to ascertain the privacy preferences of users and the level of control they desire over different aspects of privacy and usability. The proposed approach manages individual users' privacy needs and preferences in a useful and centralized manner. It also assigns priorities to an individual user's privacy requirements to provide timely and reliable notifications about important privacy issues. The results from the study shows that privacy concerns, knowledge about privacy and the desire for multilevel privacy controls vary among users. This makes it imperative to develop a holistic model tailored to meet the address specific privacy concerns and requirements of individual users. Other factors apart from technical knowledge, privacy concerns, trust and user awareness influence online behaviour and attitude to privacy. Research suggests the existence of a relationship between religious beliefs, online behaviour and social media use [17]. The study proposed a partial least square structural equation model which uses religious orientation scale (ROS) to access the level depth of an individual's religious beliefs and communication privacy management (CPM) to evaluate essential privacy parameters. These parameters include privacy concerns, privacy awareness, knowledge of risks and controls related to privacy and attitude towards privacy. The study revealed a positive relationship between CPM and users' activities on social media. It also shows a user's level of religiosity determines his privacy concerns and affects the way he uses the social media. Unlike previous studies which focused on the effects of technical knowledge, privacy awareness and desire of users for privacy on actual online behaviour, a unique approach for evaluating privacy awareness focused on online behaviour without considering the users' level privacy awareness, economic power and technical skills [18]. An experiment was conducted by giving adequate amount of money to students who are highly skilled mobile app users to buy licensed or pay-per-use apps. Experimental results reveal no correlation between actual user behaviour and other factors such as technical knowledge, economic power and level of privacy awareness. Concerns about the functionality, features and cost of applications far outweigh the desire of users for privacy. The users engaged in risky online behaviour despite their awareness of the negative implications of such behaviour on privacy.

There are privacy issues and challenges associated with the deployment of location aware technologies and related products and services [19]. The privacy concerns associated with location aware mobile devices include improper collection (acquisition), improper retention (storage), improper use, and unauthorized disclosure of user's data [20]. This poses significant privacy risks to users as the applications can reveal the personal information of a user and his actual physical location at any particular time [21]. However, data gathering by mobile applications is not necessarily for malicious purposes [22]. Mobile applications may ask users to provide sensitive data such as email addresses, calendar records, call logs, and location data via a mobile device for legitimate purposes. For example, online ride booking apps such as Bolt and Uber may ask for users' names, phone number and location information. This provides good user experience such as disclosing the identities of a driver and a rider to each other and enables a driver to know where to pick up a prospective rider.

A number of country-specific studies assessed the level of privacy awareness of users in a specific country or multiple countries. A study of 575 participants from Germany, Romania and Spain revealed that many users (about 50% of the participants) understand the implications of being connected to a smart environment (smart home and smart health applications and services) and

have expressed concerns about one or more privacy issues [23]. Findings from the study showed that participants from Germany have higher security and security and privacy concerns than those from Romania and Spain. It also revealed variations in level of security and privacy awareness, data protection regulations as well as the implementation and enforcement among the countries studied. This presents tremendous challenges to global enforcement of data protection regulations as Internet services are cross boarder in nature. Owners and operators of smart home and smart health platforms collect data without letting users know the extent to which third parties would have access to such data. Most of the users feel unconcerned about unauthorized access to personal data by third parties' despite being aware of the sensitive nature of such data. This is due to the high level of trust the users have in the operators of these platforms. Overall, the study showed that cultural factors and operational environment of a specific platform or data exchange affects the security and privacy of the end users. Similarly, a mobile privacy initiative by the Global System for Mobile Communications Association (GSMA) conducted a survey on more than 4,000 mobile users across UK, Singapore and Spain to understand the privacy concerns of mobile device users and its effect on their attitudes towards and willingness to use mobile services and applications [24]. Findings from the study showed that the countries surveyed have large numbers of sophisticated internet and mobile applications users. However, majority of respondents from UK and Spain were medium/light users who used mobile internet and applications for five hours or less in a week. This was unlike Singaporeans who used mobile internet and applications for at least six hours per week and are considered heavy users. The study also revealed that knowledge of mobile internet and applications and frequency of usage affect users' attitudes towards privacy and general use of services and applications. Heavy internet users generally have similar attitudes towards privacy, while the attitudes of non-users towards privacy in one country is the same for non-users in the other two countries. A modified measurement method to access the level of security and privacy knowledge and awareness of smartphone users in Indonesia revealed that many Indonesian smartphone users do not possess adequate knowledge and awareness of security and privacy [25]. The results of analysis show that the modified approach provides a more variable Level of Awareness (LoA) compared with previous techniques. The modified solution has an average LoA of 23%, which is a significant improvement over the existing method with average LoA of 17%. A comparative study the security and privacy awareness (and concerns) of Internet users in East Africa (EA) and those in the United States (U.S) used a quantitative research technique to identify the similarities and differences in the attitudes of these groups of users towards security and privacy [26]. A study of EA internet users (from the Open University of Tanzania) and U.S internet users (from Kansas State University) revealed very little difference in online privacy awareness of these two groups of users. There is however, significant difference in concerns about online privacy, which differ with the type of information shared. However, users from the United States have more online privacy concerns and are more disposed towards taking necessary actions to protect their online privacy. Hence EA users are at a much higher risk of online privacy attacks such as identity theft and reputation damage.

Technologies have been proposed to identify privacy risks and promote privacy awareness among mobile device users. One of such is a novel solution known as PriView, which allow users to see privacy-invasive devices located in their vicinity [27]. The goal is to counter the use of sensors for tracking and obtaining sensitive personal data in both audio and video format. The presence of such privacy invasive sensor-based devices is usually unknown to users. Hence PriView was proposed to enable users identify places where sensors have been installed to track/record information that can violate privacy. PriView consists of two prototypes which include a mobile application which uses a thermal camera to detect smart devices in an area and another application which records images of six possible scenarios for the tool. Experimental results show that users are comfortable with simple, permanent indicators of privacy invasion and would like to decide whether they want a detailed visualization of privacy intrusion or not. A related work

proposed a system known as PrivacyCamera to prevent privacy violation caused by unintentional exposure of a person's location via photos taken by a third party [28]. The victim's photo may be inadvertently included in the photo taken by a third party. The system uses cooperation between a person and a third party to blur a would-be victim's face based on his request at the time of taking the photograph. Experimental results show that the technique prevents unintended inclusion of a person's face in photographs without his consent and provides efficient protection of users' privacy. An earlier solution is a prototype for privacy awareness known as "interactive social translucence map" (an on-line interactive tool, component or user-interface) in applications to promote users' privacy awareness and enhance their understanding of on-line privacy risks [29]. The proposed solution reveals the flow of a user's personal information, asks the user about his privacy and presents a set of interactive frequently asked questions to enable a user highlight his privacy concerns in a preferred language and context. An evaluation of the prototype involved the selection of 100 respondents consisting of both experienced and not so experienced users in order to access its usability and demonstrate its effectiveness on privacy awareness. The evaluation also focuses on the ability of the prototype to support users' identification and understanding of privacy risks. Findings suggest that proposed tool enhances users' privacy awareness and improves their ability to identify and understand privacy risks. The study also revealed a positive correlation between the acceptance of a privacy awareness feature and the level of ICT skills and Internet experience of users. Human computer interaction can also be used to provide a set of well-tailored tools that determines users' perception of privacy threats, uncover how they people share sensitive information with third parties, and examines the degree to which a given system provides (or restricts) desired privacy practices [30].

Several suggestions and recommendations have been made to enhance privacy awareness level of mobile device users, minimize privacy risks and likelihood of privacy attacks. One of the measures to mitigate security and privacy violations include secured programming or security conscious development to ensure that developers provide applications with in-built security and protection mechanisms, instead of attempting to integrate security and privacy modules at the endo of the development process [31]. Another suggestion is the provision of mechanisms to enforce secured/safe application download to prevent users from installing applications that can compromise the security and privacy of users. The paper also proposed hardening mobile operating systems and deploying biometrics in mobile devices to mitigate the security and privacy risks of mobile device users. Privacy regulations the world over require mobile application developers to build software that meet approved privacy principles and standards. This is quite challenging as developers find it difficult to understand the legal principles that must guide software development. Hence, Hatamian [32] proposed a privacy and security design catalog for app developers to assist them in understanding and adopting the most relevant privacy and security principles in the context of smartphone apps. This catalog maps specific legal and regulatory requirements to practical privacy and security mechanisms that developers can implement to enhance privacy in conformance with existing laws. The use of a case study to test the proposed design catalog revealed a lot of app develops do not provide privacy enhancing mechanisms in mobile apps contrary to what they have promised to do. Mobile application developers should adopt the US's mobile privacy compliance which revolves around two major requirements namely, transparency and privacy-by-design [33]. Transparency involves a complete disclosure of sensitive information an application may collect and if (and how) that information may be shared with third parties. It also focuses on disclosing the location information that will be collected and issues related to location data retention and usage of location information for other purposes. Privacy-by-design, on the other hand, requires taking privacy into consideration during the entire software development life cycle and providing users with the right to decide how their data is used.

ISSN: 1693-3656

3. Methodology

This research used survey method to obtain the views, perception and opinions of the study population on the privacy issues as it relates to mobile device users. Survey method collects data from a specified population (or sample) in order to gain insights into the topic of interest. This method involves data collection and analysis from a sample obtained from the study population (Eguzoikpe, 2008). The population for this study consists of the students of five tertiary institutions in Plateau State, Nigeria namely, University of Jos, Plateau State University Bokkos, Plateau State Polytechnic Barkin Ladi, College of Forestry Jos and College of health Zawan. The selected sample of study includes five hundred (500) students drawn across the aforementioned tertiary institutions. Time, financial, logistical and statistical constraints do not allow effective and efficient study of an entire population. Hence, we used simple random sampling (or probability sampling) for data collection. It is a method which ensures that each element of the population has the same likelihood of being included in the sample. The study used a sample size which actually is a fraction of the population. We applied the the Taro Yamane formulae to compute the sample size.

The formula is defined as $n = \frac{N}{1 + N(0.05)^2}$ (1)

Where n = desired sample size and N = population size (number of students in the selected tertiary institutions). The value 0.05 is the significance level of the percentage error for the 95% confidence interval. It is important to note that the actual number of students in these institutions is more than 50,000, but the exact population could not be determined in the course of this research. Hence, an estimated population of 50,000 was adopted for our study. This implies that the estimated sample n, for the study is

$n = N/[1 + N(0.05)(0.05)]$
$= 50{,}000/[1 + 50{,}000(0.0025)] = 50{,}000/(1 + 125)$
$= 50{,}000/126 = 396.82539$
$\cong 397$

A total of 500 respondents instead of 397 were randomly selected from the population in order to increase the coverage of sampling across the population. This also provides the respondents in the research population with equal chance of being selected. The study acquired data only from primary sources using questionnaire. The questionnaires were distributed locally by administering them on respondents using the face-to-face method. Each questionnaire was divided into five sections. The first section covers the basic usage and demographic information of the respondents with variables such as institution, gender, age range, residency and internet usage. The other sections focused on the research questions. Data analysis was used to arrange, organize and present the data in a way that provides suitable answers to research problems. Descriptive statistics was used to analyze the responses. The approach summarizes sample and measures, while providing simple graphical analysis of quantitative data. The data was analyzed using SPSS and the summary presented in graphical format.

4. Result and discussion

The results are presented in the form of bar charts. These are obtained from analysis carried out using the SPSS package.

4.1 Users Demographic Information

Figure 1 presents the number of male and female respondents, age range, and place of permanent residence; that is whether they live in Plateau state permanently.

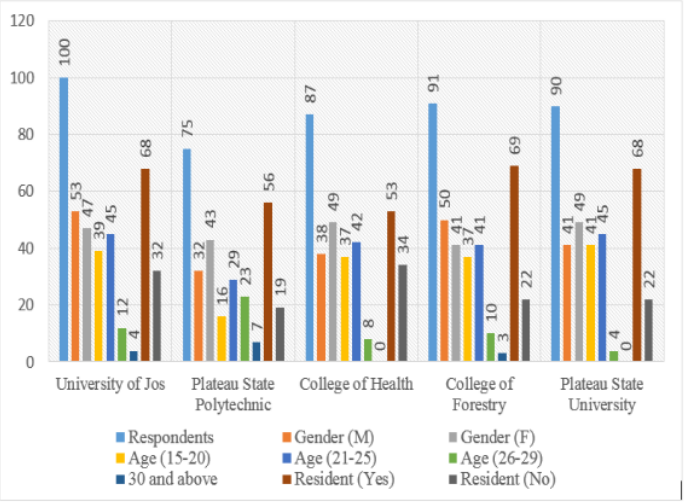

Figure 1: User demographic information

More male respondents were recorded in University of Jos and College of Forestry while the reverse was the case for the remaining three institutions. The age range of 20-25 had more responses because most students gain admission into tertiary institutions between the ages of 17 and 18. Students would have reached between 20 and 25 years of age before graduation. There are more respondents who are permanently residents in Plateau State because the state is a catchment area for these institutions. Many of the students also chose to attend these schools because of proximity and lower cost of living.

4.2 Internet Usage and Subscription to Online Services

Figure 2 illustrates the patterns of internet usage and subscription to online services.

ISSN: 1693-3656

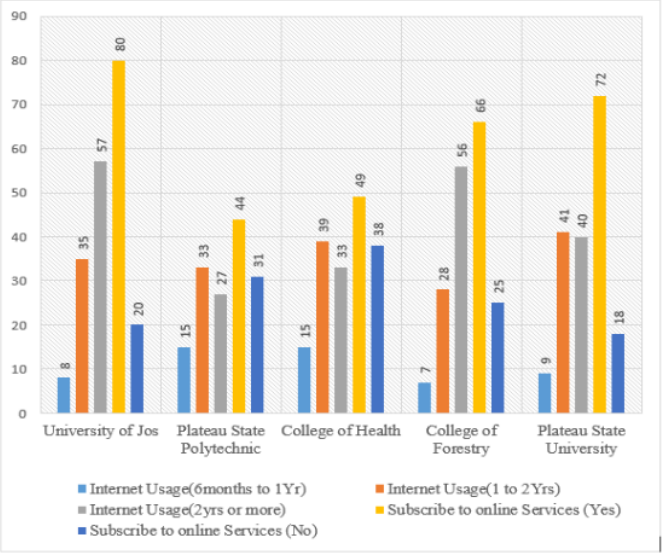

Figure 2: Internet usage and subscription patterns

The figure shows that the number of respondents who have used the internet for more than a year is more than those who have not done so. This is because students are the most active users of the internet. They always want to be up to date with latest information from friends, teachers and the social media. More respondents from all institutions say they subscribe to online services. This is because they are active users of the internet.

4.3 Purpose of Internet Usage

Figure 3 depicts the pattern and the purpose for which the respondents make use of the internet.

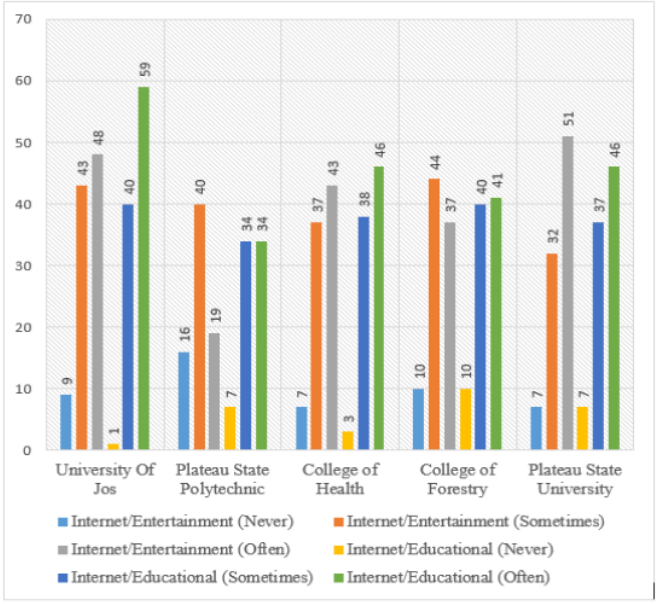

Figure 3: Purpose and pattern of internet usage

The figure shows that the respondents use the internet for both educational and entertainment purposes. This is because of the prevalence in the use of technology and the ease with which digital versions books, journals and other publications can be accessed online. However, more respondents use the internet for entertainment than for education. This is because they are mostly young people who want to keep abreast of the news and trends in the entertainment world.

4.4 Provision of Personal Information to Websites

Figure 4 describes the ease with which respondents across the five institutions divulge sensitive personal information to publicly accessible websites. Majority of the respondents claimed they have been asked to provide personal information when they visit websites. This is because t they are active users of the internet who subscribe to various online services (see

ISSN: 1693-3656

Figure 2). Further discussions with some of the respondents revealed that they have to be part of the community or platform in order to get information from some sites.

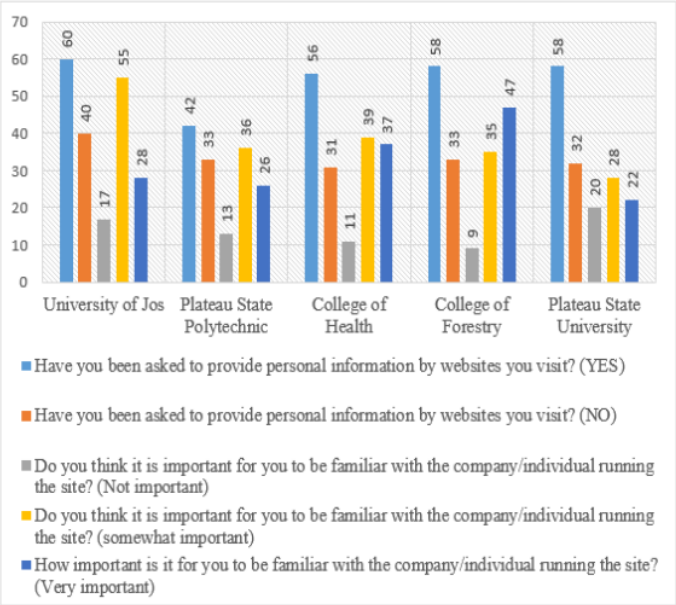

Figure 1: Trust in public sites

More respondents think it is not important for them to know the individual or company running the site as long as they have somewhat important or very important reasons to access the site. Some respondents feared that impostors could steal their information and use it for fraudulent activities.

4.5 Company Reputation Vs Divulgence of Personally Identifiable Information

The chart in Figure 5 illustrates the relationship between company reputation and the ease with which the respondents provide sensitive personal information to websites belonging to reputable organizations. Many respondents feel the reputation of the company who owns or

operates a website should be considered before providing personally identifiable information over the internet. Fewer respondents think this is very important.

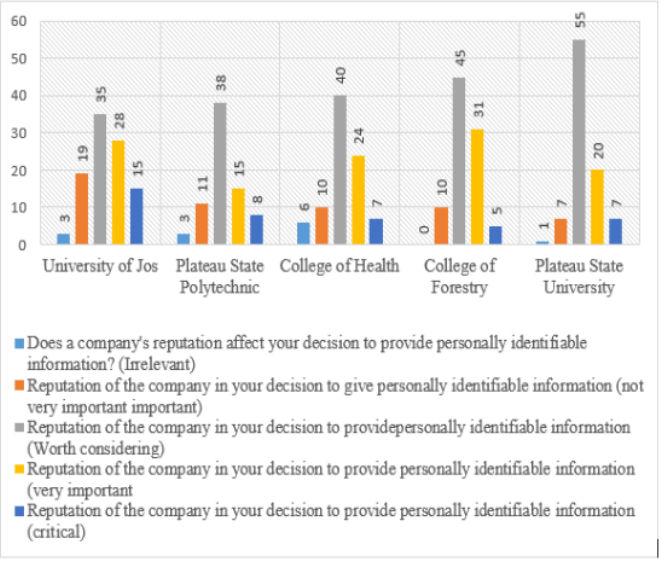

Figure 2: Company reputation vs divulgence of personal information

This may be due to the fact that respondents know little or nothing about security and privacy issues associated with most of the websites they visit. They believe everything is good as long as the company/site provides them with information they need. It is necessary to correct this erroneous belief by educating users on the need to take online security and privacy seriously.

4.6 Company Targeted Tastes and Compensation

More respondents claimed they are somewhat willing to provide personal information to websites so that online advertisement can be targeted to their tastes and interests (see Figure 6). This relieves them of the burden of looking for what they need. A large number of respondents are willing to provide personal information to online platforms in return for compensation by advertisers. Some respondents believe this is a way to earn money without working. Others claim they can give false information to these websites without the operators knowing how true the information is.

ISSN: 1693-3656

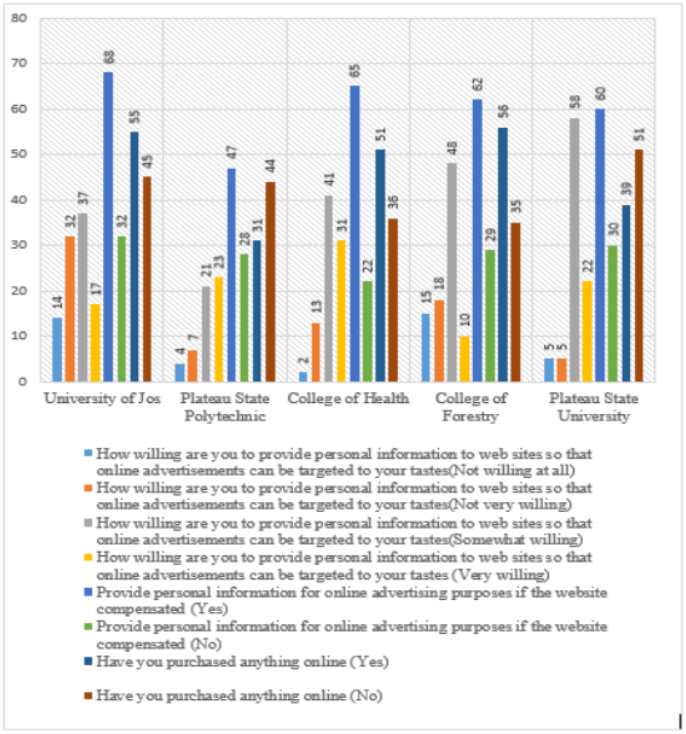

Figure 6: Target tastes and compensation

This shows how these respondents are ready to sell their personal information for money ignoring the fact that they can lose more when malicious these website owners decide to share their information illegally. Furthermore, many respondents from three out of the five institutions support the idea of purchasing items online, while majority of respondents from the remaining two institutions are not inclined to making online purchases. Further discussions revealed that many of the respondents prefer to purchase items online instead of open markets, while others lack the patience to wait for days or weeks to get a purchased item. Many other respondents are scared of online transactions due to the risk of fraud.

4.7 Recording and Sharing of Personal Information

As shown in Figure 7, majority of respondents from four institutions think their consent is somewhat important before sites can share their personal information with others. Respondents from one institution believe that website owners or operators must obtain their consent prior to sharing their information with a third party.

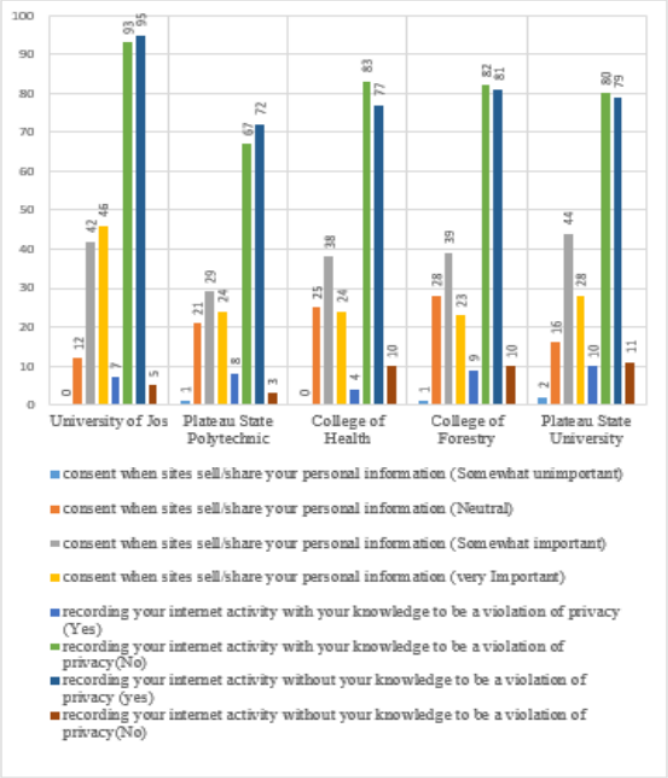

Figure 3: Recording/sharing of personal information

Some respondents are careful on how they use the internet because they do not want to be victims of identity theft. A large number of respondents from all the institutions do not want websites to record their internet activities, while a few others think that keeping record of their online activities with their consent is not a violation of privacy. Some respondents believe that despite giving their consent, sites that record more than they ask for have violated their privacy.

4.8 Concerns About Privacy of Data Transmission

Figure 8 shows that many respondents have similar concerns about privacy on the internet and on telephone. This means that the respondents are aware of the need for privacy on the internet and mobile devices.

ISSN: 1693-3656

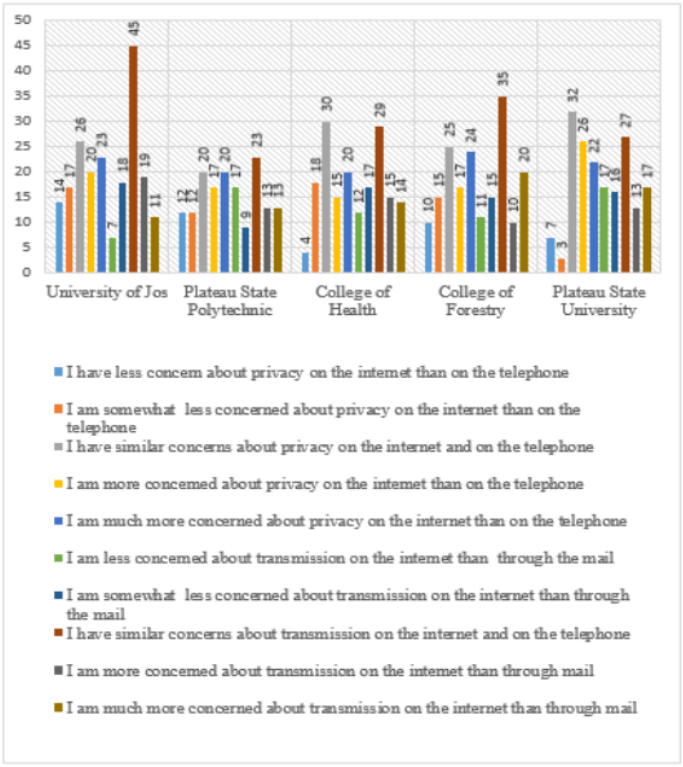

Figure 4: Concern about privacy of data transmission

They also have great concern about the privacy risks associated with data transmission over internet and telephone.

4.9 Disclosure and Assurance

Majority of the respondents are concerned about possible disclosure of data transmitted over the internet for various unspecified reasons.

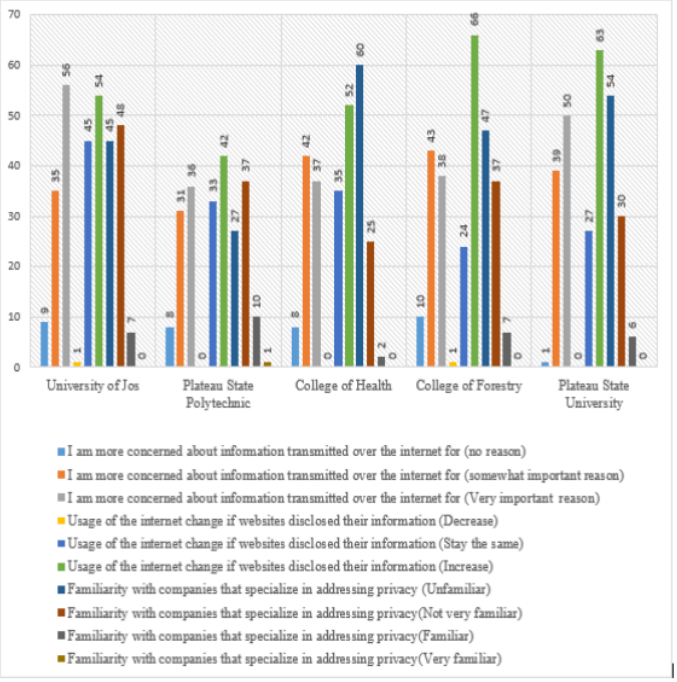

Figure 5 Disclosure and Assurance

Many of the respondents are aware of the high prevalence of online scams and they do not to become victims of online frauds. However, majority of the respondents have very little knowledge of companies that provides privacy and assurance services.

5. Conclusion

This research used survey and descriptive statistics to determine the level of privacy awareness among users of mobile devices in selected tertiary institutions in Plateau State. Although the use of mobile devices is very popular among the students of these institutions, a significant number of them are not aware of privacy risks associated with the use of mobile devices. Many of them share sensitive personal information freely on both trusted and untrusted websites. They simply log on to websites that can provide them with information or services they need without considering whether such activities can compromise user privacy. Others are willing to give personally identifiable information to untrusted parties in exchange for monetary rewards. The ability of the students to log on to institutional portals or access the internet via institutional networks makes the situation more precarious. This is because they may take actions which can compromise the security of other users and devices on the network. Security and privacy risks associated with mobile devices occur due to loss of a device, accidental download of malicious software, unauthorized access and use of unsecured public Wi-Fi. Low level of cyber security education is a major challenge to privacy awareness among mobile devices users. The management of these institutions should engage relevant stakeholders towards providing continuous cyber security education and training to staff and students of the institutions. Information technology experts, security professionals and security evangelists in the institutions to collaborate with the management to provide cyber security education and training to students of tertiary institutions in the state. This may take the form of workshops, seminars, radio jingles and pamphlets that

highlight dangers of privacy violations and the strategies for ensuring mobile device users' privacy. Governments, standards organizations, industry groups, public interest groups, and marketplace forces have important roles to play in addressing privacy issues. Governments can enact and enforce new and more stringent privacy laws to prevent and punish privacy violations. The judicial arm of governments consisting of various courts can also extend existing laws to cover new privacy related offences. Non-governmental organizations such as standards bodies, industry/trade groups, and advocacy/public interest groups can develop policies, standards and procedures to that enhance user privacy. The opinion of users and the preferences of consumers may provide a significant control over the way and manner their data are acquired, stored, used and disclosed. A future work will access privacy awareness of mobile device users in the state civil service and extend the scope of evaluation of privacy awareness to cover the north central region of the country, which consists of five other states apart from Plateau State

References

[1] Lea D, Bradber J, Oxford Advanced Learners Dictionary, 10th Edition. Oxford, United Kingdom: Oxford University Press, 2020.
[2] Terranova. *Data privacy day 2021: 6 best practices for your end users*.
[3] Cavoukian A, "Online privacy: make youth awareness and education a priority," Information and Privacy Commissioner of Ontario, Ontario, Canada, 2009.
[4] Trend Micro. *Data privacy day: why data privacy awareness is important*. 2015.
[5] Merton-Mccann A. *Privacy awareness week 2019 – protect your online privacy*. 2019.
[6] Mari A. *Data privacy awareness grows in Brazil*. 2020.
[7] Genetec. *75% Of Americans Very Concerned About Online Privacy, But Most Don't Take Any Significant Action*. 2021.
[8] ITBE Staff. *Study Finds Mobile Data Privacy Concerns Remains High; Awareness Growing*. 2013.
[9] Khalfan A, Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*. 2004; 24: 29-42.
[10] Stanton J.M, Mastrangelo P. R, Stam K. R and Jolton J, Analysis of end user security behaviors, *Computers and Security*. 2005; 24: 124-133.
[11] Liu R, Cao J and Yang L, Smartphone privacy in mobile computing: issues, methods and systems. *Information and Media Technologies*. 2015; 10: 281-293.
[12] Soumelidou A and Tsohou A, Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness, *Telematics and Informatics*.2021; 61: 101-120.
[13] Paramarta V, Jihad M, Ardhian D, Chandra H, Puspa I.S and Hidayanto N. A. *Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: facebook, twitter, and Instagram*. International Conference on Advanced Computer Science and Information Systems. Yogyakarta, Indonesia. 2018; 271-276.
[14] Tuunainen K.V, Pitkänen O, and Marjaana H. *Users' awareness of privacy on online social networking sites – case facebook*. 22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety. Bled, Slovania. 2009; 1-17.
[15] Ali M.N.Y, Rahman M.L and Ifrat J. Security and privacy awareness: a survey for smartphone user. *International Journal of Advanced Computer Science and Applications*. 2019;10: 483-488.
[16] Alshehri A, Clarke N.I and Li F. *Privacy enhancing technology awareness for mobile devices*. Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance. Nicosia, Cyprus. 2019; 74-88.
[17] Baazeem R and Qaffas A, Benson V and Mcalaney J. The relationship between user religiosity and preserved privacy in the context of social media and cybersecurity. *Emerging Cyber Threats and Cognitive Vulnerabilities*. Cambridge, MA: Academic Press. 2020. 93-116.

[18] Bartha S, De Jong M.D.T, Junger M, Hartel P.H and Roppelt J.C, Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics* 2019; 41: 55-69.

[19] Minch R.P, Privacy issues in location-aware mobile devices. *Proceedings of the 37th Hawaii International Conference on System Sciences*, Big Island, Hawaii. 2004; 1-10.

[20] Wang H, Lee M.K.O and Wang C. Consumer privacy concerns about internet marketing. *Communications of the ACM*. 1998; 41(3): 63-70.

[21] Karygiannis A, Antonakakis E, Barley M, Mouratidis H, Unruh A, Spears D, Scerri P and Massacci F. Security and privacy issues in agent-based location-aware. *Safety and security in multiagent systems. Lecture Notes in Computer Science*. 2009; 4324: 1-21.

[22] CISA. *Security tip (ST19-003) - privacy and mobile device apps*. 2019.

[23] O. Kulyk, B. Reinheimer, L., Aldag, M., Peter N., Gerber, and M. Volkamer. Security and privacy awareness in smart environments - a cross-country investigation. *AsiaUSEC 2020*. Kotakinabalu Sabah, Malaysia. 2020; 1-18.

[24] GSMA. *Research into user perspectives on mobile privacy: Key findings from UK, Spain and Singapore*. 2011.

[25] Amin M, Alam N, Dhahirl D.F, and Hadiyat Y.D. Security and privacy awareness of smartphone users in Indonesia. *Journal of Physics: Conference Series*. 2021; 1882: 1-11.

[26] Ruhwanya Z.S. Attitudes toward, and awareness of, online privacy and security: a quantitative comparison of East Africa and U.S. internet users. MS Thesis. Kansas State University, United States. 2015.

[27] Prange S, Shams A, Piening R, Abdelrahman Y, and Alt F. *PriView– exploring visualisations to support users' privacy awareness*. ACM Conference on Human Factors in Computing. 2021; 1-18.

[28] Li A, Qinghua L and Gao G. *PrivacyCamera: cooperative privacy-aware photographing with mobile phones*. 13th Annual IEEE International Conference on Sensing, Communication, and Networking. London, United Kingdom. 2016; 1-9.

[29] Kani-Zabihi E and Helmhout M. Increasing service users' privacy awareness by introducing on-line interactive privacy features. *Information Security Technology for Applications (NordSec 2011), Lecture Notes in Computer Science*. 2012; 7161: 4-10.

[30] Giovanni I and Hong J. End-user privacy in human–computer interaction. *Foundations and Trends in Human–Computer Interaction*. 2007; 1(1): 1–137.

[31] Khan J, Abbas H and Al-Muhtadi J. Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science*. 2015; 56: 376 – 383.

[32] Hatamian E. Engineering privacy in smartphone apps: a technical guideline catalog for app developers. *IEEE Access*. 2020; 8: 35429-35445.

[33] Golden Data Law. *Mobile privacy in the US*. 2019.

bbbb

ORIGINALITY REPORT

10%	8%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Dian Nuswantoro Student Paper	1%
2	www.researchgate.net Internet Source	1%
3	www.slideshare.net Internet Source	1%
4	"Aplikasi Musik Orkestra Angklung Multi Oktaf Berbasis Android Dengan Sensor Accelerometer", 'Universitas Semarang' Internet Source	1%
5	Submitted to Universitas PGRI Semarang Student Paper	1%
6	krex.k-state.edu Internet Source	1%
7	docplayer.net Internet Source	<1%
8	eprints.kingston.ac.uk Internet Source	<1%
	munin.uit.no	

9	Internet Source	<1%
10	www.gssrr.org Internet Source	<1%
11	8e585dfa-e129-45af-b2c2-777a20a3e9cd.filesusr.com Internet Source	<1%
12	www.trendmicro.com.ru Internet Source	<1%
13	"Trust, Privacy and Security in Digital Business", Springer Science and Business Media LLC, 2021 Publication	<1%
14	Theses.ubn.ru.nl Internet Source	<1%
15	ieeexplore.ieee.org Internet Source	<1%
16	aisel.aisnet.org Internet Source	<1%
17	docs.neu.edu.tr Internet Source	<1%
18	erepository.uonbi.ac.ke Internet Source	<1%
19	www.sidley.com Internet Source	<1%

20	www.us-cert.gov Internet Source	<1%
21	ebin.pub Internet Source	<1%
22	www.theijbm.com Internet Source	<1%
23	"Safety and Security in Multiagent Systems", Springer Science and Business Media LLC, 2009 Publication	<1%
24	Fouad Youssouf Osman, Nor Zairah Ab. Rahim. "Self-disclosure and Social network sites users' awareness", 2011 International Conference on Research and Innovation in Information Systems, 2011 Publication	<1%
25	Ioannis Chrysakis, Giorgos Flouris, Maria Makridaki, Theodore Patkos et al. "Chapter 15 A Rewarding Framework for Crowdsourcing to Increase Privacy Awareness", Springer Science and Business Media LLC, 2021 Publication	<1%
26	link.springer.com Internet Source	<1%
27	terranovasecurity.com Internet Source	<1%

28	www.mdpi.com Internet Source	<1%
29	Athanasios Karygiannis. "Security and Privacy Issues in Agent-Based Location-Aware Mobile Commerce", Lecture Notes in Computer Science, 2009 Publication	<1%
30	Majid Hatamian. "Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers", IEEE Access, 2020 Publication	<1%
31	Olli Pitkänen, Virpi Kristiina Tuunainen. "Disclosing Personal Data Socially — An Empirical Study on Facebook Users' Privacy Awareness", Journal of Information Privacy and Security, 2015 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		