A Characterization of Digital Native Approaches To Mobile Privacy and Security

Sarina Till
Independent Institute of Education
Durban, South Africa
University of Cape Town
Cape Town, South Africa
ctill@varsitycollege.co.za

Melissa Densmore
University of Cape Town
Cape Town, South Africa
mdensmore@cs.uct.ac.za

ABSTRACT

Despite their familiarity with the digital, so-called 'digital natives' are not tech-savvy, particularly with respect to privacy and security. In this study we characterize this problem by looking at a cohort of South African students. We employ a web-based survey of 100 students, supplemented by in-depth interviews with 10 additional students. In both cases we inquired about, and observed knowledge of permissions, encryption and application installation practices. Our findings show that most students (80%) do not look for or understand permissions or encryption, and use location-based services unsafely. Based on these results we argue that digital natives lack the technical skills and understanding to properly engage with mobile privacy and security. We further argue that this generation has been so over-exposed to mobile requests that violate their privacy and security that they have become desensitized and their definition of privacy and security has changed. Lastly, we discuss the implications of our findings for higher education institutions, policy, and mobile application design.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**;

KEYWORDS

android, mobile security, mobile privacy, university students, South Africa

ACM Reference Format:
Sarina Till and Melissa Densmore. 2019. A Characterization of Digital Native Approaches To Mobile Privacy and Security . In *Proceedings of 2019 Annual Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT'19).* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3351108.3351131

SAICSIT'19, 17-18 September, Skukuza, South Africa

ACM ISBN 978-1-4503-7265-7…$15.00
https://doi.org/10.1145/3351108.3351131

1 INTRODUCTION

South African Higher Education is in a process of reform and restructuring to redress the past and to move South Africa closer to a knowledge economy [10]. Part of this process is the drive to include ICT (Information and Communication Technology) in the Higher Education sector driven by government policies such as: The National Development Plan, the National Development plan for Higher Education and The National Research Development Strategy. All of these documents speak to the need for Higher Education to adopt ICT in order to deliver graduates who are equipped with 21st Century skills to join the Knowledge economy [10]. In response to this movement Higher Education institutions (HEIs) have seen a particularly large growth in mobile phone usage on their networks. According to Porter et al [37] more and more HEIs are implementing blended learning using popular Learning Management Systems such as Blackboard. To ensure accessibility to these systems, institutions often offer free WiFi to their students. These students access networks and institutional content on their mobile phones through a mobile application often provided by the developers of the LMS.

Most students currently enrolled in these institutions were born in the digital age and are often referred to as digital natives. Barak [6] describes these students as immersed in technology, more tech-savvy than the generations before them and well versed in the online world. However, Kurkovsky and Sytya's 2010 study *Digital Natives and Mobile Phones* [29] found that digital natives are not technologically advanced, lack knowledge on privacy and security and often down play the risks of using mobile phones. We argue that the digital proficiency of these students may still be overestimated, particularly in their awareness and perception of mobile security and privacy. Later works by Gkioulos et al [19] indicate that Kurkovsky's findings are still valid today. Both sets of authors argue that while digital natives might interact with technology differently than previous generations, there is little evidence that they have a better understanding of privacy and security. This lack of "tech-savvyness" combined with the drive for ICT in HEIs in South Africa, which in turn leads to the en masse uptake of mobile technology, pose very real implications for both the design of mobile security and HEIs

In order to further investigate, we surveyed 77 and conducted in-depth interviews with 10 students at a premier private undergraduate university in South Africa.

We tested the interactions of digital natives with Android-based application permissions, location-based services and encryption technologies to understand how students interacted with mobile

privacy and security features. In this paper we present the results as well as the implications for the design of Android's mobile security and HEIs.

2 BACKGROUND AND RELATED WORK

In the South African context, eighty nine percent (89%) of South African institutions make use of a BYOT (Bring Your Own Technology) policy to harness the prospects of blended and m-learning [13, 34, 38]. Of these devices, Android is the most popular mobile operating system with over 70% [47] of the market share. Unfortunately, the open source nature of this operating system also makes it the most likely to be attacked by malware [15, 31, 41]. Mobile devices are infected by malware either by attackers finding and exploiting vulnerabilities or by users being tricked into installing malicious applications [28]. This malware is then able to exploit users' private information. Android offers a permissions-based model aimed at assisting users and protecting their privacy [2]. However, this model comes with shortcomings of its own. The model is too coarse [47], places too much responsibility on the user, uses no sand-boxing and an open market [43]. Applications also often make use of more permissions than explicitly disclosed to the user [7]. Android relies on developers to include encryption in their applications. Sadly users do not normally enable encryption services [35], even if they are available. It is a well-known fact that users are often the weakest link in any security system [30]. In line with this, previous works have indicated that users do not understand mobile permissions [27] and therefore tend to ignore them [24]. Furthermore, users tend to be neglectful when it comes to security features [24, 35]. This behavior can be attributed to the fact that users are unaware of the possible dangers that lurk on their mobile devices, nor are they aware of the value of their personal data. Little attention has been paid to the effect this may have on institutional policy. The Council for Higher Education (CHE) makes mention of the lack of a coordinated policy to govern ICT in HEIs. This is echoed by Jaffer et al [25] who state that no coordinated policy exists at government or institutional level. Czerniewicz et al [12]explains that Higher Education ICT policy in South Africa is an emerging field of enquiry that has not enjoyed much attention. Ruxwana and Msibi [40] found that most South African HEIs are only partially ready for the adoption of a BYOT approach, with student education in terms of privacy and security being one of their main areas of concern. In line with Ruwana and Msisibi, Chin et al [11] argues for a fit for purpose and effective training program that would assist students with the safe and secure use of mobile devices on campuses.

3 METHODS

Because this study aimed to look at complex user behavior, a mixed method approach was used. The use of qualitative observations and interviews allowed us to gain deeper insights into the quantitative data gathered from our survey. We also used the qualitative data to validate the quantitative data . This process was chosen in order to gain an holistic view of students interactions with mobile privacy and security.

Simple random sampling was implemented by obtaining a list of the 1450 students enrolled at the HEI, but not including the students studying information technology, since android security and privacy is taught as a part of their curriculum. The list was scrambled to ensure that the names were not in alphabetical order or listed by qualification. Next, the list was numbered sequentially. An online random number generator was used to randomly generate 150 numbers. 150 students matching the randomly generated numbers were selected for the study. We targeted 120 responses for the survey, thus the 150 selected students were invited to complete the survey. 130 Students responded. 27 Incomplete responses were removed. The first question of the survey also queried whether the respondents were android users. 26 responses of non-Android users were removed. This left 77 completed responses from confirmed Android users. . It is possible that the removal of non Android users could introduce selection bias into the study. However, the wide range of responses and anonymity of the survey mitigates these effects.

3.1 Survey

The survey was designed to include questions aimed at testing the validity of the student's responses. For example, we presented the students with three questions regarding granting permissions to the custom developed applications. We first showed them the permissions in a list form and not in the familiar Google Play store setting. We then asked the students to tick each of the listed permissions they would allow for the application. In the very next question, we showed them the permissions as listed on the Google Play Store in a screen shot, these permissions are identical to the permissions in the first question. We asked the students if they would install the application and to give reasons for either installing or not installing the application.

To gather qualitative data a new was used. Ten additional numbers were randomly selected from the original list (excluding anyone originally selected for the survey) and asked to install two custom developed applications under observation. Following the observation, the students underwent a brief interview.

3.2 Observations and In-depth Interviews

In order to gather observation data two custom applications were developed: a chat application and a rating application. The chat application (See Figure 1) requested permissions one would expect from a chat application, however the functionality of the application did not match the permissions requested. The application is a text-only chat application which includes no functionality for uploading images, sharing contacts, voice notes and so forth. The application was published to the Google Play Store and listed as a text only chat application named Chatter. This application also contained an image of an open lock on the chat screen. This image indicated that the application is not making use of encryption and was selected from the Android Materials development icons.

Canteenrater (See Figure 2) allowed the students to give a star-rating for the university canteen. The application was also over-provisioned and blatantly requested permissions that one would not expect from a rating application. This application simply allowed users to give a rating value and a comment.

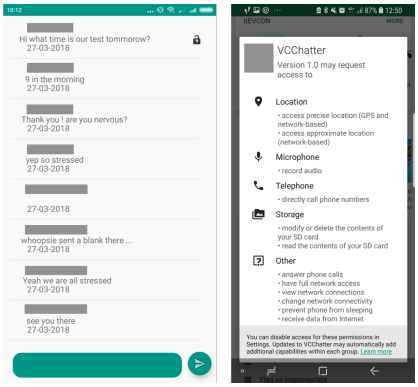

Figure 1: Screenshot of the Chatter app used during interviews and for the survey.

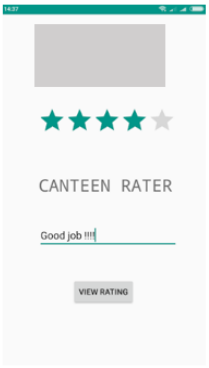

Figure 2: Screenshot of the Canteenrater app used during interviews and for the survey. .

3.3 Deception

Since we aimed to study the normal behavior of students, deception was introduced into the study. If we had informed the students that the study explored their perceptions and behaviors with mobile privacy and security, undue attention could have been drawn to these areas. To counter the phenomenon the participants were briefed that they were taking part in a usability study for two applications developed for the institution. The deception was revealed during the one on one interview or in a written disclosure at the end of the survey. A campus counselor was made available to all participants after the experiment. Any students who experienced emotional distress were directed to the counselor and had the option to exclude their data from the study. None of the participants needed the services of the counselor. The interview and observation participants were remunerated with a fifty rand canteen voucher redeemable at the institution's on campus canteen. We discuss our findings in the section that follows:

4 FINDINGS

4.1 Understanding of Permissions and Security

4.1.1 Students do not pay attention to application installation permissions. Only four out of 77 (5%) of the students paid attention to mobile permissions whilst they installed applications. 14 out of 77 (18%) of the surveyed students indicated that they would abort an installation due to discomfort with the permissions requested. Two out of 10 of the observed students denied the over-provisioned permissions for both applications and two out of 10 of the interviewed students listed the permissions of the applications as unusual. When we asked the interview candidates why they did not pay attention to the permissions they offered the following comments:

> "I never read those permissions, I just click yes, yes, yes."
>
> " Those things are irritating - I just want to get to try the app."

When we asked why they were not worried about installing applications without considering the permissions, many of the students comments such as:

> "No one is out to get me."

4.1.2 Students do not pay attention to run time permissions. We found a large disparity between what students believe they do and what they actually did. When seeing a list of permissions outside of the Play Store environment an overwhelming number of students indicated that they would not allow the mobile permissions used for our two mobile applications : 49 out of 77 (64%)for chat application and 55 out of 77 (71%) for rating application. This changed when we showed them screen-shots of the very same application permissions, taken from the Play Store. Then, 56 out of 77 (72%)of the students indicated that they *would* install the chat application and 40 out of 77 (52%) of the students indicated that they *would* install the rating application. Of those students who still chose not to install the applications, permissions was only a factor in 16 out of 77 (20%) for the chat application and 19 out of 77 (25%)for the rating application. Some of the reasons students provided for not installing the applications are as:

> " I do not buy food from the canteen."
>
> " I don't think that the application would be useful to me."

4.1.3 Students have become desensitized to permissions that are often requested. An interesting finding that emerged is that 9 out of 10 of the students referred to the dangerous permissions requested by the applications as *standard, default* or *expected* permissions. Some of their responses are:

> "Yes, they are the standard permissions that all applications ask for."
>
> "Yes, those are fine – they are the standard permissions".

When questioned further it emerged that students trust these permissions because they are requested by most applications. Over time, students have become desensitized to these permissions and now believe that these permission requests are safe. The list of permissions that students described as standard permissions is detailed below:

- Access to Camera

- Access to Microphone: Allows applications to turn the voice recorder on and off.
- Access to Storage: Allows application to read the files stored on the mobile device.
- Access to Wifi: Can turn wireless network on or off and make connections.
- Access to Location: Discloses the physical location of the user using GPS coordinates.
- Access to Phone Calls: Can make and accept phone calls on the mobile device.

The Android App Permissions Best Practices Guide instructs developers not to use more permissions than needed and to step back the functionality of their application for those users who elect to deny permissions. [3]. Unfortunately the open nature of the android markets and the lack of an in depth evaluation process makes it possible for developers to ignore these best practices [46].

4.1.4 Students are not aware that applications make use of more permissions than the explicitly requested permissions. None of the students were aware that applications make use of more permissions than those explicitly requested. Furthermore none of the students knew how to display the list of full permissions on their device nor where to look for the permissions used by each application. All the students were unnerved when they were shown the full list of permissions used by each application. The students responded with statements such as:

> "No!"
>
> "I seriously did not know that, this is so scary."

Gerber and Volkamer [18] found similar behavior in their study. They attributed these findings to the fact that other permissions (as the Play Store refers to protection level normal permissions) are hard to find and not disclosed to users. [4]. Fang et al [17] further explains that these unknown permissions could stealthily leak users private data.

4.2 Technical Ability with regards to permissions and privacy

4.2.1 Students do not match the permissions requested to the functionality of the application. None of the interviewed students matched the functionality of the applications to the permissions requested by the application. When this was further queried, most of the students indicated that the idea of matching permissions requests to the functionality of the application was not something they had ever thought about.

One out of 77 (1%) of the students noticed that the permissions requested by the chat application did not match its functionality . This is interesting, since we clearly stated that the chat application was text-only. Some of their comments were:

> "I would not install the app [sic] as a text only app does not need permission to camera."

13 Out of 77 (16%) noticed that the rating application was over provisioned. This likely due to the over provisioning of the application being extremely evident. The following comments provide more information on the above.

> " The app doesn't necessarily need any of those permissions to work "
>
> " I would ask myself why the app will need any of those permissions - and for what reason."
>
> "An application of this nature should not need access to contacts as well as camera and microphone as it only needs to rate the canteen. "

Liu et al [32] attributes similar findings to user's expectations and mental models. The students expected a chat application that requested access to certain permissions however, they did not expect the same permissions from a rating application. These students have created a mental model [26] of what permissions a chat application or rating app would require, the over provisioning matched their expectations and mental model. This clearly indicates that students will pay little attention to the actual functionality of an application versus the permissions that the application requests if their mental models and expectations are matched.

4.2.2 Students do not notice if updates change mobile permissions. 15 Out of 77 (33%) of the surveyed students indicated that they considered changes in mobile permissions when they updated mobile applications. One out of 10 of the observed students indicated that they checked if the permissions changed after an application updated. Unfortunately, none of the observed students could successfully show us where to check the mobile permissions used by each application. This finding can be attributed to the fact that Android based updates are now largely automatic. Android handsets now ship with the Automatic updates over Wi-Fi feature enabled by default. This setting allows applications to not only install patches or update features, but to also automatically update the dangerous permissions used by the application. A recent XDA article [14] explains the security loophole created by this default setting by stating that a Reddit user was able to automatically update the permissions of his android app. These updated permissions allowed him to format the storage of any device the application is installed on.

4.3 Student Understanding of Location Based Services

4.3.1 Students believe they consider location services, however the data indicates that they do not. When students were shown the Access to Location permission requested by each mobile application in a survey question, 59 out of 77 (77%) students indicated that they would not allow this permission for the text only chat app. A further 56 out of 77 (72%) indicated that they would not allow the permission for the rating application. However, in spite of these responses 56 out of 77 (72%) students elected to install the chat application listing the very same permissions they denied. Only 12 out of 77 (16%) students indicated that they consider location services when installing applications. Li et al [30] had similar findings in their study looking into the attack vectors created by LBS. They found that surprisingly few users paid attention to the applications on their handsets that made use of LBS. Many of the interviewed students indicated that they were not aware which applications on their mobile phones used LBS and most of them did not consider the applications that are pre-installed.

4.3.2 Students are unsure how location tracking services works. At least two out of 10 (20%)interviewed students indicated that they were not concerned with location services since they never turn it on for too long or only use it to check in quickly. None of these students paid attention to the fact their current location would be known regardless of how long they enabled the service for. Some of the comments offered were as follows:

> "I only turn my location on quickly to check in, then I turn it back off."
>
> "I don't leave it on all the time, only when I am out and about."

Further to this, 31 out of 77 (40%) surveyed students indicated that they were not worried about location services because: "No one is out to get them". Li et al [30] supports this finding by stating that users have little understanding around the danger posed by location based services.. No exploits are needed to track user locations and display individual identities, the data released by the LBS service was enough to gather the information.

4.4 Understanding of encryption as a security measure

4.4.1 Students do not know what encryption is nor do they recognize encryption symbols. 2 Out of 10 of interviewed students indicated that they knew what encryption was and provided a very vague explanation of encryption. The survey respondents provided inconsistent answers when asked if they would abort an install based on the lack or presence of encryption in a single survey question. The inconsistency was introduced in two survey questions in order to ensure that our findings were correct (the research questions listed both the presence and lack of encryption as a reason to not install an application). Mylonas [35] had similar findings, only

Table 1: Students displaying inconsistent encryption related answers

What would prevent you from installing an app from *HEI Name*?		
	Y	N
Presence of Encryption	4%	96%
Lack of Encryption	12%	85%

twenty two percent (22%) of his subjects understood or enabled the encryption features on their mobile devices. None of the observed and interviewed students noticed the open lock on the chat application's chat screen None of the students linked the lock to encryption. This is not a problem unique to South Africa or even to third world countries. The European Data Protection Supervisor (EDPS) [45] states that all mobile applications should use and adequately display the fact that they use encryption. The EDPS goes on to state that users recognize that "https" in a web browser URL indicates encryption**??**,however few mobile applications make use of consistent symbols to indicate whether encryption is present. The EDPS 2015 guidelines state that more should be done to explicitly show that applications make use of encryption [45]. The EDPS further urges developers to make use of encryption, especially for international connections. Developers could also include a short explanation of why encryption is important.

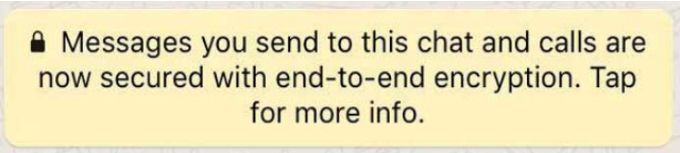

Figure 3: Example of WhatsApp using both an encryption icon and a short message to indicated the presence of encryption.

4.5 Overall student competency in terms of mobile permissions, encryption and location based services

Only two of the surveyed students and one of the interviewed students were consistent and competent in their answers when it came to considering privacy and security. Rashidi et al [39] found that three percent (3%) of their survey respondents consistently answered the security and privacy questions and could thus be seen as competent. This is an alarmingly small amount of Rashidi et al's and our population which speaks directly to the usability of the Android security and privacy ecosystem. These authors go as far as to recommend a secondary security measure to decide if applications should be placed in a probation setting before they can be deemed as safe.

5 DISCUSSION

In line with Kurkovsky's findings, it is clear that the security and privacy behavior of digital natives have not changed much. However, the mobile privacy and security landscape has changed and is now much more complex. The amount of mobile applications and in turn, malicious applications has grown from thirty-eight thousand available applications in 2009 to over three million applications in July of 2018 [1]. Popular applications such as Facebook, Twitter and LinkedIn have drastically altered their privacy statements [50] and machine learning algorithms now actively use the data we supply as we navigate the digital world [44]. If we consider these changes, it becomes evident that a good understanding of how digital natives approach mobile privacy and security is needed to inform security and privacy design decisions. We characterize these approaches below:

5.1 Digital natives lack the necessary technical skills to engage with mobile privacy and security.

Kurkovsky and Syta [29] found that digital natives lacked the technical skills to understand and safely use different authentication methods. We can expand on this finding by stating that digital natives lack the technical skills to properly engage with mobile privacy and security as a whole. Our findings indicated that digital

[1] https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

natives lacked the skills to recognize encryption symbols with none of the interviewed students recognizing the lock icon as an indicator for encryption. None of the students were able to navigate to and show the full list of permissions used by the applications installed on their phones. Students were further unable to explain to us how to toggle dangerous permissions on and off and could not explain how encryption works. It is this lack of skills that keeps this generation from being able to act securely and make informed decisions when they use mobile phones. It is true that they are well adapted to social media and can be seen as very able in the context of these platforms, however, this generation still has a lot to learn when it comes to the general privacy and security settings made available to them. This lack of skill leaves them vulnerable to threats such as: identity theft, ransomware, spyware, data leaks, viruses and a wide range of attacks. It is clear that mobile applications' privacy and security features need to be designed for better understanding. We need to create approaches that will actually be understood by and match the technical ability of digital natives, since our current approaches have clearly failed.

Lastly, it is imperative that Higher Education policy makers and institutions take cognisance of the fact that this generation of students require training specific to mobile privacy and security features.

5.2 Digital natives do not understand mobile and privacy features and therefore ignore them.

Our findings indicated that digital natives do not understand how mobile security and privacy works: They did not understand the reason for permissions and in turn did not pay the necessary attention to the permissions during the installation or use of an application. They failed to match the permissions of an application to its functionality and happily installed over provisioned applications. Lastly, they did not understand how Location Based services worked nor that their phone ships with applications that might have LBS enabled. Mylonas et al [35] had similar findings and agrees that users opt to ignore security features that they do not understand or find overwhelming. They further found that many of the participants in their study did not enable the encryption features available to them. Hanus et al [20] explains that users' privacy and security awareness plays a key role in their ability to protect themselves or to safely use technology. Chanderman and Van Niekerk [9] echo these findings by explaining that better security behavior is only possible with better security awareness.

Unfortunately our findings showed that the current methods of requesting permissions are not understood and therefore ineffective.

In order to possibly mitigate the above, the following should be considered: Permissions should not be requested in permission groups. It is true that Android no longer allows all the permissions in a permission group upon a single permission request [5], however permissions are still requested in permissions groups that show only one rationale for all the permissions existing within that group. For example, an application that requires access to answer phone calls will show the same rationale as an application that requires access to write to your voice mail. Students have no understanding of permission groups and do not even know that they exist. They therefore do not understand that the request they see does not explain exactly what the application will be able to access and can in fact be misleading. It might be better to list a rationale for each of the permissions in a group when an application requests only that permission.

Table 2: Android Phone Permission Group

Android Mobile Permission Group : Phone	
Phone	Read_phone_state
	Read_phone_numbers
	Call_phone
	Answer_phone_calls
	Add_voicemail
	Use_sip

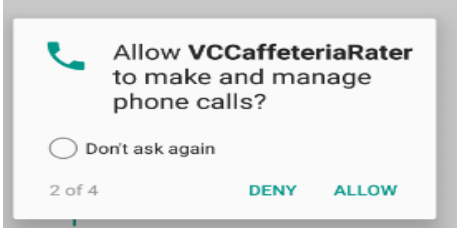

Figure 4: Phone Permission Group Rationale.

Digital natives do not understand the full extent of what they are allowing applications access to on their mobile phones. Android and Android developers should use better, more descriptive language in their permission requests. Each request should explain why the permission is necessary, what the permission will do and what will happen if the user elects not to allow the permission. Android does offer permission rationales to address this problem, however the language in the rationales are still not user friendly enough, and fail to communicate possible dangers of allowing unnecessary permissions[2]. These rationales are over-simplified and bunch permissions into groups which digital natives do not understand [3].

Lastly, HEIs should carefully consider the mobile applications that they prescribe. Institutions should take time to investigate the application in order to ensure that it employs good privacy and security standards.

5.3 Digital natives have been over exposed to application requests that violate their privacy and have become desensitized.

Our findings and those of Harris et al [22] indicate that digital natives have become desensitized to mobile permissions. Harris et al focuses on the end user's rationale that they have experienced no adverse effect when installing mobile applications and accepting

[2]Android Central. https://www.androidcentral.com/run-permissions-why-change-android-60-may-make-you-repeat-yourself Last Accessed 21 Sept 2018.

permissions. My study found that almost the entire list of Android's dangerous permissions are requested so frequently and by so many applications [21] that digital natives now believe that these are a set of standard or default permissions. They see these permissions as a step in the installation process, rather than a security and privacy feature that requires their attention. This has led to permission requests providing little or no security and privacy to digital natives as they allow these permissions by default.

5.4 Digital natives trust the authors of software and fail to act securely when security and privacy features are requested out of context.

The majority of the survey candidates and nine out of the ten interviewed students believed that Google checks every application that is uploaded to the play store. They trust that mobile developers take the time to develop and deliver safe and secure mobile applications that will not leak their data. This is a fairly concerning characteristic since the Cambridge Analytica [8] scandal clearly indicated the consequences of believing that the information you see and share is handled in a safe and secure manner. It is even more concerning if one takes a look at the applications currently available for download on the play store. Below is a snippet of the various available applications with an almost identical icon to that of Facebook's messenger- all produced by different authors. Students could inadvertently download the incorrect application and in turn provide unknown parties with valuable and private information. As mentioned before, students provided inconsistent

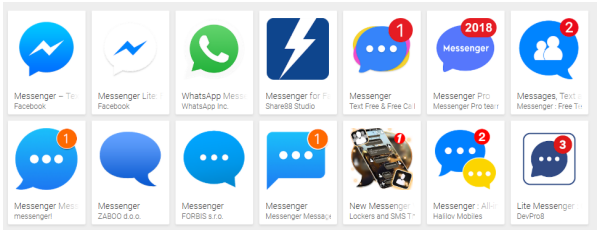

Figure 5: Similar Messenger Application Icons with Different Authors on the Google Play Store.

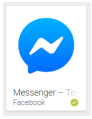

Figure 6: Actual Facebook Messenger App.

responses when they were asked if they would install the custom developed applications in two separate survey questions. The students did not notice that the permissions were identical and in fact for the same application. They were unable to navigate the change in the context with regards to permission requests. This means that HEIs can no longer assume that students will be able to safely navigate mobile application markets and higher education policy makers need to consider the fact that the drive for the uptake of technology in Higher Education needs to go hand in hand with policies to ensure that this is done safely.

5.5 Digital natives' need for instant gratification has consequences for privacy and security.

Santos and Rosati [42] argue that the need for immediate gratification is still one of the human race's largest decision biases. Digital natives grew up in a world where instant gratification is not only a possibility, but a standard [48]. Our study indicated that their attitude to security is no exception. Students admitted that they would rather accept the permissions or any other requested security feature to get the gratification of experiencing the application. By doing this students could have inadvertently installed malicious and possibly dangerous applications on their mobile phones. When students were asked if they would have acted in the same manner if the true nature of the applications were known upfront, almost all of them indicated that they would have acted very differently. They offered comments such as:

> "I would not have installed the application, I see how my actions were not smart."
>
> "It does not seem worth it now, does it. "

Santos and Rosati further state that humans have learned to wait for a better reward or lesser consequences in certain settings which Fang and Wang [16] explain as hyperbolic discounting. They explain that humans are more likely to overlook or withstand instant gratification if the rewards are more long term, however humans are much more likely to opt for immediate gratification in the short term. Unfortunately, the immediate access and quick turnaround time of application downloads and installations leads to a much higher likelihood of hyperbolic discounting taking place. If we consider the fact that over eighty percent (80%) of the students we observed installed the application with no regard for the permissions, it is clear that hyperbolic discounting does take place.

Unfortunately the presence of hyperbolic discounting means that any security feature aimed at providing protection to users which is paired with instant gratification will be ineffective.

5.6 Digital natives' definition of privacy is different than those of previous generations.

Both Kurkovsky and Palfrey [36] explain that digital natives' definition of security is different than it was for previous generations. They happily share their location, photographs, thoughts, music play-lists, political beliefs, etc online. Palfrey goes as far as to say that a radical paradigm shift took place and that this generation also has a very different expectation of privacy. It could be possible that this generation's sense of security has eroded [23] and that they are far easier to exploit than previous generations. Both Kurkosky and Syta [29] and ourselves noted that Digital natives displayed *lack of fear* or *carelessness* in their approaches to mobile privacy and security. We now believe that this *lack of fear / carelessness* is in fact a manifestation of these students eroded definition of privacy.

HEIs and policy makers should consider this finding when they prescribe applications to students. The onus lies on the institution to ensure that they prescribe applications that are not over provisioned and safe to use. Given the above discussions it is clear that there is still a lot of research that needs to be done in this area of privacy and security. We conclude our study and discuss some of the possible future works next.

6 CONCLUSIONS AND FUTURE WORK

Our findings were similar to those of Kurkovsky and Syta [29] who also found that digital natives were not tech-savvy and in many instances lacked the necessary skills needed to safely use mobile applications. However, our study represents an in depth look at how South African Higher Education students interacted with mobile privacy and security features by focusing specifically on application permissions, encryption and location based services. We offer a characterization of their behavior in order to inform HEIs, Higher Education Policy and mobile privacy and security designers.

We urge the above mentioned bodies to explore future works into Higher Education Policies. If these policies are going to mandate and drive the use of technology in HEIs, they should do so in an ethical and safe manner.

HEIs need to conduct research into and then design a program tailored to educating Digital natives about safe and secure mobile application usage and general safe and secure online behaviour.

Lastly, both the Higher Education and development communities need to introduce ethics to developers as soon as possible. HEIs that offer computer science and information technology related degrees need to include a section on ethics. Unfortunately, unethical behavior in this realm has far reaching consequences which are not always considered.

6.1 Limitations of the Study

This study only made use of students from a premier private higher education institution. These students all attended majority private schools and can be classed in LSM (Life Style Measurement) seven and eight (Middle to Higher income brackets). No students from the lower LSM's or public institutions form part of the study.

We take cognisance of the work done by Ahmed [1], however, South Africa has a large divide between the rich and poor in and turn the ICT services these groups have access to. Molawa [33] discusses the *first* and *third* world in Africa by describing the differences with regard to first and third world living. Within South Africa exist well developed, first world-like urban areas which are usually populated by affluent South Africans and do not necessarily match the populations discussed by Ahmed.

It is further possible that participants in the observation were more trusting of the applications because they were led to believe that the applications were being launched by the HEI they attend. This possibly could have led students to act in a less secure manner than they normally would.

This study made use of only millennials, which can be defined as individuals born roughly between 1981 and 1996 [49] and heavily influenced by the technology era. Because of this the findings of this study could possibly not be extrapolated to the population as a whole.

REFERENCES

[1] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 906–918.

[2] Android. 2018. Developers Guide Permissions Overview. https://developer.android.com/guide/topics/permissions/overview

[3] Android. 2018. Developers Permission Best Practices. https://developer.android.com/training/permissions/usage-notes

[4] Android. 2018. Manifest Permissions Change Wi-Fi Sate. https://developer.android.com/training/permissions/usage-notes

[5] Android. 2018. ReleaseNotes SDK Platform Release Notes. https://developer.android.com/studio/releases/platforms

[6] Miri Barak. 2018. Are digital natives open to change? Examining flexible thinking and resistance to change. *Computers & Education* 121 (2018), 115–123.

[7] Balbir S Barn, Ravinder Barn, and Jo-Pei Tan. 2014. Young people and smart phones: An empirical study on information security. In *2014 47th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 4504–4514.

[8] Carol Cadwalladr and E Graham-Harrison. 2018. The Cambridge Analytica Files. *The Guardian. Retrieved Mar* 17 (2018), 2018.

[9] Rajesh Chandarman and Brett Van Niekerk. 2017. Students? cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication* 2017, 20 (2017), 133–155.

[10] CHE. 2018. Counsel for Higher Education Review of Higher Education in South Africa. http://www.che.ac.za/sites/default/files/publications/Review_HE_SA_2007_Complete_0.pdf

[11] Amita Goyal Chin, Ugochukwu Etudo, and Mark A Harris. 2016. On mobile device security practices and training efficacy: An empirical study. *Informatics in Education* 15, 2 (2016), 235.

[12] Laura Czerniewicz, Neetha Ravjee, and Nhlanhla Mlitwa. 2006. ICTs and the South African higher education landscape. (2006).

[13] Ryan De Kock and Lynn A Futcher. 2016. Mobile device usage in higher education institutions in South Africa. In *Information Security for South Africa (ISSA), 2016*. IEEE, 27–34.

[14] XDA Developer Admin. 2014. XDA 2017 Year in review. https://www.xda-developers.com/play-store-permissions-change-opens-door-to-rogue-apps/

[15] Yao Du, Junfeng Wang, and Qi Li. 2017. An android malware detection approach using community structures of weighted function call graphs. *IEEE Access* 5 (2017), 17478–17486.

[16] Hanming Fang and Yang Wang. 2015. Estimating dynamic discrete choice models with hyperbolic discounting, with an application to mammography decisions. *International Economic Review* 56, 2 (2015), 565–596.

[17] Zheran Fang, Weili Han, and Yingjiu Li. 2014. Permission based Android security: Issues and countermeasures. *computers & security* 43 (2014), 205–218.

[18] Paul Gerber, Melanie Volkamer, and Karen Renaud. 2015. Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *ACM SIGCAS Computers and Society* 45, 1 (2015), 16–21.

[19] Vasileios Gkioulos, Gaute Wangen, Sokratis K Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou. 2017. Security awareness of the digital natives. *Information* 8, 2 (2017), 42.

[20] Bartlomiej Hanus and Yu "Andy" Wu. 2016. Impact of usersâĂŹ security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management* 33, 1 (2016), 2–16.

[21] Huikang Hao, Zhoujun Li, and Haibo Yu. 2015. An effective approach to measuring and assessing the risk of android application. In *Theoretical Aspects of Software Engineering (TASE), 2015 International Symposium on*. IEEE, 31–38.

[22] Mark A Harris, Robert Brookshire, and Amita Goyal Chin. 2016. Identifying factors influencing consumersâĂŹ intent to install mobile applications. *International Journal of Information Management* 36, 3 (2016), 441–450.

[23] Cullen Hoback. 2013. *Terms and Conditions May Apply*. iMDB.

[24] James Imgraben, Alewyn Engelbrecht, and Kim-Kwang Raymond Choo. 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology* 33, 12 (2014), 1347–1360.

[25] Shaheeda Jaffer, Dick Ng'ambi, and Laura Czerniewicz. 2007. The role of ICTs in higher education in South Africa: One strategy for addressing teaching and learning challenges. *International journal of Education and Development using ICT* 3, 4 (2007), 131–142.

[26] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. my data just goes everywhere:âĂÎ user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association Berkeley, CA, 39–52.

[27] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *International Conference on Financial Cryptography and Data Security*. Springer, 68–79.

[28] Ankita Khandelwal and AK Mohapatra. 2015. An insight into the security issues and their solutions for android phones. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*. IEEE, 106–109.

[29] Stan Kurkovsky and Ewa Syta. 2010. Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In *Technology and Society (ISTAS), 2010 IEEE International Symposium on*. IEEE, 441–449.

[30] Qing Li and Greg Clark. 2013. Mobile security: a look ahead. *IEEE Security & Privacy* 11, 1 (2013), 78–81.

[31] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 501–510.

[32] Bin Liu, Jialiu Lin, and Norman Sadeh. 2014. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?. In *Proceedings of the 23rd international conference on World wide web*. ACM, 201–212.

[33] Segametsi Molawa. 2010. The âĂIJfirstâĂİ and âĂIJthird worldâĂİ in Africa: knowledge access, challenges and current technological innovations in Africa. (2010).

[34] Wulystan P Mtega, Ronald Bernard, Andrew C Msungu, and Rachel Sanare. 2012. Using mobile phones for teaching and learning purposes in higher learning institutions: The case of Sokoine University of Agriculture in Tanzania. (2012).

[35] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis. 2013. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security* 34 (2013), 47–66.

[36] John Gorham Palfrey and Urs Gasser. 2011. *Born digital: Understanding the first generation of digital natives*. ReadHowYouWant. com.

[37] Wendy W Porter, Charles R Graham, Kristian A Spring, and Kyle R Welch. 2014. Blended learning in higher education: Institutional adoption and implementation. *Computers & Education* 75 (2014), 185–195.

[38] Patient Rambe and Aaron Bere. 2013. Using mobile instant messaging to leverage learner participation and transform pedagogy at a S outh A frican U niversity of T echnology. *British Journal of Educational Technology* 44, 4 (2013), 544–561.

[39] Bahman Rashidi, Carol Fung, and Tam Vu. 2015. Dude, ask the experts!: Android resource access permission recommendation with RecDroid. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*. IEEE, 296–304.

[40] Nkqubela Ruxwana and Mncedisi Msibi. 2018. A South African university's readiness assessment for bringing your own device for teaching and learning. *South African Journal of Information Management* 20, 1 (2018), 1–6.

[41] Ganesh Ram Santhanam, Benjamin Holland, Suresh Kothari, and Jon Mathews. 2017. Interactive visualization toolbox to detect sophisticated android malware. In *Visualization for Cyber Security (VizSec), 2017 IEEE Symposium on*. IEEE, 1–8.

[42] Laurie R Santos and Alexandra G Rosati. 2015. The evolutionary roots of human decision making. *Annual review of psychology* 66 (2015), 321–347.

[43] Pooja Singh, Santosh Singh, and Pankaj Tiwari. 2016. Discovering persuaded risk of permission in android applications for malicious application detection. In *Inventive Computation Technologies (ICICT), International Conference on*, Vol. 3. IEEE, 1–5.

[44] Chris Sumner, Alison Byers, Rachel Boochever, and Gregory J Park. 2012. Predicting dark triad personality traits from twitter usage and a linguistic analysis of tweets. In *Machine learning and applications (icmla), 2012 11th international conference on*, Vol. 2. IEEE, 386–393.

[45] European Data Protection Supervisor. 2014. EDPS Guidelines on the Protection of Personal Data Processed By Mobile Applications. https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_mobile_apps_en.pdf

[46] Darell JJ Tan, Tong-Wei Chua, Vrizlynn LL Thing, et al. 2015. Securing android: a survey, taxonomy, and challenges. *ACM Computing Surveys (CSUR)* 47, 4 (2015), 58.

[47] Junwei Tang, Ruixuan Li, Hongmu Han, Heng Zhang, and Xiwu Gu. 2017. Detecting Permission Over-claim of Android Applications with Static and Semantic Analysis Approach. In *Trustcom/BigDataSE/ICESS, 2017 IEEE*. IEEE, 706–713.

[48] Timothy Teo. 2016. Do digital natives differ by computer self-efficacy and experience? An empirical study. *Interactive Learning Environments* 24, 7 (2016), 1725–1739.

[49] Scott A Wheeler. 2017. Thriving Millennials: The Next Generation of Industry Professionals. *The Journal of Equipment Lease Financing (Online)* 35, 3 (2017), 1–6.

[50] Ran Yang, Yu Jie Ng, and Arun Vishwanath. 2015. Do social media privacy policies matter? Evaluating the effects of familiarity and privacy seals on cognitive processing. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 3463–3472.