Effects of Mobile Application Security Strategies on Privacy Invasion among Mobile Shop Operators in Nakuru East Sub-County, Kenya

Angela Wanjiku Kivindyo, Nelson Masese, John Kipkorir Tanui

Abstract*— Privacy invasion is an offence perpetrated by availability, access, and use of advanced mobile devices when they land in the wrong hands of people who have the intention of infringing into the space of either organizations or individuals. There has been infringement of people's rights by exposing their personal lives to third parties and the general public, a factor which is associated with detrimental effects, therefore the study sought to evaluate the effects of mobile application security strategies on privacy invasion with special focus on mobile shop operators within , Kenya, The study specifically sought to establish the effect of data encryption on privacy invasion and privacy settings on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya. The study was guided by the Technology Acceptance Model and control theory of privacy. The study adopted a cross-sectional research design, and was carried out inNakuru East Sub-County. The units of observation were mobile shops withinNakuru East Sub-County, while the units of analysis were operators of mobile shops. According to Nakuru East Sub-County Business Register (2019), there are 221 mobile shops within Nakuru East Sub-County. The researcher purposively selected one respondent (Operators) from each of the 221 mobile shops therefore the study population had 221 respondents. Nassiuma's (2000) formula was used to determine the sample size of 70 operators of mobile shops. The study used structured questionnaires to facilitate data collection. The pilot study was conducted in Eldoret town where questionnaires were issued out to 7 selected operators of mobile shops. The collected data was analyzed with the aid of the Statistical Package for Social Sciences. Descriptive statistics encompassing frequencies, percentages, means, standard deviations, and chi-square were used in the analysis. In addition, inferential statistics such as correlation and multiple regression analysis were used. From the findings the researcher concluded that, mobile shopoperators in Nakuru East Sub-County always use specific keys on all the data that they save on their phones. From the findings the researcher concluded that, mobile phone operators in Nakuru East Sub-County have embraced most of the mobile application security strategies on their phones and thus, lowering the chances of becoming victims of privacy invasion.The study recommended that mobile shop operators within Nakuru East Sub-Countyshould adopt data encryption security because it allows protection of data that they do not want anyone else to have access to. The researcher also recommended that mobile should adopt privacy setting techniques.

***Index Terms*— Data Encryption, Mobile Application Security Strategies, Privacy Invasion, Privacy Settings and Risk Analysis.**

Angela Wanjiku Kivindyo, Kabarak University, Kenya
Nelson Masese, Kabarak University, Kenya
John Kipkorir Tanui, Kabarak University, Kenya

I. Introduction

According to Moore (2008), privacy is defined as a moral claim or condition on others to desist from certain activities. It is also perceived as a derivative notion which is founded on basic rights like liberty or property. Arguably, privacy is contested. This is premised of the assertion that, it is transformable due to the ever changing technological and social conditions (Mulligan, Koopman& Doty, 2016).

Mobile application security strategy is defined as a comprehensive security solution for mobile applications which run on mobile devices like tablets and smartphones (Park, 2012). The object of mobile application security is to safeguard data of individuals and organizations that are stored in the aforementioned devices. The security of mobile applications entails how well the applications are protected from compromise by crackers, hackers and criminals

The security of mobile applications is paramount especially to users who transact online. If a mobile application is not properly encrypted, there may be breach of privacy with such information as credit card, passwords and other crucial company data being accessed by unauthorized persons. Indeed, Trust wave 2012 Global Security report affirms that there have been 300 data breaches in 18 countries around the world. It is further stated that most mobile platforms are targets for what is called banking Trojans. Statistics indicate that 29.6%, 10.5% and 7.6% of the mobile applications attacks are noted to come from the Russian Federation, the United States of America and Eastern Europe respectively (Park, 2012).

Australia has witnessed the upsurge of mobile phone handsets which is an opportunity for privacy invasion which, at times, borders on criminality. It is reported that there is hacking and/or stealing of mobile phones with the motive of accessing sensitive data. Despite the smartphones functioning as computers, security is an issue. These mobile phones are hacked with the intention of committing financial fraud and theft of identity. Indeed a report by Symantec shows that attackers have shifted their focus on mobile devices where they steal data through malware or smashing (Liu & Yao, 2017).

It is stated that 8.8 million South Africans experienced cyber-crimes and privacy invasion between the year 2015 and 2016. Further reports indicate that 47% of smartphone users in the country experienced mobile cyber-crime in the year 2013, either by being robbed their money or by privacy invasion. The vulnerability of the mobile device applications and little concern on security put by manufacturers make it cheap for criminals to hack the mobile devices (Symantec Report, 2016).

Mobile device applications are critical in spurring growth of businesses by easing marketing of different goods and services in Kenya. Businesses customize mobile applications to aid in performing specific tasks. Despite these good tidings, mobile applications are prone to attack or breach. A survey conducted by Waithaka and Mnkanda (2017) shows that there are security challenges that affect the use of mobile applications in electronic commerce. The security concerns relate to access of important business information by third parties, loss of money to fraudsters and receiving fake news intended for fraud. The insecurity of mobile applications perpetrated by a clique of fraudsters hinders their effective use in e-commerce.

A. Problem Statement

According to a global survey on Internet Privacy and Freedom of Expression, concerns have been raised with regard to the potential of invasive information technologies to violate women's privacy for sexual purposes, and also to violate 'enforced privacy' perpetuated by patriarchal cultures on women and girls (Mendel, Puddephatt, Wagner, Hawtin& Torres, 2012). Not only are the rights of women to privacy infringed on, but also those of men. Information technology has acted as a suitable platform through which privacy is invaded. It was reported by the Kenya Human Rights Commission (KHRC) that during the election week in 2013, more than 300,000 text messages per day were intercepted by the NCIC. Though the texts allegedly bordered on hate speech, the fact is, there was privacy invasion especially because NCIC has not clearly defined what hate speech is (KHRC, 2014). The fact that invasion of privacy is an offence punishable by law, makes it imperative to analyze how mobile applications security strategies influence the said invasion. There is hacking of personal accounts running on various mobile applications. This also is tantamount to privacy invasion. It is also imperative to note that past empirical studies have fallen short of adequately examining the subject of mobile application security on one hand, and privacy invasion on other hand, especially in the context of Kenya. In response to the acknowledgement of the problem of mobile application security breach and privacy invasion, and scarcity of empirical evidence to support the same, the present study purposes to examine various mobile application security strategies and how they affect privacy invasion.

H_{01}: There is no significant effect of data encryption on privacy invasion in Nakuru East Sub-County, Kenya

H_{02}: Thereis no significant effect of privacy settings on privacy invasion in Nakuru East Sub-County, Kenya.

II. LITERATURE REVIEW

The paper was based on technology acceptance model and control theory of privacy. Technology acceptance model was developed by Davis (1986). It is an information system model which theorizes how people accept and use technology. When users are presented with new technology, there are a number of factors that influence their decisions on when and how they will use it. These factors include; perceived usefulness which refers to the degree in which a person believes that using a particular system will improve his/her action and perceived ease of use which refers to the belief that using a particular system would not require any effort (Davis, 1989). The theory is relevant to the current study in that it helps to explain the development of advanced software testing techniques on privacy invasion. The mobile app developers should align the various features of the applications to the target consumers' characteristics. The application developed should provide opportunities for businesses to improve their service offering, that is, it should be applicable to the business environment and processes.

The control theory of privacy states that one has privacy if and only if one has control over information about oneself (Westin, 1967). According to Miller (1971) the theory is about the ability to control the circulation of information about oneself. It separates the concepts of liberty and solitude. In respect of mobile application security, control theory of privacy is applicable in that users of mobile applications or companies that develop such apps can control, to a certain extent, the information accessible to the public. Mobile devices' users can make use of passwords or other encryption measures to limit the access to specified applications that have sensitive information. However, on successful hacking users can lose control and consequently privacy of sensitive information stored in mobile devices. In this case the user has no absolute control of their personal information.

A. Data Encryption and Privacy Invasion

A study conducted by Basharat, Azam and Muzaffar (2012) examined data security and encryption in Pakistan. The study sought to identify the issues and threats in database security and how encryption is used at different levels to provide security. The study uses the analysis of past empirical literature to draw its findings. The results of the study were that encryption provides confidentiality, however, fails to give any assurance of integrity unless there is digital signature or hash function. The study also established that the use of strong encryption algorithms leads to a reduction in performance of the database system.

In Nigeria, a study conducted by Azeez, Abubakar (2018) analyzed encryption algorithms. The purpose of the study was to conduct a comparative assessment of Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms in order to identify the best in relation to its reliability, functionality and dependability. The implementation was carried out using C# and the study method used was experimental in nature. The results of the study found out that AES used the lowest time for encryption, RSA uses up the most encryption time. The study also indicated that the performance of RSA and DES algorithms was low. The study, therefore, concluded that AES was the most efficient algorithm.

A study conducted by Kazungu (2015) assessed information security and performance at Kenya power. One of the objectives of the study sought to establish the extent to which Kenya Power has secured its information assets. Descriptive research design was used for the study. The study sample comprised of 97 employees from Kenya Power who were selected using simple random sampling technique. Questionnaires were used as sources of data. The findings of the study revealed that the organization engages in encryption and protection of passwords.

B. *Privacy Settings and Privacy Invasion*

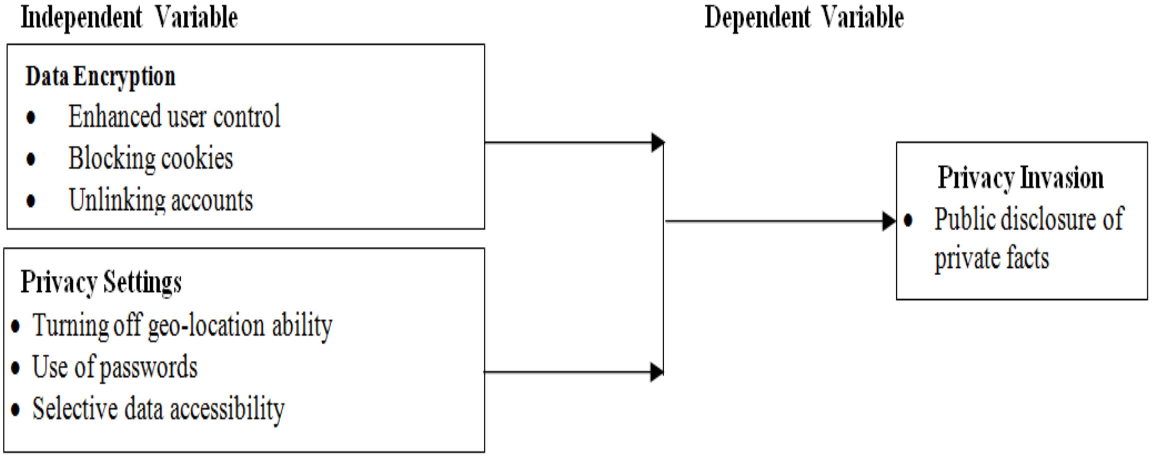
A study was carried out by Alsaleh, Alomar and Alarifi (2017) on understanding how security mechanisms are perceived and new persuasive methods by smart phone users in Saudi Arabia. The study aimed at investigating how smart phone users' privacy related decisions and security were influenced by their perceptions, understanding different security risks and their attitude. Quantitative data was collected for the study. From the analysis of the literature, there was a relationship between privacy and security related acts. The study also revealed that making the right security decisions might not be related to people's consciousness of the results of security warnings. The study suggested an implementation of additional persuasive approaches that focused on attending to technological and social aspects of the problem.

A study conducted by Nyokabi (2016) on the management of security and privacy concerns by smart phone and social media users in Nairobi. The purpose of the study was to investigate the challenges of security and privacy of smart phone users on social media experience and if the users actually protect themselves. The study adopted survey questionnaires and focus group discussions as the methods of data collection. A sample population of 160 respondents aged between 18-35 years who were active social media users and had access to smart phones and was taken. The findings revealed that people were aware of some threats to privacy on social media and smart phones. It was recommended that there was a need for more awareness and education on the impact of digital footprint on personal, financial and professional lives of users.

A study was undertaken by Waithaka (2013) on internet use among university students in Kenya. The study was aimed at finding out internet usage among the students at the University of Nairobi. The study adopted quantitative technique. A survey using questionnaires was carried out among 381 students and interviews conducted with the library staff of the university. The findings of the study established that the level of awareness that was offered in school on internet services was remarkable. The study further revealed that students used the internet to do research, study and also messaging their peers which could be public or private, depending on their privacy settings. The study recommended a formal internet training and free internet access to all the students.

A study was done by Osho, Yisa, Ogunleke and Muhammad (2016) on mobile spamming in Nigeria. The purpose of the study was to investigate the incidences of spam messages. Questionnaires were used to collect primary data. From a population of 270 mobile users, a sample of 191 users was used for the study. The study found out that all the mobile subscribers received spam SMS. It was also revealed that only a few mobile-users report cases of fraudulent spam messages to network providers or security agencies. The study recommended that guidelines and regulations needed to be reviewed so as to manage spam SMS.

C. *Conceptual Framework*



The study adopted a cross-sectional research design. The rationale of adopting this design is premised on the assertion that cross-sectional studies provide a clear snapshot of the outcome and the characteristics associated with it, at a specific point in time (Hall, 2008). The study was carried out in Nakuru East Sub-County. The units of observation were mobile shops within Nakuru East Sub-County; while the units of analysis were operators of mobile shops. According to Nakuru East Sub-County Business Register (2019), there are 221 mobile shops within Nakuru East Sub-County. The researcher purposively selected one respondent (Operators) from each of the 221 mobile shops therefore the study population was 221 respondents. The operators were selected since they are involved in the day to day operations of the mobile shops. Nassiuma's (2000) formula was used to determine the sample size of 70 operators of mobile shops. A self-designed, structured questionnaire was used to facilitate collection of requisite data. The pilot study was conducted amongst purposively selected operators of mobile shops in

Eldoret town. Structured questionnaires were used to facilitate data collection from the sampled respondents. The Statistical Package for Social Sciences (SPSS) tool was employed to facilitate processing and analysis of the collected data. Both descriptive and inferential statistics was used

III. RESULTS

Response Rate

The study administered 70 questionnaires for data collection. However, 62 questionnaires were properly filled and returned. This represented 89% overall successful response rates

Table 4.1: Duration in the mobilephone business

Duration	Frequency	Percentage
Less than 1 Years	20	33
1-5 Years	22	35
6-10 Years	12	19
More than 10 years	8	13
Total	**62**	**100**

According to the findings, 20 (33%) of the respondents indicated that they have been selling mobile phones for less than 1 years, 22(35%) of the respondents indicated that they had been selling mobile phones for 1-5 years, 12(19%) of the respondents indicated that they had been selling mobile phone for 6-10 years while 8(13%) of the respondents indicated that they have been operating a mobile shops for more than 10 years. The duration of service an individual has worked determines his/her capacity. Employees who have longer working experience tend to have better skills. This shows that majority of the respondents had been operating mobile shops for less than 1 years.

Data Encryption on privacy Invasion

Statement	SA %	A %	U %	D %	SD %	Mean	Std
My mobile device has strong data/file encryption capability, where only people with certain key can access the said data.	26	47	17	10	0	3.887	0.907
My device is installed with software that enables effective blocking of cookies.	37	45	13	5	0	4.113	0.870
I always use specific keys on all the data that I save on my phone.	55	42	0	0	8	4.516	0.565
My device has enhanced user control, meaning that I have a large room of controlling who can and who cannot access data stored on my phone	57	37	6	0	0	4.500	0.621
Most of the time, I block cookies that pop up on my device	39	44	11	6	0	4.145	0.866
Privacy Invasion overall mean						**4.232**	**0.766**

According to the findings, majority of the respondents (73%) agreed that their mobile device has strong data/file encryption capability, where only people with certain key can access the said data with a mean of 3.887 and the standard deviation of 0.907. The findings concurs with, Asikoyo (2016) who observed that encryption scrambles text to make it unreadable by anyone other than those with the keys to decode it, and it’s becoming less of an added option and more of a must-have element in any security strategy for its ability to slow down and even deter hackers from stealing sensitive information. The findings further indicated that majority of the respondents (82%) agreed that their device are installed with software that enables effective blocking of cookies. with a mean of 4.113 and the standard deviation of 0.870. In addition majority of the respondents (97%) agreed that they always use specific keys on all the data that they save on their phone with a mean of 4.516 and the standard deviation 0.565. The findings further indicated that majority of the respondents (94%) agreed that the their device has enhanced user control, meaning that the respondents have a large room of controlling who can and who cannot access data stored on their phone with a mean 4.500 and the standard deviation of 0.621.

In addition majority of the respondents (83%) agreed that the most of the time, they block cookies that pop up on their device with a mean of 4.145 and the standard deviation of 0.866. The standard deviation ranged from 0.565 to 0.907 indicating that the dispersion of the respondents from the mean was minimal. This implies that data encryption affects privacy Invasion. The findings are in line with Mutua(2015) study who noted that most mobile users in Kenya often block cookies that pop up on their device while using the online platforms. Most modern websites use cookies in some way, and it is unlikely that the majority of internet users even notice cookies working away in the background as they browse from site to site. Until now it has been up to individual users to either block or allow cookies using settings in their internet browser.

Privacy Settings on Privacy Invasion

Statement	S A %	A %	U %	D %	SD %	Mean	Std
My mobile phone has the option of turning off accessibility of the phone's location	37	34	10	16	3	3.855	1.185
I frequently use passwords to safeguard the data stored on my phone.	55	34	8	3	0	4.403	0.778
I sometimes select the type and amount of data which can be accessed by outsiders.	44	46	7	3	0	4.307	0.738
I often restrict sharing of data on my location.	37	44	16	3	0	4.145	0.807
I sometimes accept privacy related pop-ups that regularly feature on the screen of my device.	55	33	7	5	0	4.387	0.869
Privacy Invasion overall mean						**4.219**	**0.875**

According to the findings majority of the respondents (71%) agreed that their mobile phone has the option of turning off accessibility of the phone's location with a mean of 3.855 and a standard deviation of 1.185. According to Xiaoman, (2017) in mobile accessibility, screen contents are displayed in Braille in a way that will give you an idea of visual information such as format, hierarchy, control type, and phone location. In this mode, mobile speak sends information to the display that is relevant to the current cursor position. The information sent includes things such as control type, dialog name, or number of items in a list (where the list index is not really displayed visually) and the options for turning off the mobile location.

Majority of the respondents (89%) also agreed that they frequently use passwords to safeguard the data stored on their phone with a mean of 4.403 and a standard deviation of 0.778. They further agreed (90%) that they sometimes select the type and amount of data which can be accessed by outsiders. with a mean of 4.307 and a standard deviation of 0.738. According to Konglin (2017) most of the mobile users frequently use password to secure their data such as copies of their driver's license, employer data, insurance details, social security card, bank account information and passwords on their mobile device

In addition majority of the respondents (81%) agreed that they often restrict sharing of data on my location with a mean of 4.145 and a standard deviation of 0.807. Majority of the respondents (88%) also agreed that they sometimes accept privacy related pop-ups that regularly feature on the screen of my device with a mean 4.387 and a standard deviation of 0.869. The finding agrees with Arif(2016) study which found that only a few mobile-users report cases of fraudulent spam messages to network providers or security agencies and some of the mobile subscribers received spam SMS and accept the privacy related to the pop-ups that regularly feature on the screen of my device.

Privacy Invasion

Privacy Invasion	SA (%)	A (%)	N (%)	D (%)	SD (%)	Mean	Std.
I have in several occasions experienced privacy breach when using my mobile device.	58	24	8	4	6	4.177	0.912
I have never experienced my private data or information stored in my mobile device being disclosed to the public.	40	48	4	8	0	3.984	1.032
I have experienced impersonation of my identity.	50	34	8	4	4	4.145	0.921
Third parties occasionally intrude into the content of my mobile device.	54	36	2	5	3	4.563	.608
I have experienced presentation of false information regarding me on mobile device.	48	40	3	5	4	4.181	.513
I am greatly concerned by invasion of my privacy by unsolicited persons/entities.	58	24	8	4	6	4.177	0.912
Invasion of my privacy through mobile device has greatly affected my day-to-day life.	40	48	4	8	0	3.984	1.032
Privacy Invasion overall mean						**4.173**	**0.8471**

From the findings 58% of the respondents strongly agreed that they have in several occasions experienced privacy breach when using my mobile device, 24% agreed 8% of the respondent were neutral 4% disagreed while 6% strongly disagreed (mean=4.177, SD=0.912). From the finding 40% of the respondents strongly agreed that they have never experienced private data or information stored in their mobile device being disclosed to the public, 48% agreed, 4% were neutral while 8% disagreed (mean=3.984, SD=1.032). On the same note, 50% of the respondents strongly agreed that they have experienced impersonation of their identity, 34% agreed 8% were neutral 4% disagreed while 4% strongly disagreed (mean=4.145, SD=0.921).

The study sought to find out whether third parties occasionally intrude into the content of their mobile device. From the findings 54% of the respondents strongly agreed, 36% agreed, 2% were neutral, 5% did not agree while 3% strongly disagreed (mean=4.563, SD=0.608). Moreover, 48% of the respondents agreed that they have experienced presentation of false information regarding on their mobile device, 40% agreed, 3% were neutral 5% did not agree while 4% strongly agree (mean=4.181, SD=0.513). Further, the study findings revealed that 58% of the respondents strongly agreed that they are greatly concerned by invasion of their privacy by unsolicited persons/entities, 24% agreed 8% of the respondent were neutral 4% disagreed while 6% strongly disagreed (mean=4.177, SD=0.912). From the finding 40% of the respondents strongly agreed that invasion of their privacy through mobile device has greatly affected my day-to-day life 48% agreed, 4% were neutral while 8% disagreed (mean=3.984, SD=1.032). The findings are congruent to those of Ratemo (2015) study which found out that most of the respondents reported that have in several occasions experienced privacy breach when using my mobile device.

Correlation Analysis

Data Encryption on Privacy Invasion

		Privacy Invasion
Data Encryption	Pearson Correlation	-.323*
	Sig. (2-tailed)	.000
	N	62

*. Correlation is significant at the 0.05 level (2-tailed).

As indicated in Table 4.10, the study indicates that there was a negative and statistically significant correlation between data encryption and privacy invasion of the mobile users in Nakuru East Sub-County. ($r = -.323$; $p < 0.05$). This implies that an increase in data encryption will result to reduction in privacy invasion. The findings of the study concurs with to Zappala, (2018) study which noted that, encryption of health electronic records resulted to reduction in privacy and protection from issues such as theft, data breaches, loss, inaccuracies, exposure of personal data and medical identity.

Privacy Settings on Privacy Invasion

		Privacy Invasion
Privacy Setting	Pearson Correlation	-.441*
	Sig. (2-tailed)	.000
	N	62

*. Correlation is significant at the 0.05 level (2-tailed).

The study as shown in Table 4.18 established that a strong negative correlation existed between Privacy setting and privacy invasion ($r = -0.441$; $p < 0.05$). The results of the correlation analysis indicated that better privacy setting improve the privacy invasion of the mobile users in Nakuru East Sub-County. The findings is in agreement with Venkat, Pichandy, Barcla, and Jayaseelan (2014) study on Facebook privacy management the study revealed that privacy setting had a positive relationship in protecting the data of the mobile users in Facebook accounts.

Regression Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Variance Inflation
		B	Std. Error	Beta			
1	(Constant)	1.195	.130		9.165	.796	
	Data encryption	-.047	.023	-.082	-2.026	.023	1.813
	Privacy settings	-.439	.230	.360	-1.909	.003	1.976

The interpretations of the findings indicated follow the following regression model.

$Y=1.195 - 0.047 X_1 -0.439X2$

According to the intercept (β_0), when the four independent variables are held constant, the value of privacy invasion among the mobile users in Nakuru East Sub-County will be 1.195. In addition, holding all the other independent variables constant, a unit increase in data encryption would lead to a -.047 reduction in privacy invasion among the mobile users in Nakuru East Sub-County, Kenya. Further holding all the other variables constant, a unit increase in privacy setting would lead to a -0.439 reduction in privacy invasion among the mobile users in Nakuru East Sub-County, Kenya. From these findings we can infer that data encryption is affecting privacy invasion among the mobile users in Nakuru East Sub-Countymost, followed by pprivacy settings, risk analysis and advanced software testing techniques

Hypothesis Testing

From the findings the p-value for data encryption was

0.023 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis (H01) and concluded that data encryption has a significant effect on privacy invasion in Nakuru East Sub-County.

The study also found out that the p-value for privacy settingswas 0.003 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis (H04) and concluded that privacy setting has a significant effect on privacy invasion in Nakuru East Sub-County, Kenya.

IV. CONCLUSION & RECOMMENDATION

Conclusion

From the findings the researcher concluded that, mobile phone users in Nakuru East Sub-County always use specific keys on all the data that I save on my phone. Their device has enhanced user control, meaning that they have a large room of controlling who can and who cannot access data stored on their phone and most of the time, they block cookies that pop up on my device. From the Hypothesis test the researcher concluded that data encryption has a significant effect on privacy invasion in Nakuru East Sub-County.

Based on the findings on the effects of privacy setting on privacy invasion the study concluded that mobile users in Nakuru East Sub-County sometimes select the type and amount of data which can be accessed by outsiders. They often restrict sharing of data on my location. Sometimes they accept privacy related pop-ups that regularly feature on the screen of my device. Finally it was concluded that there was a strong positive correlation existed between privacy setting and privacy invasion ($r = -0.441$; $p < 0.05$). The results of the correlation analysis indicated that better privacy setting reduces cases of privacy invasion of the mobile users in Nakuru East Sub-County.

Recommendation

The study recommended that mobile shop operators within Nakuru East Sub-County should adopt data encryption security because it allows protection of data that they do not want anyone else to have access to. As businesses people it will help them to protect corporate secrets and secure classified information, and many individuals use it to protect personal information to guard against things like identity theft. The researcher recommended that mobile phone users ought to adopt privacy setting techniques because it will help them to detect when their devices are being hacked and take measures to protect themselves online from malicious cyber attackers.The researcher recommended that a study should be conducted on the management of security and privacy concerns by smart phone and social media users in Nakuru East Sub-County.

REFERENCES

[1] Alsaleh, M., Alomar, N., &Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. Plosone , 12 (1), 1-35.

[2] Azeez, N. A., &Abubakar, A. B. (2018). Comparative analysis of encryption algorithms. Journal of Informatics and Communication Technology, 6(1), 16-30.

[3] Basharat, I., Azam, F., &Muzaffa, A. W. (2012). Database Security and Encryption:A Survey Study. International Journal of Computer Applications, 47(12), 28-34.

[4] Davis, F. D. (1989). Peerceived usefulness, perceived ease of use and user acceptance of information technology. MIS Quartely, 13(3), 319-340.

[5] Kazungu, A. G. (2015). Information security and performance at Kenya Power. Unpublished MBA Thesis, University of Nairobi, Nairobi.

[6] Liu, L.C., & Yao, D. (2017). Enterprise data breach: Causes, challenges, and prevention and future directions. WIREs Data Mining Knowledge Discovery, 7 (5).

[7] Mendel, T., Puddephatt, A., Wagner, H., & Torres, N. (2012). Global Survey on Internet Privacy and Freedom of Expression. Paris: The United Nations Educational, Scientific and Cultural Organization.

[8] Miller, A. (1971). The Assault on Privacy. Cambridge: Harvard University Press.

[9] Mulligan, D.K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. Phil. Trans. R. Soc. A, 374.

[10] Mutua , V. (2013). An implementation of advanced encryption starndards in mobile communication: Secure messaging application. Unpublished Master of Science Thesis, University of Nairobi, Nairobi

[11] Nassiuma, K. (2008). Survey Sampling: Theory and Methods. Nairobi, Kenya: Nairobi University Press.

[12] Nyokabi, M. G. (2016). The Management of Security and Privacy Concerns by Smart Phones and Social Media Users in University of Nairobi. Unpublished Master of Arts thesis, University of Nairobi, Nairobi.

[13] Osho, O., Yisa, L. V., Ogunleke, O. Y., & Muhammad, S. (2016). Mobile spamming in Nigeria: An empirical Survey.

[14] Park, M. (2012). Mobile application security: Who, how and why. Trustwave Retrieved 30th January, 2019 from https://www.owasp.org/images/c/cf/ASDC12Mobile_Application_Security_Who_how_and_why.pdf

[15] Venkat, A., Pichandy, C., Barclay, F. P., &Jayaseelan, R. (2014). Facebook Privacy Management: An Emoirical Study of Awareness, Perception and Fears. Global Media Journal, 5 (1), 1-20.

[16] Waithaka, S.T.,&Mnkanda, E. (2017). Challenges' facing the use of mobile applications for e-commerce in Kenya's manufacturing industry. EJISDC, 83 (1), 1-25.

[17] Westin, A.F. (1967). Privacy and Freedom. New York: Atheneum Press