Android applications access permissions as a mechanism for smart market intelligence.

أذونات وصول تطبيقات الأندرويد كآلية للاستخبار الذكي للأسواق.

Hichem MEKKI, (University of Chlef), ***h.mekki@univ-chlef.dz***

Received: 18/08/20 ; Accepted for reviewing16/10/20 ; Accepted for publishing: 30/09/21

Abstract:

This study aims to analyze the nature of data that applications seek to access. It will also determine the extent of exploitation of the Algerian community for these applications, their awareness of the terms of use, and the risk of accepting conditions for running applications. This study will be conducted on a sample of 259 individuals, where data will be analyzed using descriptive and inferential statistics to achieve the objectives of the study, which allows access to results that enable us to propose recommendations on the subject under consideration.

Keywords: Android applications; terms of use; access permissions; smart market intelligence.

JEL classification code: M30, C8.

Hichem MEKKI,
e-mail: h.mekki@univ-chlef.dz

1. Introduction

The manufacturers of digital devices depend on information systems such as Android and IOs as a platform to exploit and run these devices, through which they develop services for users, knows as First-Party App. In addition, they can rely on a partnership with free-lancing developers to offer similar services at device-level known as Second-Party Apps. On the other hand, the developers who offer applications to the users for their devices on electronic stores, whether free or for sale, these are called Third-Party Apps.

To run these applications, the user must agree to certain conditions that are set by the developer to ensure that the application performs its essential task (Wang, Cao, & Zhang, 2005, pp. 425–436). These conditions revolve around the possibility of having the developer access and exploit certain personal data—which is considered to be a matter of privacy to the user (Zhang, Shen, Wang, & Yong, 2016, pp. 1281–1293). Based on this, privacy and the protection of data is a field of paramount importance to social activists and researchers.

Studies have shown that users often check Privacy Policy and believe that their personal information is protected via specific methods, and assume that developers and website-owners do not share the user's personal data with other parties—evidently; it is the opposite case (Turow, Hoofnagle, Mull, Nathaniel, & Grossklags, 2007, pp. 723-724). This is what another study has confirmed, in other terms, it has shown that the user is unaware of their personal data is managed by the app's developers while displaying a high level of reliability (King, Lampinen, & Smolen, 2011, pp. 20-22). However, a study though it arrived at similar results, it has shown that the user often does not read the terms and conditions of usage (Kesswani, Lyu, & Zhang, 2018). Moreover, this information can be used to develop malware (Peng, Zeng, Sun, Huang, Wang, & Tian, 2018, p. 91), since Android devices have become a major target for malignant software (Gamao, 2018), and the latter does not notify the user of data leaks (Sakamoto, Okuda, Nakatsuka, & Yamauchi, 2014, pp. 55-69).

Privacy Policy is more of a corporates' way to avoid the responsibility that it is a way to guarantee the users' data privacy (Tene & Polonetsky, 2012, p. 68). In this respect, it is worth mentioning that the exploitation of users' data is not restricted to what data the user consents to declare, for that the latter have become easier to understand than the users' digital devices due to a technology called Streams of Sensor Data, such as images, audios, and the activities the device senses around itself even (Krishnan & Cook, 2012, pp. 138-154).

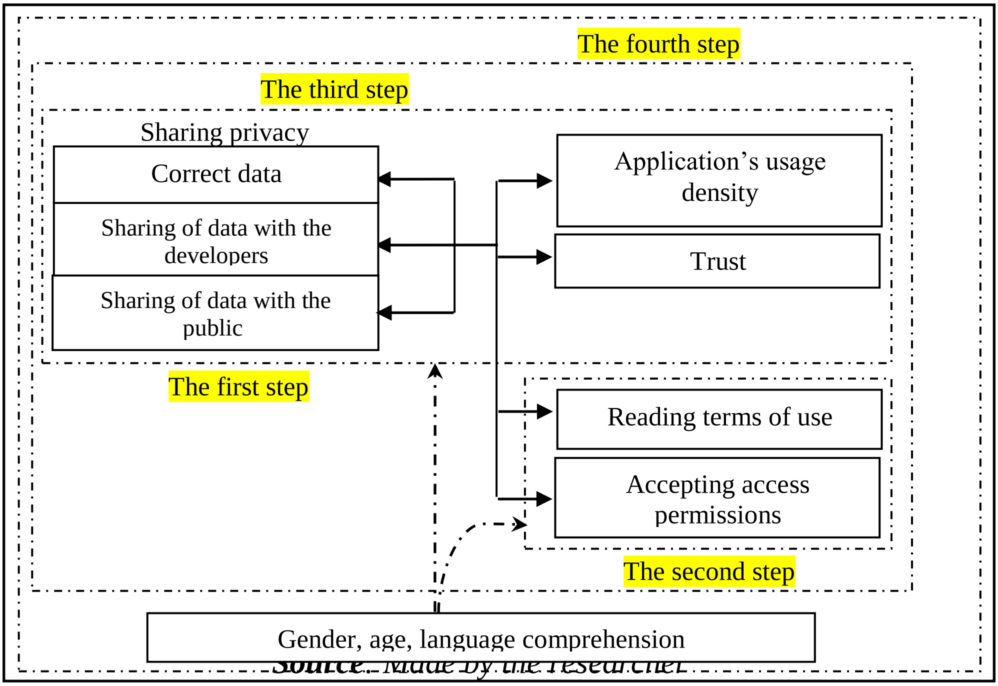
The user's data that applications can access are, for example, short messages, contacts, videos, saved emails on device, etc. (Gruschka, Iacono, & Tolsdorf, 2018, p. 02). within the condition of usage, some applications request access to certain user's data that are not essential to the app's function (Felt, Chin, Hanna, Song, & Wagner, 2011, pp. 627–638), and this poses difficulties for the user to pinpoint the actual conditions of usage that are necessary for the app, and in consequences, this leads to the user accepting all of them (Felt, Ha, Egelman, Haney, Chin, & Wagner, 2012, p. 03), meaning, the developer will have access to all of the data that is requested by the application at the time of accepting app's permission. In regard to this, a study has unraveled that there is a possibility to remove or disable the various permissions that applications request to protect users' privacy while maintaining the functionality of the application (Qatrunnada, Tousif, Kelly, Apu, & Reite, 2017, pp. 119–137). In spite of that, access permissions on digital devices still pose a threat to privacy, and such systems are exploited and used as mechanisms of the smart marketing intelligence. From this starting point, a question is asked: is the Algerian society aware of the terms and conditions of usage of the applications on their devices?

This study aims to determine how exploitative the Algerian is of the applications, the extent of the data they share, their awareness of terms of use, and the risks of accepting access permissions. The importance of this study is derived from the fact that applications allows for collecting data of users and accessing their privacy, which permits the penetration of societies, and posing a form of control on their lifestyles.

2. Study Methodology

We resorted to the analytical descriptive method by describing the reality of the Algerian society's stance to the study's variables and analyzing it statistically by following the steps illustrated in the following figure:

***Figure 01**: The Proposed Model of the Study.*


The fourth step
The third step
Sharing privacy
Correct data
Sharing of data with the developers
Sharing of data with the public
Application's usage density
Trust
The first step
Reading terms of use
Accepting access permissions
The second step
Gender, age, language comprehension

Source: Made by the researcher

The figure above represents the proposed model of the study, which is constructed based on the practical steps that the application's user goes through from downloading the application to launching it.

In the first step, the analysis is concerned with the sample, the participants' attitude, regarding how often they use the applications, their trustfulness in the application, and also, how much privacy they share. The second step is related to analyzing the participants' attitudes regarding reading the terms of use and accepting access permissions. The third step is about identifying the extent of awareness the participants have regarding the risks that accompany the acceptance of access permissions. The fourth step dealt with studying the statistical differences among the participants' tendencies toward the variables in due to their personal variables; testing the correlation between all of the study's variables, Using the multi-dimensional scaling to reform the model and present a comprehensive conception of the study.

2.1 Data Collection and Measurement: Data has been collected by means of a questionnaire that constitutes five sections, where the first four sections involve 25 questions addressed to measure the study's variables via the Interval Scale (Five-Level Likert Scale), while the fifth section contained 03 questions concerned with collecting personal data about the participants via the Nominal Scale.

An electronic questionnaire was prepared using Google Form, and was extended and shared on social media both in Arabic and French, of course, we have exclusively targeted the Algerian society, and this has taken place from September 2019 to January 2020. The size of the sample has reached 259 participants. Moreover, the measurement tool's reliability has been tested and confirmed using Cronbach's Alpha, wherein the coefficient's value has reached 0.86 which exceeds 0.6.

2.2 Data Analysis: In this respect, numerous statistical tools have been used, such as: Descriptive Statistics (Mean, Standard Deviation, Variance, Ratios, Frequencies, and Average), Inferential Statistics (ANOVA, Student's t-test for Independent (unpaired) and Paired Samples, Correlation Factor, Scheffé's Method, Hierarchical Classification, Multi-Dimensional Scaling (MDS), and Factor Analysis for Principal Components.)

3. Study Results

3.1 Display of Personal Data

3.1.1 Gender and Age:

***Table 01**: Distribution of the sample based on Gender and age*

Age (mean)	Gender (%)	
31,4934	Male	58,7
28,5421	female	41,3
30,27	Total	100

***Source**: Made by the researcher according to the outputs of SPSS software*

The table above shows that the majority of the sample is males (58.7%) whose age average amounts to 31.49 years, as for females (41.3%), the age average totals to 28.54 years. The overall sample's age average then equals to 30.27 years. These results indicate that the sample is characteristically youthful, and that the percentage of male's and female's participation is convergent, which has served the study's examinations better.

3.1.2 Level of Language Comprehension: the table below shows the results of this analysis.

***Table 02**: Level of Language Comprehension of the study sample*

	Ar (median=4,65)	Fr (median=3,51)	Eng (median=3,21)
I understand nothing	0,8	2,7	1,5
Weak	0,8	12,0	21,6
medium	5,4	34,4	39,0
good	25,1	36,3	29,7
Excellent	68,0	14,7	8,1
Total	100,0	100,0	100,0

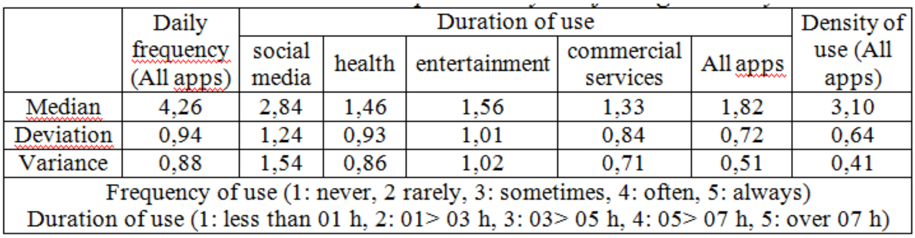
***Source**: Made by the researcher according to the outputs of SPSS software*

It is exhibited that the majority of the sample (68%) have an excellent comprehension of the Arabic language (Median = 4.65), and this is due to Arabic being the native language of Algeria; whereas French is the most comprehended foreign language known by the sample (M = 3.51), followed by the English language with an average level of comprehension by the sample (M=3.21).

3.2 The Descriptive Analysis of the Study's Variables:

3.2.1 Usage Density: The analysis of the usage density has unveiled the results shown in the table below:

***Table 03**: The Descriptive Analysis of Usage Density.*



	Daily frequency (All apps)	Duration of use					Density of use (All apps)
		social media	health	entertainment	commercial services	All apps	
Median	4,26	2,84	1,46	1,56	1,33	1,82	3,10
Deviation	0,94	1,24	0,93	1,01	0,84	0,72	0,64
Variance	0,88	1,54	0,86	1,02	0,71	0,51	0,41

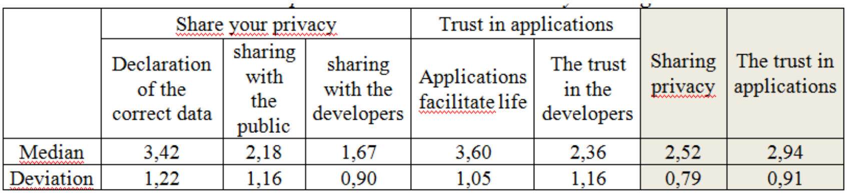
Frequency of use (1: never, 2 rarely, 3: sometimes, 4: often, 5: always)
Duration of use (1: less than 01 h, 2: 01> 03 h, 3: 03> 05 h, 4: 05> 07 h, 5: over 07 h)

***Source**: Made by the researcher according to the outputs of SPSS software*

From the table above, it is clear that the sample possesses a medium attitude concerning the density of usage of Android applications (M=3.10) without marking a high values in either variance or standard deviation. This variable is expressed in terms of two dimensions. The first dimension expresses the frequency of daily use, which value is high (M=4.26), where 47.1% of the sample *always* use these applications, and 24.7% *normally* do (Table 01 in the Appendices list). The second dimension is represented by low frequency of use (M=1.82), where the duration of use goes between 1h to 3h daily, and is presented in first hand by the use of Social Network applications (3h to 5h daily).

3.2.2 Privacy Sharing and Trust: The analysis of this variable has uncovered the results shown in the table below:

***Table 04**: the Sample's Attitude towards Privacy sharing and Trust.*



	Share your privacy			Trust in applications		Sharing privacy	The trust in applications
	Declaration of the correct data	sharing with the public	sharing with the developers	Applications facilitate life	The trust in the developers		
Median	3,42	2,18	1,67	3,60	2,36	2,52	2,94
Deviation	1,22	1,16	0,90	1,05	1,16	0,79	0,91

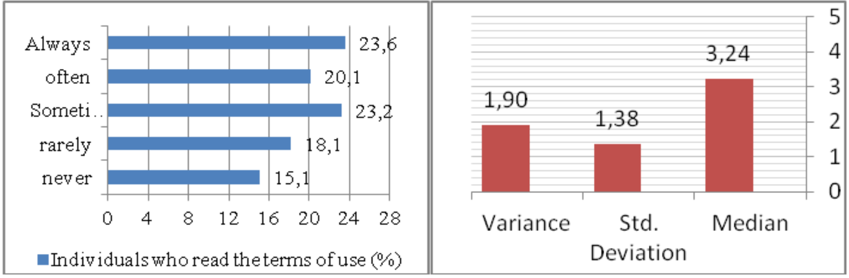
***Source**: Made by the researcher according to the outputs of SPSS software*

The table above shows that the participants do not completely trust the developers of applications (M=2.94). Even though the sample strongly believes that the aim of the developers is to facilitate the participants' lives through these applications (m=3.60), but they nonetheless do not trust them (m=2.36). And this does not match the findings of the studies of (Turow, Hoofnagle, Mull, Nathaniel, & Grossklags, 2007) and (King, Lampinen, & Smolen, 2011) which results have shown that the user exert high levels of trust in the developers even though they are not aware of how to manage their private data.

The table 04 shows is that the sample have a low tendency towards sharing their private data (M=2.52), be it with the public (M=2.18) or with the developers (M=1.67). Regardless of that, and what is worthy of notice, is that the sample has a high tendency towards declaring their correct data on the applications (M=3.42).

3.2.3 Reading Terms of Use: The analysis of this variable has uncovered the results shown in the figure below:

***Figure 02**: Attitude towards Reading Terms of Use*

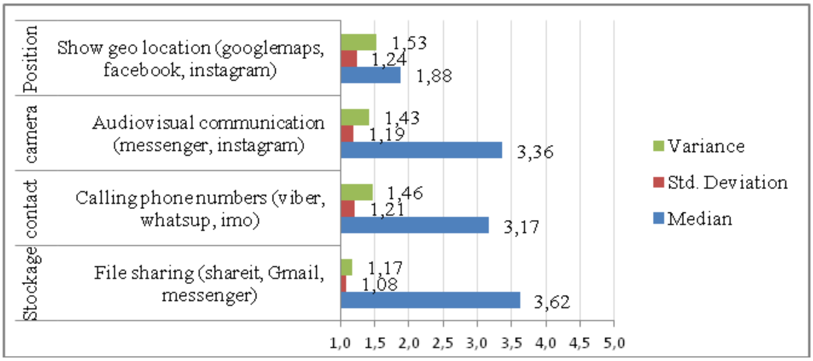


***Source**: Made by the researcher according to the outputs of SPSS software*

We notice that the sample has a mild tendency towards reading the terms of use of applications (M=3.24). 23.55% of the sample *always* read the terms of use before using the application, whereas 15.05% do not read them at all. This dovetails with the results of the referenced studies (Kesswani, Lyu, & Zhang, 2018), (Turow, Hoofnagle, Mull, Nathaniel, & Grossklags, 2007). What is worthy of remark about these results is that the Standard Deviation and the Variance points to the existence of differences between the individuals of the sample which were tested statistically (Hypotheses H_{0a}, H_{1b}).

3.2.4 Conditions Acceptance: we have analyzed the sample's tendency towards the accepting access permissions demanded by the applications that offer social connections between the users. The results were as follow:

***Figure 03**: the tendency towards the Accepting Access Permissions*



***Source**: Made by the researcher according to the outputs of SPSS software*

From the figure above, it shows that the individuals of the sample use the file-exchange feature that is built in the applications in a high frequency (M=3.62). As for the location feature, it is not of the sample's interest and they rarely share it (M=1.88). Based on the standard deviation and the variance values (*Figure 03*), we notice that there exists a differences among the participants' answers to the variable in question—which will be statistically examined later.

3.3 Testing the Study's Hypotheses: The hypotheses have been phrased based on the results of the descriptive analysis of the study and the previous studies.

H_{0a}: the sample individuals are not aware of the risks of accepting the access permissions requests, at a level of statistical significance of 0.05. This hypothesis has been examined using the Student's t-test for Paired Samples by testing the variables of Privacy Sharing and Accepting Access Permissions.

A: The results of this test have shown that there exist disparities of among the attitudes of the sample individuals towards accepting access permissions in terms of privacy sharing. Also in the respect of the dimension that is related to privacy sharing with the developers, the results of the test were also statistically significant. On the other hand, there were no disparities found on the level of the dimensions: the declaration of correct data and the privacy sharing with the public, due to the signification value which was not statistically significant. (Table 02 in the Appendices list)

B: To understand the nature of accepting access permissions and privacy sharing in terms of whether it differs when the sample reads the terms of use, we used ANOVA. The results show that there exist differences attitude towards the accepting access permissions in due to the reading terms of use, hence, the test was statistically significant. As for the declaration of correct data and sharing privacy, the result showed no disparities in due to the reading terms of use (Table 03 in the Appendices list).

The Scheffé's Test of the Relationship between Accepting Access Permissions and Reading Terms of Use show that the higher the sample's tendency towards reading the terms of use the higher their disposition towards accepting access permissions; and this is in accord with the studies of (Turow, Hoofnagle, Mull, Nathaniel, & Grossklags, 2007) and (King, Lampinen, & Smolen, 2011), which have shown that even though the user believes that their personal data is protected by certain ways, and this explains why they accept the access permissions. However, and in fact, the terms of use offer no guarantee to the user that their privacy is secure as pointed to by the study of (Tene & Polonetsky, 2012).

Based on these results, it could be said that the sample shows no signs of awareness regarding the risks of accepting access permissions requests, in particular, at the sharing privacy with the developers. Also, reading the terms of use does not make any difference regarding the sharing of privacy; however, to some extent, it increases the tendency to share privacy.

H$_{1b}$: There exist disparities for the sample's individuals attitude towards the study's variables in due to their personal variables (age, gender, level of Arabic comprehension, level of French comprehension, level of English comprehension), at a significant value of 0.05.

We have used ANOVA technique to test this hypothesis, where the results have indicated that the age is in effect relation with the sample's tendency towards the density of applications' usage, whereas the individual's language comprehension (Arabic and French) is in effect relation with the sample's tendency towards usage density, privacy sharing, and access permissions acceptance. As for the English language comprehension, it determines the usage density and accepting access permissions, but has no relation with sharing privacy. Also, it has not been verified that there is a disparity the sample's attitude towards the study's variables in terms of the gender (Table 04 in Appendices list).

The Scheffé's analysis' results of the H$_{1b}$ hypothesis show that are a disparities among the participant's tendencies in terms of their age and their level of language comprehension. What is worthy of notice also is the direct relation between the Arabic language comprehension level and the privacy sharing, between French language comprehension level and both usage density and accepting access permissions, also between English language comprehension level and both usage density and accepting access permissions. However, the relation is weak due to the difference between the highest and the lowest value of mean for the sample's tendencies towards the study's variable affected by their own personal data; and this has pointed to the existence of a weak direct relation between these variables, which has been tested in the H_{1c} hypothesis.

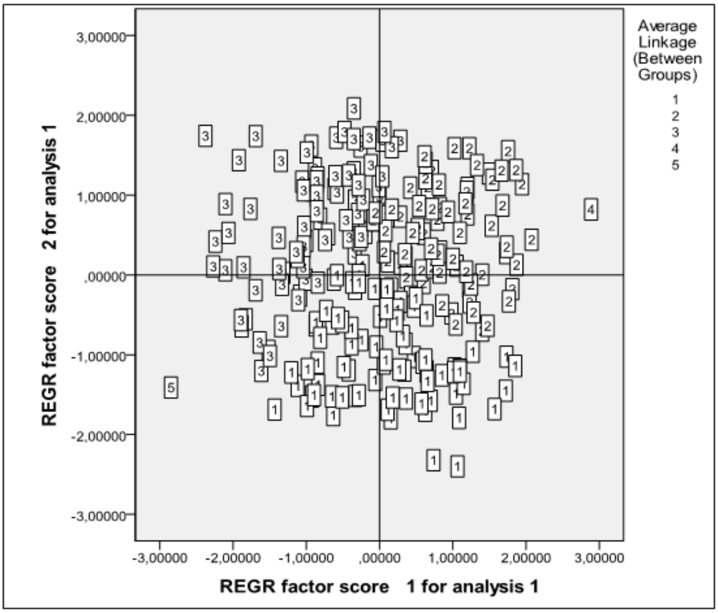
H_{1c}: There is a correlation of statistical significance between the variables of the study (usage density, trust in the developer, reading terms of use, accepting terms of use, privacy sharing, and personal data through which disparities of statistical significance have been identified). The hypothesis has been phrased in the aim of understanding the relationship between the variables under study and offering a thorough conception of the study's model. In addition, the results of Scheffé's test for the hypotheses, H_{0a} and H_{1b}, have led us to test this hypothesis, and the results of the test as shown as follows:

- There is a weak direct correlation between the principal variables of the study (Table 05 in Appendices list), where the higher value of this correlation has been recorded between the density of usage and accepting access permissions (r=0.431), and a smaller value has been recorded between the reading terms of use and density of usage (r=0.241).
- As for the personal data, we identified a weak, inverse relation between age and usage density (r=-0.174), and between age and trust (r=-0.176). Moreover, there is a correlation between Arabic language comprehension and the usage density, privacy sharing, and accepting access permissions. We also have identified a correlation between the latter variables and French language comprehension. As for English language comprehension, we just identified a correlation with the usage density and accepting access permissions (Table 05 in Appendices list).

3.4 Multidimensional Scaling of the Study's Variables: The factor analysis for the principal components (Varimax technique) arrived at two dimensions; the first dimension includes four variables: privacy sharing, accepting permissions, usage density, and trust. And the second dimension includes one variable: reading terms of use (The table 06 in the Appendices list,).

We have classified the sample's tendencies towards the two dimensions extracted from the factor analysis of the principal components, where we measured the tendencies using Euclidean Squared Distance; as for accumulating the tendencies, we used Classes Average Distance. The results were as listed in Table 07 in Appendices list, which were graphed in the figure below:

***Figure 04**: Projection of Classes over the Extracted Dimensions from PCA*



***Source**: Made by the researcher according to the outputs of SPSS software*

The classification has yielded five principal groups, we elucidate them as follows:

- First group: forms 38.6% of the study's sample. The individuals of this group *sometimes* use applications, trust them, accept the requested access permissions, and share their privacy. However, they rarely read the terms of use and conditions despite their excellent level of Arabic and French comprehension. According to this, this group shall be labeled as: the interested risk-takers.
- Second group: occupies 29.7% of the study's sample. The individual of this group *often* use applications, read terms of use, trust them, and accept access permissions; however, they *sometimes* have a tendency towards sharing their privacy. This group can be labeled as: the enthusiastic.
- Third group: represents 30.9% of the sample, where the individuals sometimes use the applications and trust them, but they often read the terms of use, and rarely accept access permissions; moreover, they tend to never consent to sharing their privacy. We label this group as: the cautious.

- Fourth and fifth group: these are marginal groups each of which represents 0.4% of the study's sample. In consequences, it can't be relied on for the analysis of the study; instead we settle for the previous, three groups only.

4. Result Discussion

4.1 Discussion of the First Phase of the Study: What the results have shown is that the Algerian society uses Android applications daily and in a high frequency, though the logging in and out of these applications is short in duration. The majority of the kinds of applications the society uses are social media and entertainment applications, where the individuals appear to declare their correct data amidst using them. It follows that the density of data can be conceptualized (frequency and duration of flow) which can be investigated by the applications' developers.

4.2 Discussion of the Second Phase of the Study: This phase shows that there is a clear variance regarding the reading the terms of use and accepting access permissions. In that the latter has a lot to do with the services of file sharing, video/audio calls, and calls using phone numbers. Despite that the sample individuals has no desire to share their privacy, with the developers especially, we have found that there is group worthy of mention whose percentage of the Algerian society tallies up to 38.6% who rarely read the terms of use and conditions of using the applications which is something that notifies them about that the developers are capable of intruding on their privacy.

4.3 Discussion of the Third Phase of the Study: In this phase, it is found there this a portion of the Algerian society who consents to access permissions even though they have no intent to share their privacy with the developers; even in the case where they read the terms of use, this only increase their tendency to accept access permissions. This can be interpreted as that there is a group in the Algerian society who is not aware that the moment they accept access permissions, their privacy becomes automatically accessible to the developers, or aside from the unawareness about this, it could be enthusiasm and recklessness on the group's part, and this is what phase four of the study have shown.

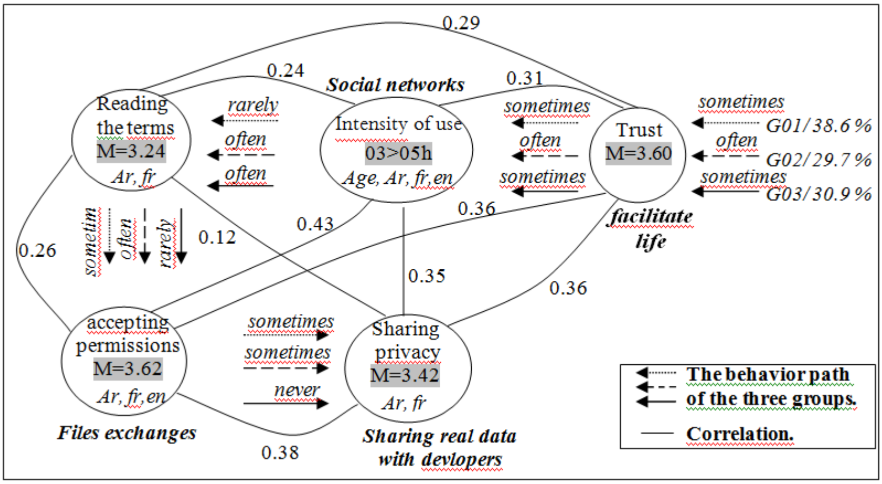
As for the privacy sharing with the public and declaring of correct data, it is known by the users of the general applications that they can control these variables post accepting access permissions by not showing the data to the public and reserve it to themselves. This explains why these variables have not caused any statistical disparities in the sample's tendency towards accepting access permissions.

4.4 Discussion of the Fourth Phase of the Study: Through this phase, it has been ascertained that there are differences among the Algerian society concerning the density of application usage in terms of age, where there exists between the two an inverse relation; and the same goes for the age and trust in the applications. This is due to the fact that the youth are the ones who extensively use applications. In additions, Arabic and French languages determines the tendencies towards the density of usage, accepting access permissions, and privacy sharing; and this has been examined and confirmed by the correlation relation, which was found to be direct. This is due to the Arabic language being the mother-tongue of the Algerian society, and the French language being the first foreign language; and this has enabled the society under study to have more control over the applications due to the understanding of the features and services offered by the applications.

Furthermore, studying the correlation between the variables and scaling them multi-dimensionally have yielded three groups of the Algerian society that share the characteristics of: holding onto privacy, the high level of Arabic and French comprehension, and the intermediate level of English comprehension (except for the second group whose comprehension was also intermediate for Arabic and English languages). The first group is represented by risk-takers who are careless about the consequences of trusting the applications and accepting their access permissions (they rarely read terms of use). As for the second group, it is represented by enthusiasts who even though read the terms of use, they nonetheless accept access permissions and trust them. The third group is the cautious ones who read the terms of use and rarely accept the access permissions due to the lack of trust in the applications.

Integrating the aforementioned results and the results from previous studies has led to the graphing of the figure below to give a thorough conception of the study at hand:

***Figure 05**: Comprehensive Conception of the new Study's Model*



***Source**: Made by the researcher according to the results of the study*

The comprehensive conception of the new study's model is that the applications are used with the aim to facilitate the lives of the individuals (the users); this usage lasts from 3 hours to 5 hours of social networking mostly for files exchange, where real data is declared and shared with the developers through means of accepting access permissions. The level of awareness about the risks and the level of caution concerning the usage of applications vary from one individual to another; however, most of them are careless risk-takers and enthusiasts.

5. Conclusion

It is evident that the developers of applications exploit personal data for marketing; personal data can also be used for other unknown goals. However, this study has shown that the majority of the users are risk-takers or enthusiasts who are careless about the dangers of using applications. What is alarming about these facts is that accessing data is not exclusive to the user, but also inclusive of their network, which allows those who are in possession of the data to control the lives of everyone through creating and changing their lifestyle.

For these reasons, we advise the users of Android applications specifically to be aware of the nature of the application, in that, to know whether the app is a first or a second or a third-party app, by investigating the source of it; this in consequence helps to know whether the app is a malware or not. We also advise the users to read the terms of use before accepting the access permissions in the purpose of knowing how their data is managed by the developers.

The results of this study needs to be delved into deeper through other studies, where a light can be shed on the studied variables, further measured by Regression Analysis in the purpose of isolating the independent and dependent variables.

At the end of this study, we have reached multiple questions: is the user's lack of trust in the developer what leads them to rejecting access permissions, and in consequence, not use the app? Or is it the reading of terms of use that leads to that? Is the lack of trust leads to read the terms of use? Does the direct relation between reading the terms of use and accepting access permissions is a consequence to the high confidence the user has in the application?

6. REFERENCES:

- Felt, A., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. *Proceedings of the 18th ACM Conference on Computer and Communications Security.*, October 17–21, Chicago, USA.
- Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS)*, July 11-13, Washington, USA.
- Gamao, A. O. (2018). Malware Analysis on Android Apps: A Permission-based Approach. *Social Science and Humanities Journal, 02* (11).
- Gruschka, N., Iacono, L. L., & Tolsdorf, J. (2018). Classification of Android App Permissions. *17th European Conference on Cyber Warfare and Security*, June, Oslo, Norway.
- Kesswani, N., Lyu, H., & Zhang, Z. J. (2018). Analyzing Android App Privacy with GP-PP Mode. *IEEE journal, 06 (01),* Open access (online).
- King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is There An App for That? *SOUPS 2011 Symposium On Usable Privacy and Security*, July 20-22, United States.
- Krishnan, N. C., & Cook, D. J. (2012). Activity Recognition on Streaming Sensor Data. *Pervasive and Mobile Computing, 10*(01).
- Peng, M., Zeng, G., Sun, Z., Huang, J., Wang, H., & Tian, G. (2018). Personalized app recommendation based on app permissions. *World Wide Web, 21*(08).

- Qatrunnada, I., Tousif, A., Kelly, C., Apu, K., & Reite, M. (2017). To Permit or Not to Permit, That is the Usability Question: Crowdsourcing Mobile Apps' Privacy Permission Settings. *Proceedings on Privacy Enhancing Technologies* (04).
- Sakamoto, S., Okuda, K., Nakatsuka, R., & Yamauchi, T. (2014). DroidTrack: tracking and visualizing information diffusion for preventing information leakage on Android. *Journal of Internet Services and Information Security, 04*(02).
- Tene, O., & Polonetsky, J. (2012). *Privacy in the Age of Big Data: A Time for Big Decisions. STANFORD LAW REVIEW ONLINE, 64*(63)
- Turow, J., Hoofnagle, C. J., Mull, D. K., Nathaniel, G., & Grossklags, J. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade. *A Journal of Law and Policy for the Information Society, 03*(03).
- Wang, H., Cao, J., & Zhang, Y. (2005). A flexible payment scheme and its role-based access control. *IEEE Trans Knowl, 17*(03).
- Z. Y., S. Y., W. H., & Y. J. (2016). On secure wireless communications for iot under eavesdropper collusion. *IEEE Trans, 13*(03).

7. Appendices:

Notice: all the tables below sourced by the outputs of SPSS

***Table 01**: The Descriptive Analysis of Usage Density.*

Frequency	**Never**	**Rarely**	**Sometimes**	**Often**	**Always**	**Total**
Percent	**0,8**	**2,7**	**24,7**	**24,7**	**47,1**	**100**

***Table02**:Student t-test for Independent Paired Samples on privacy sharing in terms of accepting access permissions.*

		Différences appariées					T	Sig.
		Moyenne	Ecart-type	Erreur standard moyenne	Intervalle de confiance 95% de la différence			
					Inf	Sup		
Paire 1	Provide the correct data.	0,104	1,717	0,107	-0,106	0,314	0,977	0,329
Paire 2	Share data with the public	-0,058	1,654	0,103	-0,260	0,145	-0,563	0,574
Paire 3	S D with developers	-0,255	1,569	0,097	-0,447	-0,063	-2,614	0,009
Paire 4	S D with developers and the public	-0,946	1,377	0,086	-1,114	-0,777	-11,055	0,000
Paire 5	Privacy sharing	0,402	1,341	0,083	0,237	0,566	4,818	0,000

***Table 03**: One way Anova test about the extent of differences towards the privacy sharing (disassembled and aggregated) and the accepting access permissions in terms of reading the conditions.*

ANOVA						
		Somme des carrés	ddl	Moyenne des carrés	F	Sig
Accepting access permissions.	Inter-groupes	19,468	4	4,867	6,221	0,000
	Intra-groupes	198,717	254	0,782		
	Total	218,185	258			
Provide the correct data.	Inter-groupes	9,666	4	2,416	1,182	0,319
	Intra-groupes	519,361	254	2,045		
	Total	529,027	258			
Share data with the public	Inter-groupes	8,184	4	2,046	0,985	0,416
	Intra-groupes	527,546	254	2,077		
	Total	535,730	258			
Share data with developers	Inter-groupes	5,761	4	1,440	1,172	0,324
	Intra-groupes	312,223	254	1,229		
	Total	317,985	258			
Share data with developers and the public	Inter-groupes	4,849	4	1,212	0,717	0,581
	Intra-groupes	429,660	254	1,692		
	Total	434,510	258			
Privacy sharing	Inter-groupes	1,608	4	0,402	0,304	0,875
	Intra-groupes	335,419	254	1,321		
	Total	337,027	258			

***Table 04**: One way Anova and Student test about the extent of differences in the study variables due to their personal data variables (age, gender, level of understanding of Arabic, French, and English).*

A:Usage density, B: Reading terms of use, C: Trust, D: Sharing privacy, E: Accepting access permissions.		Test ANOVA								Test (t)		
		age		ar		fr		en				
		Moyenne des carrés	Sig	Moyenne des carrés	Sig	Moyenne des carrés	Sig	Moyenne des carrés	Sig	gender	Moyenne	Sig
A	Inter-groupes	0,977	0,046	3,211	0,000	1,478	0,005	1,305	0,011	M	3,049	0,96
	Intra-groupes	0,397		0,362		0,390		0,392		F	3,054	
B	Inter-g	0,921	0,750	4,050	0,073	2,065	0,362	4,256	0,061	M	2,914	0,878
	Intra-g	1,914		1,864		1,896		1,861		F	3,579	
C	Inter-g	1,222	0,211	1,304	0,181	2,058	0,042	0,968	0,328	M	2,802	0,64
	Intra-g	0,829		0,828		0,816		0,833		F	3,210	
D	Inter-g	1,466	0,055	2,178	0,007	2,021	0,011	0,815	0,225	M	2,594	0,559
	Intra-g	0,610		0,598		0,601		0,620		F	2,398	
E	Inter-g	1,681	0,054	3,191	0,001	2,695	0,004	2,977	0,002	M	3,034	0,937
	Intra-g	0,712		0,688		0,696		0,691		F	3,145	

***Table 05**: Pearson's correlation between study variables*

A:Usage density, B: Reading terms of use, C: Trust, D: Sharing privacy, E: Accepting access permissions.		usage density	Reading terms of use	Trust	sharing privacy	Accepting access permissions	AR comprehensio n	FR comprehensio n	ENG comprehensio n	Age
A	R	1	,241	,313	,350	,431	,258	,235	,218	-,174
	Sig.		,000	,000	,000	,000	,000	,000	,000	,005
B	R	,241	1	,294	,123	,265	,070	,111	,126	-,041
	Sig.	,000		,000	,048	,000	,066	,075	,042	,507
C	R	,313	,294	1	,360	,366	,084	,077	,053	-,176
	Sig.	,000	,000		,000	,000	,177	,218	,395	,004
D	R	,350	,123	,360	1	,380	,224	,148	,119	,098
	Sig.	,000	,048	,000		,000	,000	,017	,056	,117
E	R	,431	,265	,366	,380	1	,234	,213	,220	,026
	Sig.	,000	,000	,000	,000		,000	,001	,000	,679
AR comprehension	R	,258	,070	,084	,224	,234	1	,265	,315	,049
	Sig.	,000	,066	,177	,000	,000		,000	,000	,433
FR comprehension	R	,235	,111	,077	,148	,213	,265	1	,397	,038
	Sig.	,000	,075	,218	,017	,001	,000		,000	,548
ENG comprehension	R	,218	,126	,053	,119	,220	,315	,397	1	,007
	Sig.	,000	,042	,395	,056	,000	,000	,000		,911

***Table 06**: the quality of the representation of the variables and variance of the new basic components (dimensions).*

The quality of the representation of the variables			**Variance of the new basic components (dimensions).**					**Representation of variables for the basic components**	
				Valeurs propres initiales		Somme des carrés des facteurs retenus pour la rotation		Composante after the rotation	
	Initial	Extraction	Composante	Total	% de la variance	Total	% de la variance	1	2
Usage density	1,000	,518	1	2,270	45,408	1,993	39,867	,689	,208
Reading terms of use	1,000	,902	2	,891	17,825	1,168	23,365	,106	,944
Trust	1,000	,498	3	,703	14,057			,586	,393
Accepting access permissions	1,000	,571	4	,575	11,490			,712	,254
sharing privacy	1,000	,672	5	,561	11,220			,810	-,125

***Table 07**: Attitudes of respondents towards the study variables according to each group resulting from the hierarchical classification*

Groups	**Usage density**	**Reading terms of use**	**Trust**	**Accepting access permissions**	**Sharing privacy**	**Age**	**language comprehension**		
							AR	FR	ENG
G1	3,0350	1,8767	2,750	2,979	2,648	29,5294	4,65	3,52	3,17
G2	3,500	4,1455	3,500	3,750	3,111	27,4167	4,73	3,70	3,39
G3	2,625	4,0741	2,7805	2,583	1,796	27,6364	4,59	3,26	3,06
G4	4,500	5,000	4,500	4,792	4,556	35,0000	5,00	4,00	4,00
G5	1,000	1,000	1,000	1,583	1,000	38,0000	4,00	4,00	3,00
Global	3,105	3,240	2,940	3,083	2,519	28,5556	4,66	3,51	3,21