Exploring Social Media Privacy Preferences in Saudi Arabia

Aziz Alshehri , Salah Alamri

Computer Science Department, College of Computing in Al-Qunfudhah Umm Al-Qura University, Saudi Arabia

Summary
With the increase in the use of social networking apps in smartphones, users are increasingly concerned about the access of these apps to private and sensitive data which are highly valuable for users. Most of the prior studies assume the homogeneity of privacy preferences across users, yet these concerns differ from person to person based on many factors such as culture, age, and gender. Therefore, it is paramount to explore users' concerns for social media apps to design a system that meets and adopt users' needs and requirements. Accordingly, a questionnaire was designed that explores the most important preferences of users regarding social networking apps. Hence, the result of this study showed that users' concerns are not on one level but rather diverse and different. Moreover, age, gender and occupation play an essential role in different users' preferences. On the other hand, some demographic factors such as education and experience level do not represent a strong relationship with the level of privacy concerns.

Keywords: *Social Media Privacy Concerns, Mobile Permissions, Demographic Factors.*

1. Introduction

The huge amount of private and personal information that is saved has expanded in tandem with the rapid growth of devices, activities, services, and information. Consequently, users become more worried about their personal information, particularly its use, who has access to it, and where it is stored (Anton et al., 2010). For instance, as shown in a Consumer Report, 92 % of British and U.S. Users are concerned about their internet privacy (TRUST, 2016). When users were made aware of internet user privacy, they were asked what made them most concerned about their online privacy and what drove them to take action where personal information is shared between companies, as according 45 percent of British Internet users (Federal Trade Commission, 2013). Moreover, 89 % avoided these businesses because they believed they won't protect their personal information. Due to these worries, 76 percent of Internet users curtailed their online activity in the previous 12 months [4]. Users are adequately worried about their online privacy, according to this evidence.

Most mobile operating systems, such as Android and iOS, provide certain privacy measures for users due to user concerns about privacy protection (Kelley et al., 2012). Despite these provisions, the functionality and interface have several usability difficulties. Kelley et al., for example, discovered that users in Android struggle to grasp permissions due to a lack of usability (Kelley et al., 2012). As a result, the Federal Trade Commission believes that privacy controls must be improved to further ensure that users' privacy is protected (Federal Trade Commission, 2013).

The development of rules, procedures, and tools that assist an end-user in controlling and comprehending their privacy-related information has received special attention. These approaches, on the other hand, assume that users can accurately configure all of the generated settings and that they all have the same privacy requirements. Users, in actuality, have a variety of privacy concerns and requirements due to their diverse privacy attitudes and expectations (Agarwal & Hall, 2012). Some users, for example, regard personal information in their social media profile, such as age, address, and gender, to be more sensitive than others (Song & Hengartner, 2015). Furthermore, assuming uniform privacy standards throughout a population is impracticable in practice (Song, 2015). As a result, it is important to explore users' concerns about data sharing with applications before designing a privacy protection system. Some prior research assumes that users have one level of concern, while users' concern differ from person to person. Accordingly, a questionnaire is designed to know and understand users' concerns and what demographic factors influence users' choices. There really are five sections to this paper. The background literature is examined at Section 2. Section 3 describes how the data were gathered. Data analysis and findings are discussed in the section 4. Section 5 includes the conclusions and suggestions for future work.

2. Background Literature

This section provides an overview of current privacy solutions. In recent years, many researches have been published on privacy in many areas such as mobile applications, web application, and social networks to protect users' privacy because privacy exists wherever personal information or sensitive information is disclosed.

Manuscript received January 5, 2022
Manuscript revised January 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.1.95

However, this section merely focuses on a mobile platform due to related to the proposed system.

Taintdroid was created to identify sensitive data leaving the system through untrustworthy applications (Enck et al., 2014). It was created using a dynamic approach that is implemented while a program is running. The system can monitor data flow at four different levels: variable, method, message, and file. Despite the fact that TaintDroid detects sensitive data, it presume that users can correctly configure all of the settings that arise. As a result, this strategy may place an unnecessary burden on users. Furthermore, they do not look at the usability of the interface that is presented to users.

Balebako et al. (Balebako et al., 2013) suggested an alternative that focuses on the user's understanding of privacy concerns. The solution increases the user's awareness of possible privacy breaches. It is based on the TaintDroid platform and aids users in determining the frequency and destination of data provided by an app. It also has a variety of user interfaces that can help consumers understand which privacy-sensitive data leaves the phone. They do not, however, provide consumers control over their personal information, allowing them to designate which types of data they do not want to leave the phone.

PiOS is another tool that analyzes programs for probable sensitive data leaks from a mobile device to a third party. It discovered data breaches involving device ID, location, and phone number. PiOS also took into account the address book, internet history, and photographs. PiOS detects data flows via static analysis. They examined over 1,400 iPhone apps and discovered that the majority of them leak the device ID, which can provide extensive information about a user's behaviors. PSiOS, on the other hand, does not give users fine-grained control over their personal data.

In order to protect sensitive data, AppFence employs a replacing information method (Hornyack et al., 2011). Shadowing and blocking are two privacy measures provided by AppFence to safeguard sensitive resources. Users may be hesitant to provide applications access to sensitive data. As a result, instead of sending actual data, AppFence delivers shadow data. AppFence may give application shadow data that contains no contact entries, only those actual records not considered sensitive by the user, or wholly fake shadow entries when an application wants access to the user's contacts. The second method for safeguarding sensitive data is to prevent it from being exfiltrated from the device. TaintDroid information flow tracking is used by AppFence to track sensitive data and prevent it from being transmitted out of the device.

The Taming Information Stealing Smartphone Applications (TISSA) comprises of three key components that give users fine-grained control over the sharing of their personal information (Zhou et al., 2011). TISSA was created to safeguard four categories of personal data: phone identification, location, contacts, and call history. The first is the content provider with privacy settings. On the mobile device, it includes the current privacy settings for untrusted apps. It also gives users an interface through which they can check the current privacy settings for an untrusted app (e.g., a location manager). TISSA presents users with empty or fraudulent options for personal information that may be requested by the app in order to protect personal information. The privacy-setting manager is the second component. It enables users to modify or update the privacy settings for installed apps. The third component includes content providers or services that control access to four different forms of personal data: phone identification, location, contacts, and call log. When an app seeks access to sensitive data, for example, the system will check the privacy settings and respond to the requests based on the app's existing privacy settings. However, because the average user is unaware of the reasons for permission requirements for individual apps, it is impossible for him to assess which sort of permission poses a high or low risk to the app. Furthermore, in order to alleviate the stress on mobile users, the system does not aid the user in making the best decision.

PrivacyGuard (Song, 2015) and AntMonitor (Le et al., 2015) enable fine-grained privacy control and packet-to-application ground truth mapping. They deployed a technique that analyzes actual Android network traffic and intercepts it using the VPNService API. This method does not require root access and is compatible with all Android devices running version 4.0 or later. AntMonitor is made up of three parts: an Android app called AnyClient and two server apps called AntServer and LogServ. PrivacyGuard, on the other hand, runs entirely on the local device. The client-side analysis' goal is to protect consumers in real time while also allowing for fine-grained privacy control. In comparison to AntServer, LogServer serves as a central repository for storing and analyzing all network traffic data, and it does not have to analyze a vast volume of live traffic. They enlisted student volunteers to test the AntMonitor system by having them use AntClient on their phones. The system gathers packets from the applications chosen by the volunteers and keeps them at LogServer in order to see if any of the installed programs are sending personal data to the Internet. They discovered that 44 percent of users had programs that leak their International Mobile Equipment Identity (IMEI) and 66 percent of users have applications that leak their Android Device ID, respectively. Both PrivacyGuard and AntMonitor, on the other hand, presume that normal users

can accurately describe their personal information so that the system can detect them when they leave their phones. In this instance, these solutions do not assist consumers in alleviating the load of handling such a big amount of data.

ProtectMyPrivacy (PMP) gives consumers fine-grained privacy controls for each app, allowing them to share anonymised data rather than sensitive information (Agarwal & Hall, 2012). It identifies privacy breaches in iOS apps. A unique device identification, IMEI, Wi-Fi MAC address, and Bluetooth MAC address are the types of data that PMP safeguards. The user's address book is another type of confidential data that PMP safeguards. Because some apps upload this information to a server without the user's permission, it contains names, addresses, phone numbers, and emails. When an app requests access to sensitive data, PMP gives the user the option to decline or grant the request in real time. As a result, PMP gives the user two alternatives for protecting his address book: allowing the program to access his address book or allowing PMP to submit an alternate address book with bogus entries (names, emails and phone numbers). They've also created a crowdsourcing mechanism that delivers app-specific privacy tips to assist users in making educated selections. However, the approach only addresses access to private data within the app and does not address privacy once the data has left the app. Furthermore, the system does not offer individualized recommendations to each user. Every user has their own set of privacy preferences. As a result, when the system creates recommendations, it would be beneficial to take into consideration the user's profile in order to provide a more personalized recommendation.

4. Resesrch Methodology

The questionnaire consists of three sections. The first section of the questionnaire includes classification questions to determine some demographic information, such as gender, age, education level and level of IT skills. The second section investigated how concerned users are about such privacy-related information in social media app generally. Whilst third questions explored users' concerns about such privacy-related information for seven common social media in Saudi Arabia specifically: WhatsApp, Facebook Instagram, Twitter, YouTube, TikTok and Snapchat. In order to verify that the survey instruments were understandable and reliable, a pilot study was conducted for ten participants. The feedback from the pilot study was used to refine and enhance the survey. All the provided questions were open-ended questions which need to be answered in accordance with the perceptions of the participants.

Participants were recruited through different categories such as Email, social network, and some communities' centre. Prior to displaying the survey questions, its aims and structure were briefed confirming that the respondents should be 18 years or older and they are free to withdraw up until the final submission of their responses. In total, 381 completed responses and the total responses are within the range of other surveys in the research domain and close to the expected and targeted figure.

Demographic information was collected including questions related to gender, age, education, and the level of knowledge in order to analyze the data, though the age ratio or any other demographic composition of the participants were not specifically controlled. Among these participants, 56% of them were male; 44% of them were female. Regarding the age, almost half of the participants were between 18 and 24 which represent 48% of participants as shown in Table1. The age between 25-34 represents 24% and same percentage for age group was between 35-44 which is most interesting result. The percentage of youth age in this survey percentage the largest group which is aligned with parentage distribution of Saudi of population. According to Saudi Statical website 67% of Saudi population represents youth people (Saudi Statical, 2020). Being within an academic institution, nearly 77 percent of the participants have a bachelor or postgraduate degree, more specifically, nearly half of the participants have bachelor's degree as shown in Table1.

Factor	Category	Count	Percentage	Factor	Category	Count	Percentage
Gender	Male	213	56%	Level of IT	Novice	88	21.60%
	Female	168	44%		Intermediate	273	67.10%
Age	18-24	182	48%		Advanced	10	2.50%
	25-34	93	24%				
	35-44	90	23%				
	45-54	12	4%	Education	High school and lower	76	20%
	55-64	3	0.7%		College certificate	10	2.6%
	65+	1	0.30%		Bachelor	215	56.4%
					Postgraduate	80	21%

Table1: Summary of Respondents' Demographic Characteristics

Wisniewski et al. (2017) state that users differ significantly in how they learn and use different privacy mechanisms according to their knowledge. This draws attention to the paramount importance of considering users' level of knowledge. Therefore, this survey includes level of knowledge which represents almost half of population is between intermediate and advance.

In general, when participants were asked a general question about how they are concerned about their privacy in social media, participants' answers indicate that highly concerned (μ =1.7). Another general question is regarding how participants are concerned when social media apps

share their data with advertisements. Participants are also highly concerned about this question (μ =1.5). This outcome indicates that participants are generally highly concerned about sharing their information in social media.

4. DATA ANALYSIS

In order to analyze the users' preferences, the responses were transformed into a value number from one (Not at all concerned) to five (extremely concerned). To visualize the results, heat maps were utilized in 2D to display users' average preferences for all 381 participants in a data matrix, as shown in Figure 1. Red cells indicate a higher level of concern, while green cells indicate a lower level of concern. The empty cells indicate the absence of data for a particular data type.

Data Type	Users' Average Preferences for all Participants						
Camera	2.3	3.8	3.1	3.9	2.5	4.4	4.2
Multimedia	2.9	3.6	3.1	4.0	2.4	4.3	4.3
Contact	4.0	4.5	4.5	4.6	2.3	4.5	4.5
Location	3.7	4.5	4.5	4.7	3.4	4.6	4.5
Microphone	2.3	3.9	3.5	4.1	2.3	4.3	4.1
SMS					2.7		
Phone	3.9	4.4	4.5		2.9	4.6	4.6
Calendar				4.2		4.5	4.3
App Categories	Snapchat	Twitter	Instagram	TikTok	WhatsApp	Facebook	YouTube

Figure2: Average Preferences for Participants

The highest levels of concern were Facebook and YouTube which shared same average (μ = 4.4). In the Facebook app, the location and phone information presented the highest level of concern for the participants (μ = 4.6). On the other hand, the phone (μ = 4.6), contact and location (μ = 4.5) information presented the highest level of concern in the YouTube app. Generally, location information represents the highest levels of concern across social media app. This indicates that users sill are concerned about location information even though the mobile operating system improved privacy permissions.

The lowest levels of concern were WhatsApp (μ =2.6). where green cells represent most of WhatsApp cells. The second-lowest levels of concern were the Snapchat app (μ = 3.2). Snapchat and WhatsApp were the lowest concerns because participants may generally be less concerned when an app category access personal information related to the app's core functionality. Therefore, it is important during the design of the solution to distinguish between app permission related to the core functionality and others.

The overall picture of participants' average preferences is an useful place to start learning about current users' privacy concerns. However, the average results for each app across all participants show little diversity in user privacy preferences, despite the fact that users' privacy preferences are different, according to the literature study. As a result, as shown in Figure 2, a substantial effort was required to determine the differences in user preferences in each app.

In Figure 2, the darker shades of red imply greater variation in participants' worry ratings for different apps. The variance result reveals that participants' preferences have are definitely diverse. In most cases, variations are greater than 0.8 (of a rating on a [1 to 5] scale) and less than three. Despite the fact that Figure 1 demonstrates that respondents are unconcerned regarding their data being shared by the WhatsApp app, the variance result signifies that respondents' preferences for the WhatsApp app are in fact varied, and that the WhatsApp app reflects the highest variation among the people. By looking at data type across all apps, the multimedia information and camera appears the highest diversity among the participants. This variance in the multimedia information and camera indicates that information could not adequately be captured by a one-size-fits-all default approach. Moreover, there are different attitudes and different preferences towards this data because the level of privacy required differs from user to user.

Data Type	Variances in User Preferences						
Camera	2.0	2.3	2.6	2.1	2.1	1.3	1.7
Multimedia	2.1	2.1	2.6	2.0	2.0	1.4	1.6
Contact	1.8	1.1	1.1	0.8	2.2	1.0	1.1
Location	1.9	1.0	1.1	0.7	2.4	0.9	1.1
Microphone	1.8	1.9	2.4	1.9	2.1	1.5	1.9
SMS					2.5		
Phone	1.9	1.2	1.3		2.6	0.9	0.9
Calendar				1.7		1.2	1.5
App Categories	Snapchat	Twitter	Instagram	TikTok	WhatsApp	Facebook	YouTube

Figure 2: Variance in User Preferences

	Gender	*Age*	*Degree*	*Occupation*	*IT*	*Snapchat*	*Twitter*	*Instagram*	*TikTok*	*WhatsApp*	*Facebook*	*Youtube*
Gender		-0.276***	-0.244***	-0.029	-0.064	0.166**	0.173***	0.134**	0.082	0.011	0.211***	0.245***
Age	-0.276***		0.345***	0.610***	0.027	0.213***	0.121*	0.244***	0.154**	0.262***	-0.010	0.020
Degree	-0.244***	0.345***		0.173***	0.105*	0.083	0.084	0.151**	0.064	0.080	-0.041	0.056
Occupation	-0.029	0.610***	0.173***		0.075	0.129*	0.060	0.180***	0.104*	0.191***	0.032	0.013
IT	-0.064	0.027	0.105*	0.075		-0.134**	-0.057	-0.030	-0.098	-0.016	-0.049	-0.063

Figure 1: correlation between users' demography and social media apps where p < .0001 '****'; p < .001 '***', p < .01 '**', p < .05 '*'

except for the Instagram app. This result indicates that there is a relationship between the level of education and the participants' concerns regarding the Instagram app. As for the level of experience factor for technology, there was also no correlation between the level of experience and user preferences in most social media apps. On the other hand, the results showed that there is a difference between users' choices and type of job in some apps such as Instagram, WhatsApp, Tiktok and Snapchat.

Moreover, Spearman‘s test was performed to check for any correlation between users’ age and Snapchat app. the results indicate significant differences between users’ age in the context of camera, multimdea and location as shown in Table2. The strength of these correlations were moderate.

Another method employed in this study to examine the relationship between participants' demographic features and their preferences was statistical analysis. The R software was selected because it is one of the most commonly utilized statistical tools by researchers to do complex statistical analyses. Hence, A Spearman‘s test was performed to check for any correlation between users’ demography and social media apps. Figure 3 indicates significant differences between males and females for social media apps except TikTok and Snapchat. The results show that females are more concerned about social media' data than males.

In regard to age, A Spearman‘s test reveals a significant correlation between participants’ age and social media apps except for Facebook and YouTube which means as people get older, there are more fears of sharing data with social media. Figure 3 also shows that the factor of education level did not have a significant impact on the participants' choices

This result indicates that when the users’ age increases, level of concern increases as well in some type of data in Snapchat.

Factor	Correlation coefficient (r)	P-value	Strength of the relationship
Camera	0.4	0.001	Moderate
Multimedia	0.3	0.001	Moderate
Phone	-0.021	0.684	No correlation
Contact	-0.002	.965	No correlation
Location	0. 40	.001	Moderate

Table 3: correlation between users’ gender and Snapchat app.

5. Conclusion and Future Work

This paper explored users' concerns for social media apps accessing users' private data in Saudi Arabia and the influence of demographic factors on these concerns. The outcomes revealed that users have different privacy concerns because they have heterogeneous privacy attitudes and expectations. Assuming that users have uniform privacy requirements would be ineffective, and it could significantly increase the burden on, and frustration of, the user.

The influence of demographic factors on users’ information privacy concerns was examined. Gender, age, and occupation have a significant correlation with user concerns for most social media apps. Older users were shown to be more concerned about information privacy than younger which in turn indicates that older users are more sensitive to privacy issues. Moreover, the outcomes revealed that females and males differ toward information privacy concerns. Females are often more concerned about most of the information on social media than males. Whilst there was no correlation between the levels of education about the privacy of social media apps and level of concerns except for the Instagram app.

There have been few studies that have looked into users' concerns about data privacy in social media. This research contributed valuable information about the role of demographic factors and their relationship to the level of concerns for accessing privacy data in social networks. The findings have important implications for developing default permission settings. Hence, privacy preferences are diverse and cannot adequately be captured by one-size-fits-all default settings. Further research requires to develop a technique on how to user profiling could be utilised to cluster users into a smaller number of privacy profiles. Clustering users into a small number of groups could help to design initial interfaces which in turn, reduce individual users’ burden and frustration.

References

[1] Agarwal, Y., & Hall, M. (2012). Protect My Privacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing Categories and Subject Descriptors. Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services, 6(September), 97–110.

[2] Anton, A. I., Earp, J. B., & Young, J. D. (2010). How Internet Users ’ Privacy Concerns Have Evolved. IEEE Privacy & Security, 1936(February), 21–27. https://doi.org/10.1109/MSP.2010.38

[3] Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013). “Little Brothers Watching You”: Raising Awareness of Data Leaks on Smartphones. SOUPS ’13: Proceedings of the Ninth Symposium on Usable Privacy and Security, 12:1--12:11. https://doi.org/10.1145/2501604.2501616

[4] Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS Detecting privacy leaks in iOS applications. Proceedings of the 18th Annual Network & Distributed System Security Symposium, NDSS 2011, 11.

[5] Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., Sheth, A. N., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2014). TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. ACM Transactions on Computer Systems (TOCS), 32(2), 5. https://doi.org/10.1145/2494522

[6] Federal Trade Commission. (2013). Mobile privacy disclosures - Building trust through transparency. February, 29.
[7] Frank, M., Dong, B., Felt, A. P., & Song, D. (2012). Mining permission request patterns from Android and Facebook applications. Proceedings - IEEE International Conference on Data Mining, ICDM, 870–875. https://doi.org/10.1109/ICDM.2012.86
[8] Hornyack, P., Han, S., Jung, J., Schechter, S., & Wetherall, D. (2011). These Aren't the Droids You're Looking for: Retrofitting Android to Protect Data from Imperious Applications. In Proceedings of the 18th ACM Conference on Computer and Communications Security, 639–652. https://doi.org/10.1145/2046707.2046780
[9] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: Installing applications on an android smartphone. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7398 LNCS, 68–79. https://doi.org/10.1007/978-3-642-34638-5_6
[10] Le, A., Irvine, U. C., Langhoff, S., & Shuba, A. (2015). AntMonitor : A System for Monitoring from Mobile Devices. 1, 15–20.
[11] Lin, J., Liu, B., Sadeh, N., & Hong, J. I. (2014). Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. 12th USENIX Security Symposium., 199–212.
[12] Liu, B., Lin, J., & Sadeh, N. (2013). Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help? http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/usr0/ftp/2013/CMU-CS-13-128.pdf
[13] Saudi Statical. (2020). in Numbers.
[14] Song, Y. (2015). PrivacyGuard : A VPN-Based Approach to Detect Privacy Leakages on Android Devices. 15–26. https://doi.org/10.1145/2808117.2808120
[15] Song, Y., & Hengartner, U. (2015). PrivacyGuard: A VPN-based Platform to Detect Information Leakage on Android Devices. Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '15, 15–26. https://doi.org/10.1145/2808117.2808120
[16] TRUSTe. (2016). 2016 TRUSTe/NCSA Consumer Privacy Infographic - US Edition | TRUSTe. https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/
[17] Yang, Z., Yang, M., Zhang, Y., Gu, G., Ning, P., & Wang, X. S. (2013). AppIntent: analyzing sensitive data transmission in android for privacy leakage detection. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13, 1043–1054. https://doi.org/10.1145/2508859.2516676
[18] Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011). Taming Information-Stealing Smartphone Applications (on Android). 4th International Conference on Trust and Trustworthy Computing, 2011, 93–107.

Aziz Alshehri received his B.S. degree in Computer Science from King Abdulaziz University, Saudi Arabia in 2006, and received M.S. degree in Computer Science from university new brunswick, Canada in 2015.
He received the PhD degree in Computer Science in Auguset 2020 from Plymouth University, UK. He is currently work as an assistant professor, Computer Science department in the Faculty of Computing at Al-Qunfudhah branch at Umm Al-Qura University

Salah Alamri received his B.S. degree in Computer Science from King Abdulaziz University, Saudi Arabia in 2010, and received M.S. degree in Computer Science from Kent State University, USA in 2014. He received the PhD degree in Computer Science in Auguset 2020 from Kent State University, USA. He is currently work as an assistant professor, Computer Science department in the Faculty of Computing at Al-Qunfudhah branch at Umm Al-Qura University.