IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 5, 2018, accepted August 14, 2018, date of publication September 17, 2018, date of current version October 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2866525

Develop a Model to Measure the Ethical Effects of Students Through Social Media Use

FAHAD ABDULLAH MOAFA[1], KAMSURIAH AHMAD[1], WALEED MUGAHED AL-RAHMI[2], NORAFFANDY YAHAYA[2], YUSRI BIN KAMIN[2], AND MAHDI M. ALAMRI[3]

[1]Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia
[2]Faculty of Education, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[3]Education Technology Department, Faculty of Education, King Faisal University, Hofuf 31982, Saudi Arabia

Corresponding authors: Waleed Al-Rahmi (waleed.alrahmi@yahoo.com) and Noraffandy Yahaya (p-afandy@utm.my)

This work was supported in part by the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, in part by Universiti Kebangsaan Malaysia through the Exploratory Research Grant Scheme under Grant ERGS/1/2013/ICT07/UKM/02/1, and in part by the Research Management Centre at the Universiti Teknologi Malaysia under Grant PY/2018/02903: Q.J130000.21A2.04E40.

ABSTRACT Social media users can be negatively affected by cyber harassment. These effects can cause emotional distress and lead people to stop using social network sites or to end their life. In addition, the users of this technology usually get upset when network providers interfere and consider such interference to be unfair. Therefore, this paper attempted to mitigate the gap in the literature concerning the use of social media for engaging in cyber harassment in the context of higher education. Therefore, the main objective was to develop a model that will bridge this gap. The model developed in this paper is based on the unified theory of acceptance and use of technology, theory of planned behavior, and technology support. To achieve the study's objectives, a questionnaire was used as the main data collection method, and it was distributed to 340 students who used social media. This paper argues that these decisions of interference can be handled by employing a method that users find sufficient and appropriate. In conclusion, this research specifically proposes a model for identifying the significant factors that are anticipated to play major roles in minimizing cyber harassment among Saudi students. The proposed model will help administrations and decision makers to formulate strategies that can significantly affect anti-cyber harassment among students.

INDEX TERMS Social media used, engage in cyber harassment, ethical effects, technology use, theory of planned behavior (TPB).

I. INTRODUCTION

The situation where individuals misuse digital media for the purpose of causing emotional damage to others is called cyber harassment [1]. This behavior leads to the suffering of others. Statistics from the United States show that over a half a million people age 18 or older were victims of this harassment [2]. In addition to the fact that victims may stop using these networks, which negatively affects these networking sites [3], [4], the victims may also end their lives [5]. An example of that is the story of an 18-year-old student from the states who committed suicide after he discovered that his roommate spied on him electronically and then used Twitter to gossip about him. Currently, the ways that people communicate, study, work, and interact is strongly influenced by technology, which has penetrated communities, businesses, and the lives of individuals. Much attention by the media has been paid to the issue of cyber harassment, which has become a popular area of research and study. Researchers and the academic press in general have focused on several issues in this regard, such as stalking, the variety of stalker types and the impacts of stalking on victims. Recently, the distinction between the two concepts of cyber harassment and cyber stalking has received much attention by the researchers in this field of research [7]. Cyber harassment has received a considerable number of assessments, but looking at the existing literature, little attention has been given to support existing different opinions. One of these opinions is related to the issue of whether cyber harassment is a criminal phenotype or is the assisted use of technology in the hands of a traditional stalker. Thus, how to define the concept of cyber harassment varies sometimes depending on the context and depending on the type of definition required, which might be clinical or legal. While there are no reliable prevalent figures for cyber harassment, there can

be no doubt that the use of innovation and technology is accelerating.

In 2013, as reported by the UN's International Telecommunication Union (ITU), 39% of the people in the word (over 2.7 billion people), were using the internet. Societies are given more opportunities and privileges through the rapid development of the internet and the technology of communication. As reported by a study on the use of the internet by children, 93% of children appeared to use the internet weekly, and 60% of 9 to 16-year-olds use it daily. This study, which was conducted on more than 25,000 children in 25 European countries, also reported that 87% of these children use the internet in their homes and 63% use it in colleges. Although teenagers use various technologies to access sexual health information, digital media is still short in filling the sexual health gap.

II. CYBER HARASSMENT EFFECTS

Plenty of services are provided through the internet. Some of these common services are online information exchanges, voting, business transactions, shopping, learning, and online gaming. Regardless of this background, the internet carries much potential for its users, such as better communications, better opportunities in commerce and more developed lives for individuals. All of these privileges directly influence the various behaviors, including financial, social, and the ethical ones. Many activities done through the internet are not harmful to people or individuals, but some activities tend to be the opposite and do not abide by ethical and social norms. These actions are normally conducted by individuals who do not have the same fear of consequences as in the physical world. Some of these corrupt activities might be illegal file-sharing, the accessibility of explicit adult-oriented materials and the possibility of sending spam to millions. These activities can harm lots of users, including businesses and organizations. There is no doubt that the repercussions of cybercrime are a serious global concern. The Kingdom of Saudi Arabia (KSA) is one of many countries that is suffering from cybercrime, and the KSA is one of the most affected countries in the Middle East according to a report from Symantec. In 2014, 62% of internet users in Saudi Arabia faced cybercrimes. Cybercrime is rising across Saudi society, and protecting against cyber threats is an ongoing management challenge for organizations. The Saudi official report estimated that more than 3.6 million people fell victim to cybercrime [9], which costs individuals a combined US$0.5 billion a year [10]. Saudi Arabia is in the 16th place of the countries that suffer the most from cybercrime in the world [11]. In contrast, students and researchers [12], [13] have positive attitudes and intentions to use social media for educational purposes. As mentioned earlier, in the introduction of this study, cyber harassment is defined as a type of cybercrime in official reports made by Saudi government authorities who specialize in security aspects of information and electronic crimes. They indicate that there is a sharp rise in the proportion of electronic crimes, especially in cyber extortion crimes, and assure that cybercrime is on the rise across Saudi Arabia. The rate increased by 57% in 2014 compared to 2013, and protecting against cyber threats is an ongoing management challenge for organizations [9].

III. THEORETICAL MODEL

The supply of online services that are secure falls on the government and on educational institution managers in the case that the users are tertiary students studying in higher educational institutions. It is a serious problem worthy of investigation due to the lack of a diagnostic study that focuses on cyber harassment in the KSA. No studies are available that address the factors influencing behavioral intentions to minimize cyber harassment among youth and for all these types of crimes [9], [14], [15]. Consequently, there is an urgent need to conduct a thorough study to investigate the cyber harassment factors in the Saudi context. Thus, this research will use the Decomposed Theory of Planned Behavior (DTPB) [16], [17]. The Theory of Planned Behavior (TPB) emerged from the Theory of Reasoned Action [18]. In their study named ''Understanding Information Technology usage: a test of competing models'', conducted in June 1995, Taylor and Todd became the founders of the Theory of Planned Behavior (DTPB). This model investigates the subjective norms (i.e., social influences), perceived behavioral controls and dimensions of attitudinal beliefs. It decomposes them into precise dimensions of beliefs [16]. In DTPB, the behavioral intention is the main source of a behavior, and there are three main constructs known as the attitude toward behavior (ATB), the subjective norm (SN), and the perceived behavior control (PBC), which were first referred to in TPB and DTPB. Thinking that they need to implement changes in their work processes, the peers of users might find that they need to use a particular system. To have certain outcomes, employees may insist on using the system. In this case, subjective norms or intentions are not influenced by a monolithic normative structure because the referent groups can terminate one another. Therefore, there were some suggestions that normative beliefs should be decomposed into two referent groups (peers and superiors) since the anticipation of both peers and superiors can be different [16]. In the case of the Perceived behavior control (PBC), three constructs were identified. These constructs are self-efficacy, resource facilitating conditions, and technology facilitating conditions. The first has to do with perceived ability. It is estimated that higher levels of behavioral intentions and IT usage can result from higher levels of self-efficacy [20]. In addition, the UTAUT model is used to discover the demographic factors (moderating factors) that influence the use of new technology by individuals [21]. According to Pew Research Center, UTAUT Factors such as age and gender can affect the experience of Cyber harassment [22]. Therefore, this study will bridge this gap by introducing a conceptual framework where Theory Planned Behavior (DTPB) is decomposed into the Unified Theory of Acceptance and Use of Technology (UTAUT) and technology support. Therefore, the current

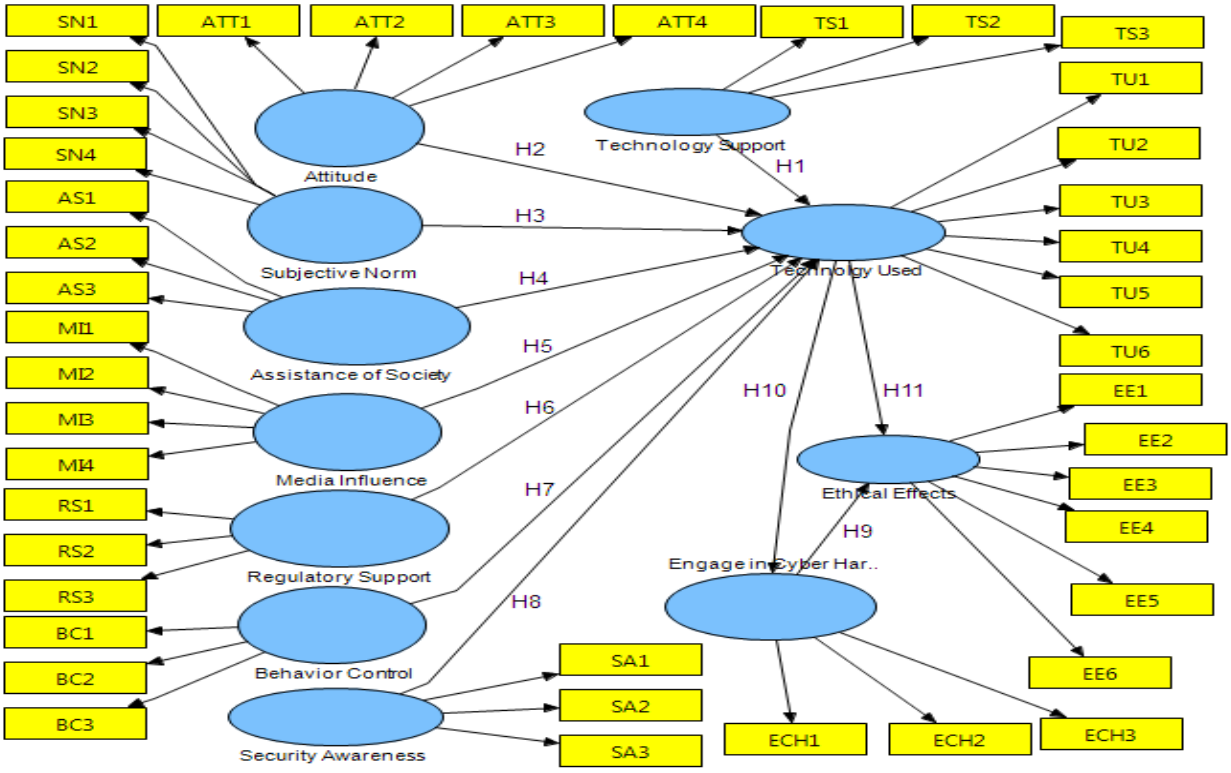

FIGURE 1. Research model.

model can benefit academics since it illustrates how these factors are related. However, this research found that technology uses for cyber harassment via students results in the three main themes of social, ethical and financial effects. Therefore, the measured, relevant variables for the technology used and the intentions to engage for cyber harassment that were adopted as independent variables in this research are the following: technological support, attitudes, subjective norms, seeking assistance from society, the mass media's influence, perceived behavioral control, regulatory support and the governmental role, and security awareness. Additionally, intentions to engage in cyber harassment and technology use for cyber harassment were adopted as mediating variables. Finally, the dependent variables that influence students are the three main themes of social, ethical and financial effects. See Figure 1.

In this section, the model of the current study and the hypotheses based on the model are presented. Moreover, the different factors related to the model of the current study are discussed in the following sections from 3.1 to 3.11.

A. TECHNOLOGY SUPPORT

One of the main reasons why some countries are not developed in terms of ICT is because they do not have easy access to the internet or computers. According to Goh (1995), the endeavors of providing the appropriate infrastructure, the necessary tools, internet access and software are known as technology support [23]. The quality of technology and internet services is connected to technology support. A significant positive relation was found between technology support and perceived behavioral control in the case of tertiary students in Malaysian universities. A study found that the availability of technology support would affect those students' adoption of the online educational services. In contrast, students and researchers [24] have a positive attitude towards and intentions to use technological tools such as social media for educational purposes.

H1: There is a significant relationship between technology support and the technology used for cyber harassment.

B. ATTITUDE

Both theory of reasoned action TRA and Theory of Planned Behavior TPB are used to estimate and describe the various behaviors that are linked to the limited set of constructs [26]. In this study, DTPB [16] is used, and five perceived attributes of innovation are identified to measure the relation between attitudinal beliefs and innovation. These attributes are perceived ease of use, perceived usefulness, compatibility, trial ability and observability. Other factors were identified by researchers that were related to the attitude dimension in terms of behavioral intentions in adopting new innovations. For example, factors such as perceived risk and trust and awareness were added to the attitude dimension towards behavioral intentions by Al-Majali *et al.* [27]. The low levels

of security and privacy over the internet create a risk that is presented by an obstacle in adopting new technology. Meanwhile, other researchers consider that the use of social media has positive impacts on collaboration and engagement among students [28].

H2: There is a significant relationship between attitudes and the technology used for cyber harassment.

C. SUBJECTIVE NORM

A subjective norm is defined as the social pressure to carry out a certain behavior [29]. The behavior of individuals to abide by security policies is influenced by Subjective norms. The recognition of the risks and the severity of threats is influenced by the protective behaviors of important people, such as mass media, family, friends, leaders, or colleagues [30]. Seeking protective knowledge from those people can enhance the way in which individuals address these threats [31]–[33]. Abiding by security protection behaviors in the workplace [33] and home [34] can be positively influenced by social norms. The DTPB model was utilized by Taylor and Todd [16] to explore the impact of the family on several computer centers' potential users.

H3: There is a significant relationship between subjective norms and the technology used for cyber harassment.

D. SEEKING ASSISTANCE OF SOCIETY

Many behavioral researchers consider social seeking assistance such as family as one of the subjective behavioral norms that has an influence upon individuals' behaviors [16]. In the field of peoples' behaviors towards IT usage, especially toward the adoption of new technology services, there are two previous studies confirming the family's influence as one of the subjective norm determinants in regard to an individual's minimization of cyber harassment and other technology services. For example, Fang and Shih [35] discuss the family's influence upon the subjective norms in the behaviors of a number of bank clients in Taiwan. The results show that family significantly and positively affects the subjective norms. Nor and Pearson [36] conducted a study in Malaysia in IBS. The researchers confirm the important role played by the family in the behaviors of a number of college students in Malaysia.

H4: There is a significant relationship between seeking the assistance of society and the technology used for cyber harassment.

E. MASS MEDIA INFLUENCE

During the last few years, the number of children and adolescents using social media sites has increased. O'Keeffe *et al.* [37] report that 22% of teens log on to a social media site more than 10 times a day and more than half of adolescents log on more than once a day. Individual identities are formed through our connection with others, and what drives online and mobile communication is a young person's desire to connect with their peers anywhere and at any time. Social networking sites also allow for the public sharing of information, which can have intended and unintended risks for teens and young adults, and sexting can also create unintended consequences, such as harmed reputations, broken relationships, and shattered friendships [38]. This contrasts with [39] and [40] where social media is used for engagement among students.

H5: There is a significant relationship between the mass media influence and the technology used for cyber harassment.

F. REGULATORY SUPPORT

On a global level, regulations for the use of the internet are posing a remarkable challenge to the law. This is due to several reasons. First, only approximately 10% of the cybercrimes are usually reported and approximately 2% of these cases are prosecuted in an appropriate way [41]. Second, it is easy for the offenders to seek shelter or hide from the local and global internet laws due to the weakness of cross-border enforcement. This is also different across countries based on their moral values and laws [42]. The concept of regulatory support is known as the roles implemented by governments to handle e-business through regulations and incentives [45].

H6: There is a significant relationship between regulatory support and the technology used for cyber harassment.

G. SECURITY AWARENESS

There are several reasons why college students use technology and information systems (IT/IS). Some of these reasons are taking online courses, using email, using the blackboard system, accessing social networks, and using their smart iPads, phones, and PCs. As this phenomenon is rapidly decreasing, there is a need to protect information and systems against security attacks. IS security, as reported by the EDUCAUSE member institution survey [46], is considered as having the first or the second highest ''potential to become increasingly important in the coming years''. It has been observed that 83% of the victims were not targets of choice but of opportunity [47]. Opportunistic attacks refer to the fact that victims are targeted in the first place because of a weakness that was utilized by the attackers. Therefore, students should be aware of how to defend their systems and information against such attacks. Non-malicious end-users who do not respect IS security policies are the direct cause of more losses than malicious users [48]. For college students, being well-informed in terms of technology does not mean that they understand how to defend their information and systems effectively against such attacks. It is suggested that users should raise their security awareness and enhance their security techniques and procedures [49].

H7: There is a significant relationship between security awareness and the technology used for cyber harassment.

H. PERCEIVED BEHAVIOR CONTROL

According to [29] and [50], the beliefs of individuals regarding the ability to a person to behave is known as perceived behavioral control. Some internal and external factors

influence these beliefs. For the internal factors, they are represented by the individual's self-belief in the ability to carry out the behavior. The external factors of behavioral control, which [55], [56] are known as 'facilitating conditions', refer to one's beliefs concerning the availability of resources, such as money, time, and other resources needed to implement the behavior. In addition, the control beliefs in the original DTPB involve two factors. These factors are resource facilities' conditions, self-efficacy and technology facilities' conditions. For this study, the self-efficacy remains under technology support but facilities' conditions are replaced with the government's roles and regulatory support. This replacement gives the study more opportunities to examine the impact of self-efficacy among young people. Furthermore, the discussion of the problem statement shows that the lack of the governmental regulatory support and the insufficiency of internet infrastructure are other factors that could cause cyber harassment to not be minimized among youth in KSA. Furthermore, authentic UTAUT includes two factors, namely, social influence and facilities' conditions. For this study, social influence is replaced with social seeking assistance and mass media, and facilities' conditions are replaced with the government's role and regulatory support.

H8: There is a significant relationship between perceived behavioral control and the technology used for cyber harassment.

I. ENGAGE IN CYBER HARASSMENT

The influence of attitudes on behaviors through behavioral intentions in TRA has been illustrated by Fishbein and Ajzen [18]. Attitudes, in some studies, were reported to have strong influences on behaviors and can anticipate behaviors more than behavioral intentions [51], [52]. Previous literature on attitudes argues that it is a significant factor in new technology adoption [28], [53]. The existing literature shows that verbal, physical and cyber harassment and negative bystander behaviors are normally associated with the attitude towards cyber harassment [54]. Compared to subjective norms and perceived behavioral controls, one of the important studies in this area discovered that adolescents' intentions to cyber bully can be mostly predicted by the attitude towards cyber bullying [55]. Similarly, adolescents with aggressive attitudes are more likely to be involved in cyber bullying. Based on the existing literature, this attitude has been approached from different perspectives. Furthermore, there is a consistency in the findings on the relationship between both behavior intentions and attitudes. It is also found that intention-formation across behavioral domains in adolescents [26] includes aggressive acts such as peer sexual harassment and abuse [59]. These domains can be interpreted by attitudes, social norms, and self-efficacy principles [29], [57]. Nevertheless, there is not much correspondence between intentions and actual behaviors [60]. Thus, it is suggested by researchers that DTPB approaches can be combined with theory-driven variables in order to explain specific behaviors in particular situations and social contexts [61]. Therefore, we recommend that colleges and universities encourage students to use social media for engagement in educational purposes [58].

H9: There is a significant relationship between intentions to engage in cyber harassment and ethical effects.

J. TECHNOLOGY AND SOCIAL MEDIA USED EFFECTS

Adolescents can get access to multiple options for interaction through social networking sites (SNS) [62], [63]. Although, there is not a unified definition of harassment, it mostly refers to the ''rude, threatening or offensive content directed at others by friends or strangers and performed via electronic means such as internet or mobile phones'' [65], [66]. Cyberbullying, hate speech, single insults, cyber stalking, spamming, identity theft or online sexual harassment are all considered forms of harassment. In statistics regarding harassment, it was reported that 21% of adolescents in Canada, 14% of Swedish boys, 20% of Swedish girls, 51% of the adolescents in Singapore, and 69.9% in Portuguese reported being the victim of cyber harassment in the past year [65], [67]. Meanwhile, other researchers consider that the use of social media has positive impacts on collaboration and engagement among students [68], [69]. Other issues were raised, such as the language barrier in using SNS on Facebook and Twitter. Although the English language is used on these sites and translation options are provided, it still does not include all languages and the accuracy level of the translations might not be appropriate [70].

H10: There is a significant relationship between the technology used for cyber harassment and engagement in cyber harassment.

H11: There is a significant relationship between the technology used for cyber harassment and the ethical effects.

K. ETHICAL EFFECTS

Sometime individuals do not use social networking sites (SNSs) appropriately and ethically. This might be related to their expanding use and flexible functionalities. There is a need for SNS users to know how to behave in these cases since they encounter ethical dilemmas on a daily basis. The use of Social Networking Sites (SNSs) became very popular among individuals for the purpose of communication. Some of the platforms also became very popular among the users of (SNSs), such as Facebook, which now has more than one-third of the world's population as users [71]. Many issue are related to ethical considerations, such as employee surveillance [72], [73], the application of users' data for advertising purposes [74], privacy [75], identity theft [76], inappropriate profile content [77], cyberstalking [78], and cyberbullying [79]. Moafa *et al.* [80], [81] have assured that the Saudis will remain at risk of cyber harassment until these factors are fully investigated among the Saudi community. Thus, they proposed a framework to help the administration and decision-makers in the KSA to formulate strategies that can significantly affect anti-cyber harassment among youths. Meanwhile, other researchers consider that the use

of social media has positive impacts on e-learning [82]. To develop moral accountabilities that lead to better ethical actions, the enhancement of individuals should be reinforced through the initial stages to the higher stages of moral development [83]. Useful tools to achieve this target are education and discussions targeting these ethical dilemmas. Ethical decisions are a complicated process that are linked to the do or don't intentions. This might be difficult since there is not a recognized approach for teaching ethical issues nor a generally accepted theory of Computer Ethics [84]. In such case, individuals' intentions to behave unethically in SNSs are more accepted than other kinds of unethical behaviors. There may be several reasons, such as opportunity, belief systems, cultural elements or social elements. Generally, preventive plans and actions fail mostly because there are no attempts to systematically theorize unethical behavior in the context of SNSs. This directly influences people who use the internet and other information and communications technologies (ICTs).

IV. RESEARCH METHODOLOGY

The current study uses a questionnaire that is administered by an enumerator. This questionnaire collected data from students with different nationalities. Using Smart PLS 3.0, the reliability and validity of the model were measured. To develop a model that can manage, be applied to, analyze e-learning use, a suitable methodology is employed to guide this inquiry. The current quantitative study uses a questionnaire as the major tool of data collection. Random sampling is used and a total number of 340 university students participated in the study of Krejcie and Morgan [85]. Undergraduate students received a total of 106 questionnaires. Smart PLS and the SPSS Version 20 software are used to analyze the data. Based on the study's objective, the instrument of data collection and the models were identified [86]–[88]. A pilot study was conducted prior to the main study and an acceptable level of Cronbach's alpha was obtained. The students had to respond on a 5-point scale ranging from (1) as ''strongly disagree'' to (5) as ''strongly agree.'' First, Partial Least Square Structural Equations Modeling (PLS-SEM) in Smart PLS 3.0 was used to confirm the validity and reliability of the measurement model. To determine the goodness-of-fit of the model, factor loadings were used to confirm the construct validity, composite reliability, Cronbach's alpha, and convergence validity. For the confirmation of discriminant validity, it was recommended by Hair *et al.* [89] to use the criterion test for that purpose. The measures used in this study were adopted from the Theory of Planned Behavior (TPB) into the Unified Theory of Acceptance and Use of Technology (UTAUT) as well as technology support. The variables that are included are technology support (TS), subjective norms (SN), the assistance of society (AS), attitudes (ATT), media influence (MI), regulatory support (RS), security awareness (SA), behavioral controls (BC), the technology used (TU), engagement in cyber harassment (ECH), and ethical effects (EE). Moreover, the measures that were used in [6], [8], [10], [24], [50], and [51] are adopted in the current study. The 42-item questionnaire was distributed among the respondents. See the Appendix.

V. RESULTS AND DISCUSSION

The questionnaires were completed by 340 respondents. There were 151 male respondents and 189 female respondents, equating to 44.4% and 55.6 of the total sample, respectively. 7 respondents (2.1%) were less than 17 years old, while 205 respondents (60.3%) were in the 18-27-year-old category. 128 respondents (37.6%) were above 28 years old. With regards to the marital status of respondents, 163 (47.9%) respondents were single, 153 (45.0%) respondents were married, 18 (5.3) respondents were divorced, and 6 (1.8%) respondents were widowed. Regarding their levels of education, 110 (32.4%) respondents were in the preliminary level, 139 (40.9%) respondents were in level one, 20 (5.9%) respondents were in level two, 25 (7.4%) respondents were in level three, and 46 (13.5%) respondents were in level four. Cronbach's alpha, the composite reliability, and the convergent validity were calculated before the hypotheses testing in order to test the construct validity. Discriminant validity was also tested for this study based on the recommendations of Fornell and Larcker [91].

A. CONSTRUCT VALIDITY OF MEASUREMENTS

The extent to which certain items measure the concepts that they are designed to measure is called the construct validity [89]. This is gained through a systematic literature review targeting items that have been assessed by other researchers. Table 1 illustrates that the items are properly constructed based on their loadings. The items have to load to the construct that they are intended to measure, as maintained by Chow *et al.* [90].

B. CONVERGENT VALIDITY OF MEASUREMENTS

The composite reliability produced satisfactory results that were above 0.70. The values ranged from 0.692 to 0.898. The results of the Cronbach were between 0.712 to 0.863, thus indicating satisfactory results. The average variance extracted (AVE) also received a value of 0.5 and ranged from 0.528 to 0.715. Table 2 below illustrated the results of the confirmatory factor analysis (CFA).

C. DISCRIMINANT VALIDITY OF MEASUREMENTS

The differences between the sets of concepts and their own indicators are known as the discriminant validity. The discriminant validity of all constructs are supported as their values were above 0.50, which are significant at $p = 0.001$ [91]. The square root of the average variance shared by a single construct's items should not be exceeded by the correlations between the items in two constructs, as indicated by Hair *et al.* [89] (See Table 3).

D. ANALYSIS OF THE STRUCTURAL MODEL

As planned in this stage, the research hypotheses are examined and the relations between the constructs were

TABLE 1. Loading and cross-loadings of items.

No	Cod	TS	ATT	SN	AS	MI	RS	SA	BC	ECH	TU	EE
1	TS1	**0.631**	0.225	0.165	0.034	0.188	0.088	0.044	0.144	0.115	0.117	0.102
2	TS2	**0.669**	0.263	0.221	0.138	0.120	0.140	0.222	0.343	0.327	0.242	0.233
3	TS3	**0.662**	0.194	0.304	0.275	0.319	0.141	0.071	0.153	0.158	0.198	0.197
4	ATT1	0.304	**0.803**	0.420	0.304	0.234	0.264	0.299	0.371	0.368	0.383	0.457
5	ATT2	0.348	**0.673**	0.364	0.319	0.165	0.165	0.340	0.346	0.391	0.258	0.424
6	ATT3	0.251	**0.836**	0.593	0.319	0.365	0.249	0.428	0.447	0.559	0.449	0.514
7	ATT4	0.167	**0.650**	0.496	0.197	0.191	0.228	0.271	0.287	0.347	0.320	0.401
8	SN1	0.359	0.536	**0.879**	0.479	0.373	0.241	0.396	0.490	0.586	0.591	0.554
9	SN2	0.232	0.448	**0.773**	0.431	0.248	0.181	0.320	0.375	0.360	0.423	0.360
10	SN3	0.305	0.406	**0.700**	0.325	0.326	0.312	0.275	0.398	0.380	0.451	0.418
11	SN4	0.221	0.613	**0.772**	0.384	0.373	0.261	0.389	0.566	0.480	0.449	0.515
12	AS1	0.113	0.259	0.290	**0.826**	0.302	0.393	0.439	0.368	0.285	0.324	0.450
13	AS2	0.141	0.436	0.364	**0.723**	0.281	0.346	0.337	0.396	0.404	0.320	0.479
14	AS3	0.232	0.434	0.447	**0.700**	0.258	0.319	0.367	0.519	0.471	0.391	0.545
15	MI1	0.242	0.105	0.189	0.298	**0.706**	0.481	0.276	0.294	0.203	0.184	0.289
16	MI2	0.130	0.072	0.167	0.277	**0.745**	0.454	0.102	0.207	0.122	0.069	0.213
17	MI3	0.195	0.005	0.091	0.206	**0.723**	0.492	0.073	0.217	0.116	0.099	0.214
18	MI4	0.264	0.459	0.502	0.249	**0.781**	0.182	0.321	0.439	0.401	0.305	0.466
19	RS1	0.166	0.318	0.362	0.365	0.387	**0.893**	0.372	0.413	0.325	0.266	0.399
20	RS2	0.202	0.207	0.142	0.247	0.349	**0.821**	0.328	0.322	0.188	0.195	0.303
21	RS3	0.126	0.236	0.263	0.421	0.426	**0.802**	0.352	0.406	0.250	0.173	0.350
22	SA1	0.219	0.281	0.499	0.300	0.267	0.308	**0.793**	0.404	0.295	0.321	0.434
23	SA2	0.171	0.236	0.321	0.300	0.244	0.383	**0.859**	0.251	0.245	0.292	0.390
24	SA3	0.170	0.350	0.340	0.435	0.273	0.221	**0.864**	0.406	0.338	0.266	0.438
25	BC1	0.237	0.342	0.456	0.340	0.330	0.336	0.315	**0.778**	0.358	0.364	0.416
26	BC2	0.326	0.357	0.460	0.499	0.439	0.364	0.515	**0.845**	0.450	0.471	0.643
27	BC3	0.289	0.473	0.498	0.308	0.336	0.390	0.405	**0.804**	0.605	0.555	0.568
28	ECH1	0.219	0.484	0.435	0.345	0.245	0.148	0.259	0.435	**0.815**	0.530	0.472
29	ECH2	0.257	0.498	0.541	0.346	0.329	0.301	0.336	0.526	**0.844**	0.613	0.502
30	ECH3	0.353	0.434	0.479	0.458	0.326	0.307	0.357	0.525	**0.827**	0.587	0.636
31	TU1	0.243	0.414	0.417	0.325	0.264	0.223	0.315	0.501	0.530	**0.745**	0.476
32	TU2	0.262	0.463	0.519	0.186	0.225	0.217	0.296	0.489	0.569	**0.820**	0.454
33	TU3	0.238	0.284	0.544	0.415	0.304	0.189	0.301	0.431	0.571	**0.784**	0.489
34	TU4	0.307	0.431	0.592	0.385	0.179	0.190	0.316	0.503	0.663	**0.879**	0.482
35	TU5	0.185	0.339	0.343	0.278	0.132	0.191	0.350	0.412	0.470	**0.717**	0.434
36	TU6	0.149	0.308	0.417	0.199	0.232	0.194	0.367	0.376	0.392	**0.673**	0.435
37	EE1	0.248	0.455	0.548	0.425	0.315	0.104	0.367	0.530	0.438	0.503	**0.656**
38	EE2	0.256	0.506	0.484	0.417	0.407	0.369	0.485	0.614	0.594	0.412	**0.818**
39	EE3	0.238	0.407	0.366	0.369	0.360	0.418	0.428	0.401	0.460	0.392	**0.718**
40	EE4	0.215	0.556	0.504	0.388	0.337	0.394	0.513	0.502	0.544	0.451	**0.780**
41	EE5	0.191	0.399	0.426	0.528	0.376	0.329	0.442	0.563	0.436	0.491	**0.791**
42	EE6	0.187	0.420	0.384	0.423	0.349	0.302	0.440	0.491	0.492	0.476	**0.790**

investigated. Through the use of Smart PLS 3.0, the PLS algorithm was applied in order to achieve this objective. The resulting path coefficients are illustrated in Figure 1, while the results of the hypotheses were illustrated in Figures 2 and 3.

Regarding the first hypothesis, the relation between technology support and technology used is positive and significant ($\beta = 0.244$, $t = 2.909$, $p < 0.001$). Thus, the results positively support the first hypothesis. The second hypothesis is also supported as the analysis shows a positive relationship between attitudes and the technology used ($\beta = 0.472$, $t = 7.775$, $p < 0.001$). The third hypothesis is also positively supported, as there is a significant relationship between the subjective norms and the technology used ($\beta = 0.367$, $t = 6.071$, $p < 0.001$). Similarly, the fourth hypothesis on the relationship between the assistance of society and the technology used is positive and significant ($\beta = 0.415$, $t = 8.341$, $p < 0.001$). Thus, the fourth hypothesis is also supported by the results of the current study. Along these lines, the results indicate that there is a significant relationship between the media's influence and the technology used ($\beta = 0.363$, $t = 7.495$, $p < 0.001$), which supports the fifth hypothesis. The next hypothesis is not supported as the analysis shows a negative relationship between regulatory support and the technology used ($\beta = 0.044$, $t = 1.002$, $p < 0.001$), which also does not support the sixth hypothesis.

TABLE 2. Constructs, items, and confirmatory factor analysis results.

No	Variables	Code	Factors Loading	Cronbach's Alpha	Composite Reliability	AVE	R Square
1	Technology Support	TS1	**0.631**	0.786	0.692	0.528	0.000
2		TS2	**0.669**				
3		TS3	**0.662**				
4	Attitudes	ATT1	**0.803**	0.732	0.831	0.555	0.000
5		ATT2	**0.673**				
6		ATT3	**0.836**				
7		ATT4	**0.650**				
8	Subjective Norms	SN1	**0.879**	0.789	0.863	0.614	0.000
9		SN2	**0.773**				
10		SN3	**0.700**				
11		SN4	**0.772**				
12	Assistance of Society	AS1	**0.826**	0.712	0.795	0.565	0.000
13		AS2	**0.723**				
14		AS3	**0.700**				
15	Media Influence	MI1	**0.706**	0.785	0.828	0.547	0.000
16		MI2	**0.745**				
17		MI3	**0.723**				
18		MI4	**0.781**				
19	Regulatory Support	RS1	**0.893**	0.794	0.877	0.705	0.000
20		RS2	**0.821**				
21		RS3	**0.802**				
22	Security Awareness	SA1	**0.793**	0.791	0.878	0.715	0.000
23		SA2	**0.859**				
24		SA3	**0.864**				
25	Behavioral Control	BC1	**0.778**	0.744	0.851	0.656	0.000
26		BC2	**0.845**				
27		BC3	**0.804**				
28	Engagement in Cyber Harassment	ECH1	**0.815**	0.774	0.868	0.687	0.487
29		ECH2	**0.844**				
30		ECH3	**0.827**				
31	Technology Used	TU1	**0.745**	0.863	0.898	0.597	0.473
32		TU2	**0.820**				
33		TU3	**0.784**				
34		TU4	**0.879**				
35		TU5	**0.717**				
36		TU6	**0.673**				
37	Ethical Effects	EE1	**0.656**	0.853	0.891	0.579	0.466
38		EE2	**0.818**				
39		EE3	**0.718**				
40		EE4	**0.780**				
41		EE5	**0.791**				
42		EE6	**0.790**				

The seventh hypothesis is also positively supported, as there is a significant relationship between behavioral controls and the technology used ($\beta = 0.326$, t = 7.548, p < 0.001). Similarly, the eighth hypothesis on the relationship between security awareness and the technology used is also supported ($\beta = 0.476$, t = 7.805, p < 0.001). The next hypothesis is also supported as the analysis shows a positive relationship between engaging in cyber harassment and the ethical effects ($\beta = 0.463$, t = 9.198, p < 0.001), which also supports the ninth hypothesis. Additionally, the tenth hypothesis on the relationship between the technology used and engaging in cyber harassment is supported ($\beta = 0.698$, t = 25.566, p < 0.001). For the final hypothesis, the relationship between the technology used and the ethical effects is significant ($\beta = 0.274$, t = 4.695, p < 0.001). The results are presented in Table 4.

E. DISCUSSION

The current study investigated the different factors attached to the prediction of teenagers' willingness to defend them against harassment online. It is of a great importance to conduct studies exploring the various factors of cyber

TABLE 3. Discriminant validity.

No	Variables	TS	ATT	SN	AS	MI	RS	SA	BC	ECH	TU	EE
1	Technology Support	**0.817**										
2	Attitude	0.381	**0.933**									
3	Subjective Norm	0.470	0.492	**0.811**								
4	Assistance of Society	0.386	0.567	0.601	**0.889**							
5	Media Influence	0.558	0.605	0.682	0.654	**0.877**						
6	Regulatory Support	0.347	0.335	0.455	0.365	0.470	**0.915**					
7	Security Awareness	0.407	0.309	0.452	0.310	0.421	0.456	**0.798**				
8	Behavioral Control	0.452	0.452	0.516	0.467	0.588	0.332	0.417	**0.891**			
9	Engagement in Cyber Harassment	0.520	0.639	0.584	0.587	0.596	0.424	0.316	0.442	**0.883**		
10	Technology Used	0.391	0.486	0.587	0.697	0.596	0.288	0.258	0.414	0.618	**0.871**	
11	Ethical Effects	0.250	0.350	0.355	0.338	0.293	0.312	0.196	0.198	0.363	0.304	**0.830**

TABLE 4. Hypotheses testing.

H	Independent	Relationship	Dependent	Path	S.E.	T. Value	Result
H1	TS	→	TU	0.244	0.045	2.909	Supported
H2	ATT	→	TU	0.472	0.043	7.775	Supported
H3	SN	→	TU	0.367	0.062	6.071	Supported
H4	AS	→	TU	0.415	0.049	8.341	Supported
H5	MI	→	TU	0.363	0.043	7.495	Supported
H6	RS	→	TU	0.044	0.042	1.002	Unsupported
H7	BC	→	TU	0.326	0.043	7.548	Supported
H8	SA	→	TU	0.476	0.041	7.805	Supported
H9	ECH	→	EE	0.463	0.052	9.198	Supported
H10	TU	→	ECH	0.698	0.028	25.566	Supported
H11	TU	→	EE	0.274	0.060	4.695	Supported

Note: S.E: standard error

harassment in the Saudi context. To achieve this purpose, the current study uses the Decomposed Theory of Planned Behavior (DTPB) [16], [17]. It also utilizes the Theory of planned behavior (TPB) [18], which is considered an extension to the theory of reasoned action. Taylor and Todd in June 1995 founded the Decomposed Theory of Planned Behavior (DTPB) in their study named ''Understanding Information Technology usage: a test of competing models''. In particular, three dimensions are investigated in the current study and decomposed into specific belief dimensions [16]. These dimensions are subjective norms (i.e., social influences), attitudinal beliefs, and perceived behavioral controls. Furthermore, the demographic factors (moderating factors) that affect the way that individuals use technology are explored through UTAUT [21]. The current study is an attempt to bridge this gap by combining Theory of Planned Behavior (TPB) the Unified Theory of Acceptance and Use of Technology (UTAUT) and technology support in the conceptual framework of the study. Computers and the internet are known as facilitating tools in classrooms [46], [49] and many the students in our sample were either involved in or heard of people involved in cyber harassment. In particular, two-thirds of students stated that they had incidents of cyber harassment while one-quarter of the sample were victims multiple times. Around a quarter of the students in our sample revealed that they use this technology to intentionally hurt their peers. Furthermore, many said that such experiences negatively affected them and that they had been victims in other ways. These results indicate that online bullying truly exists and questions such as how and why adolescents use this advanced technology to harm one another deserve more research. In addition, cyber harassment may have consequences related to bullying at college. For instance, the behaviors of ''electronic bullies'' might be worse and more harmful to their victims in the cases that they are not identified. It is suggested that future research should examine how the level of cyber bullying can be possibly alleviated and how it maintains or intensifies other forms of bullying. As revealed by Wolak *et al.* [66] and Hinduja and Patchin [79] on college bullying, feelings of stress and discomfort occur with the victims of cyber harassment. These feelings and symptoms are sadness, anger, anxiety, and fear that may have impaired their ability to

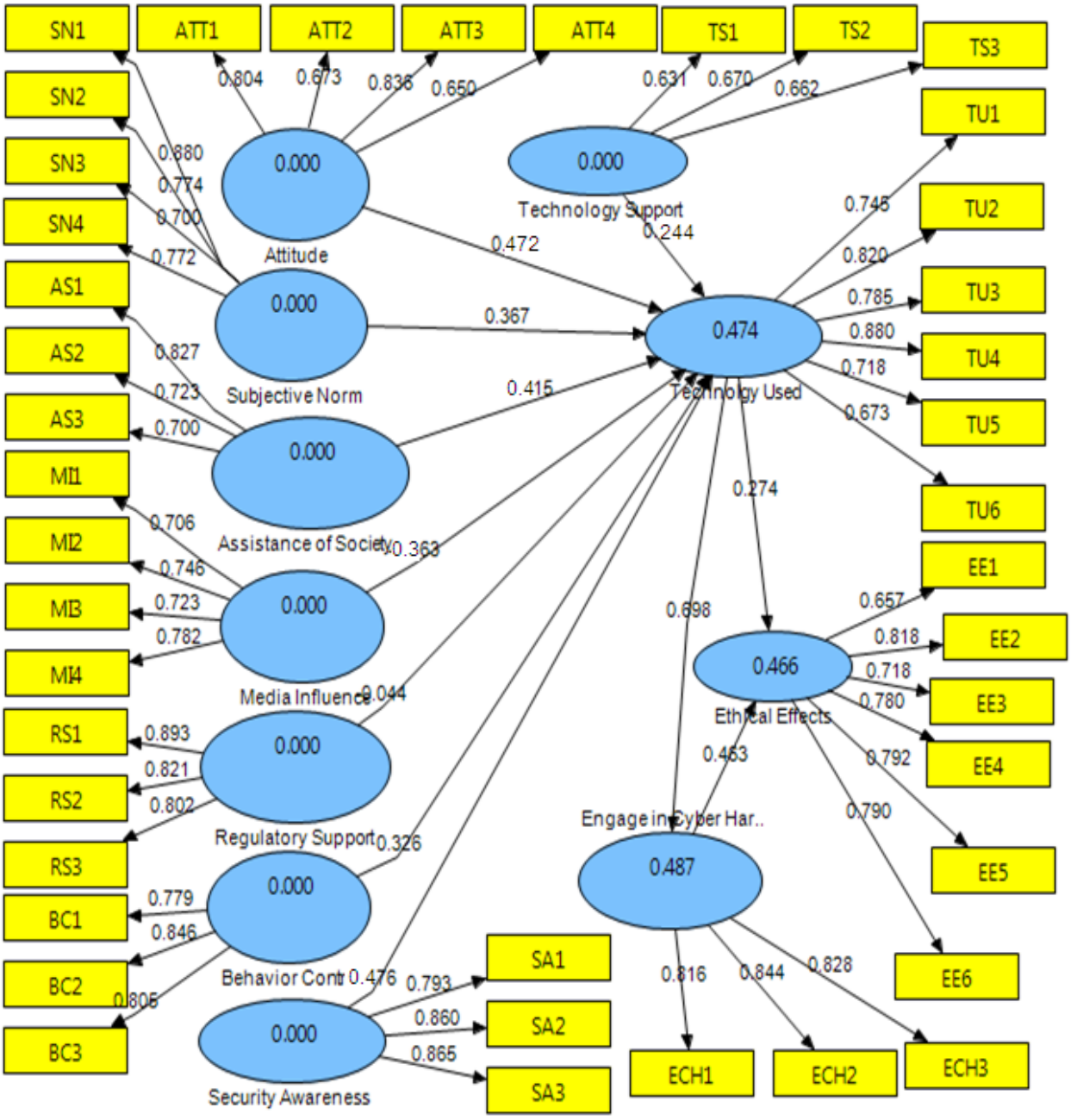

FIGURE 2. Path coefficients results.

concentrate and succeed academically. Although peer witnesses are unlikely to happen during cyber bullying, such as transmitting threatening messages through cellphones, these incidents still have similar impacts on victims as represented by the power and control they have over them through humiliation. Supported by previous studies, the victims of online harassment go through the same assessment processed as those with health risks. Cyber bullying in the current study is investigated within the confines of a certain social media platform that is considered popular among teenagers, including those in the Kingdom of Saudi Arabia (KSA). The findings of the current study indicate that regardless of the fact that these social networks are there to enhance our social experiences, many negative experiences were identified and reported. For Facebook, more than half of the people who use this platform reported that have been the victims of Facebook bullying at least one time in the last year. Additionally, most of these students have been confronted with abusive actions on this platform. As the use of the internet becomes a daily activity practiced by teenagers, it is expected that

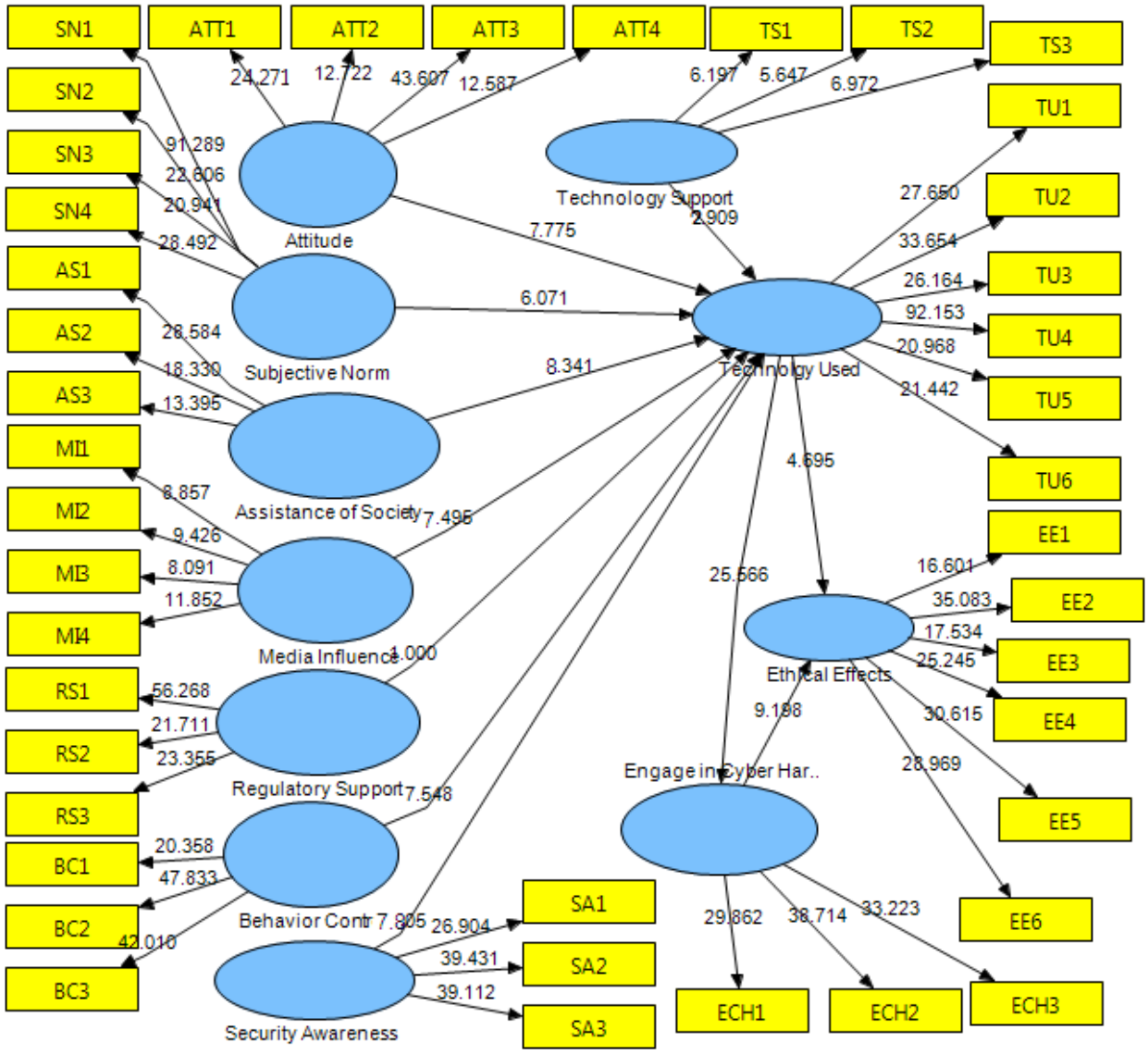

FIGURE 3. Path coefficients' T values.

they face information or experiences regarding other online threats, such as being victims of online hacking and data theft [9], [47]. Avoiding strangers on the internet and using online fabricated personas are common protective behaviors against online threats and are considered as protective measures against these attacks [65]. Conversely, the web and web-based social networking have significantly expanded in simplicity and speed, and thus social networking sites also allow for the public sharing of information, engagement, and collaborative learning [92], [93]. The findings are also in line with other previous studies conducted about Facebook is used for communication entertainment and sharing news, pictures and songs. In addition, their Facebook profile picture is alone and students were aware that swearing is considered a form of misconduct, which is a good sign [94].

VI. CONCLUSION

To sum up, there is an urgent need to raise awareness among young users on to how to address the online information. Additionally, parents and others should be able to address sexual health web sites and content in traditional media in which healthier sexual behaviors are promoted. This is of a great importance to help putting adolescents on the right track. The current research has eleven hypotheses, and the results supported and verified ten of them. A significant relationship was observed among the factors proposed in the hypotheses, such as technology support, attitudes, subjective norms, societal assistance, the mass media's influence, security awareness, perceived behavioral controls, engagement in cyber harassment, technology and social media effects, and ethical effects. However, one hypothesis that has an

TABLE 5.

Factors	No	Items
Technology Support	1	The speed of the internet connection is important in decreasing cyber harassment.
	2	The internet makes cyber harassment easier.
	3	The availability of technological materials makes cyber harassment easier.
Attitudes	1	Do you think that the student deserves the amount of cyber harassment that other students are causing to him/her just because of his/her occasional wrong behaviors?
	2	Do you think that it is possible for some students to get what they want from other students by threatening them or by sharing harmful things about them on the internet?
	3	Do you think that when two students behave badly on the internet, other students should prevent them from doing that?
	4	Do you think that when two students fight on the internet, others should stay away from them and not interfere?
Subjective Norms	1	I am expected not to harass any students on the internet, whether during my studies or at any different time.
	2	My friends will not accept any bad behavior that I do related to misusing technology, whether during my studies or afterwards.
	3	I am to respect what cybercrime professionals say and think, especially regarding cyber harassment.
	4	I expect my guardian to prevent me, now and in the future, from committing any form of cyber harassment.
Seeking the Assistance of Society	1	The parents should help in getting rid of cyber harassment crime.
	2	I will ask one of my relatives to assist me to get rid of cyber harassment crime.
	3	I will ask my friends to assist me to get rid of cyber harassment crime.
Mass Media's Influence	1	Do you think that the media is correctly doing its role in increasing the awareness in the community about cyber harassment?
	2	Do you think that the media is correctly doing its role in educating the community about the reasons behind cyber harassment?
	3	Do you think that the media is correctly doing its role in educating the youth about how to combat cyber harassment?
	4	Do you think that the media is correctly doing its role in warning about and explaining the punishments applied upon being involved in cyber harassment?
Perceived Behavior Controls	1	Families are doing their role in increasing the awareness of their children not to give their personal and important information to anyone on the internet so that they don't turn into victims of cyber harassment.
	2	Families are explaining to their children why they shouldn't accept friend requests from strangers on social media websites to protect them from cyber harassment.
	3	The pressure that families apply on their children and their tight supervision may be a reason for cyber harassment.
Regulatory Support	1	I know that there are effective laws against cyber harassment.
	2	I know and understand the effective laws against cyber harassment in my country.
	3	Do you think that publishing statistics and data about cyber harassment would decrease the occurrence of this crime?
Security Awareness	1	Emails are considered good tools for cyber harassment if their users are not aware of signing in securely, such as using a password.
	2	I always lock my computer before I leave it or stop using it.
	3	I don't open emails from unknown senders.
Technology and Social Media Used	1	Rumors on the internet are considered a form of cyber harassment.
	2	The use of bad, insulting, and inappropriate language is considered a form of cyber harassment.
	3	Writing offensive comments on the news on the internet is considered a form of cyber harassment.
	4	Pretending to be another person without that person's approval is considered a form of cyber harassment.
	5	Entering someone's personal page on the internet without their approval is considered a form of cyber harassment.
Engagement in Cyber Harassment	1	I believe that good intentions are a form of worshiping, so I don't think about any unreligious behaviors such as cyber harassment.
	2	What is visible to people should not be different than the intentions, and proper behavior forbids me from committing something as bad as cyber harassment.
	3	I don't intend to get involved in cyber harassment. That is, to save souls and to prevent trauma, hardship, and depression.
Ethical Effects	1	There's a strong relationship between ethics, raising awareness, cyber harassment, and blackmailing.
	2	Ethics help in decreasing or protecting from cyber harassment and blackmailing.
	3	People with high ethics cannot easily become victims to cyber harassment and blackmailing.
	4	Technology usage ethics should be supported by education to protect the students from cyber harassment and blackmailing.
	5	The responsibility of raising technology usage ethics is held by the families and the university in order to help the students in understanding the dangers of cyber harassment and blackmailing.
	6	Ethics could help in educating students and helping them to reveal their cyber harassment and blackmailing problems to their families and/or their educational institutions.

insignificant relationship is between the regulatory support and technology and social media effects. Thus, it is recommended that future research takes the current work as a starting point to explore and investigate more on cyber harassment and its creation. It is recommended that future research builds on the current work and investigates more aspects related to the creation of cyber harassment. Moreover, the influence of technology's and social media's effects can also be the core of future research and exploration. In future studies, other factors related to cyber harassment can be taken into consideration. In the same vein, demographic factors and a more comprehensive sample could be the targets of future attempts. For the participants, research should not be restricted only to students and it is preferred to involve other users, such as instructors and supervisors. For the research design, qualitative approaches represented mainly by interviews should be employed in future works.

ACKNOWLEDGEMENTS

We would like to thank Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia by giving the authors an opportunity to conduct this research.

APPENDIX

See Table 5.

REFERENCES

[1] P. Bocij, *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Westport, CT, USA: Greenwood Publishing Group, 2004.

[2] K. Baum, S. Catalano, M. Rand, and K. Rose, *Stalking Victimization in the United States*. 2009.

[3] J. Avery, "Gender bender brand hijacks and consumer revolt: The porsche cayenne story," in *Consumer Behavior: Human Pursuit of Happiness in the World of Goods*. 2010, pp. 645–649.

[4] K. D. Martin and N. C. Smith, "Commercializing social interaction: The ethics of stealth marketing," *J. Public Policy Marketing*, vol. 27, no. 1, pp. 45–56, 2008.

[5] I. Parker, "The story of a suicide: A gay freshman and the online world," *New Yorker*, 2012.

[6] M. Baer, "Cyberstalking and the Internet landscape we have constructed," Tech. Rep., 2010.

[7] L. P. Sheridan and T. Grant, "Is cyberstalking different?" *Psychol. Crime Law*, vol. 13, no. 6, pp. 627–640, 2007.

[8] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the Internet: The perspective of European children: Full findings and policy implications from the EU kids online survey of 9-16 year olds and their parents in 25 countries," Tech. Rep., 2011, p. 170.

[9] B. Mohamed and E. Elnaim, "Cyber crime in Kingdom of Saudi Arabia: The threat today and the expected future," *Inf. Knowl. Manage.*, vol. 3, no. 12, pp. 14–19, 2013.

[10] A. Horbury. (2013). *Cybercrime-Takes-Its-Toll*. [Online]. Available: https://www.symantec.com/connect/blogs/cybercrime-takes-its-toll

[11] K. Almarhabi, "Adherence to ICT security and privacy policies in Saudi Arabia," *Int. J. Comput. Appl.*, vol. 147, no. 4, pp. 13–18, 2016.

[12] W. M. Al-Rahmi, N. Alias, M. S. Othman, I. A. Ahmed, A. M. Zeki, and A. A. Saged, "Social media use, collaborative learning and students' Academic performance: A systematic literature review of theoretical models," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 20, pp. 5399–5414, 2017.

[13] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "The effect of social media on researchers' academic performance through collaborative learning in Malaysian higher education," *Medit. J. Social Sci.*, vol. 6, no. 4, pp. 193–203, 2015, doi: 10.5901/mjss.2015.v6n4s1p193.

[14] A. AlKaabi, "Strategic framework to minimise information security risks in the UAE," Univ. Bedfordshire, Bedford, U.K., Tech. Rep., 2014.

[15] A. Obaid and S. Alkaabi, "Combating computer crime: An international perspective," Tech. Rep., Oct. 2010.

[16] S. Taylor and P. Todd, "Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions," *Int. J. Res. Marketing*, vol. 12, no. 2, pp. 137–155, 1995.

[17] S. Taylor and P. A. Todd, "Assessing IT usage: The role of prior experience," *Manage. Inf. Syst. Quart.*, vol. 19, no. 4, pp. 561–570, 1995.

[18] M. E. Fishbein and I. Ajzen, *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*, vol. 6. Reading, MA, USA: Addison-Wesley, 1975.

[19] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," *Psychol. Rev. Univ.*, vol. 84, no. 2, pp. 191–215, 1977.

[20] D. R. Compeau and C. A. Higgins, "A social cognitive theory perspective on individual reactions to computing technology," in *Proc. Int. Conf. Inf. Syst.*, 1991, pp. 187–198.

[21] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quart.*, vol. 27, no. 3, pp. 425–478, 2003.

[22] M. Duggan, L. Rainie, A. Smith, C. Funk, A. Lenhart, and M. Madden, "Online harassment," Tech. Rep., 2014.

[23] W. Nasri and L. Charfeddine, "Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior," *J. High Technol. Manage. Res.*, vol. 23, no. 1, pp. 1–14, 2012.

[24] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Social media for collaborative learning and engagement: Adoption framework in higher education institutions in Malaysia," *Medit. J. Social Sci.*, vol. 6, no. 3, pp. 246–252, 2015, doi: 10.5901/mjss.2015.v6n3s1p246.

[25] N. O. Ndubisi, "Factors influencing e-learning adoption intention: Examining the determinant structure of the decomposed theory of planned behaviour constructs," in *Proc. Conf. HERDSA*, Nov. 2004, pp. 252–262.

[26] K. Hamilton and K. M. White, "Extending the theory of planned behavior: The role of self and social influences in predicting adolescent regular moderate-to-vigorous physical activity," *J. Sport Exerc. Psychol.*, vol. 30, no. 1, pp. 56–74, 2008.

[27] A. M. Al-Majali, A. Q. Talafha, M. M. Ababneh, and M. M. Ababneh, "Seroprevalence and risk factors for bovine brucellosis in Jordan," *J. Vet. Sci.*, vol. 10, no. 1, pp. 61–65, 2009.

[28] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Effect of engagement and collaborative learning on satisfaction through the use of social media on Malaysian higher education," *Res. J. Appl. Sci., Eng. Technol.*, vol. 9, no. 12, pp. 1132–1142, 2015.

[29] I. Ajzen, "The theory of planned behavior," *Org. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1991.

[30] E. R. Buhi, H. Clayton, and H. H. Surrency, "Stalking victimization among college women and subsequent help-seeking behaviors," *J. Amer. College Health*, vol. 57, pp. 419–426, Jan. 2009.

[31] J. Zhang, B. J. Reithel, and H. Li, "Impact of perceived technical protection on security behaviors," *Inf. Manage. Comput. Secur.*, vol. 17, no. 4, pp. 330–340, 2009.

[32] R. LaRose, N. J. N. Rifon, and R. Enbody, "Promoting personal responsibility for Internet safety," *Commun. ACM*, vol. 51, no. 3, pp. 71–76, 2008.

[33] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards is security policy compliance," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2007, pp. 1–10.

[34] Y. Li and M. Siponen, "A call for research on home users' information security behaviour," in *Proc. Pacific Asia Conf. Inf. Syst.*, 2011, pp. 1–11.

[35] K. Fang and Y.-Y. Shih, "The use of a decomposed theory of planned behavior to study Internet banking in Taiwan," *Internet Res. Electron. Netw. Appl. Policy*, vol. 14, no. 3, pp. 213–223, 2004.

[36] K. M. Nor and J. M. Pearson, "An exploratory study into the adoption of Internet banking in a developing country: Malaysia," *J. Internet Commerce*, vol. 7, no. 1, pp. 29–73, 2008.

[37] G. S. O'Keeffe, "Clinical report—The impact of social media on children, adolescents, and families," *Pediatrics*, vol. 127, no. 4, pp. 800–804, 2011.

[38] S. Livingstone and D. R. Brake, "On the rapid rise of social networking sites: New findings and policy implications," *Children Soc.*, vol. 24, no. 1, pp. 75–83, 2010.

[39] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Using social media for research: The role of interactivity, collaborative learning, and engagement on the performance of students in Malaysian post-secondary institutes," *Medit. J. Social Sci.*, vol. 6, no. 5, pp. 536–546, 2015, doi: 10.5901/mjss.2015.v6n5s2p536.

[40] W. M. Al-Rahmi, M. S. Othman, and M. Musa, "The improvement of students' Academic performance by using social media through collaborative learning in Malaysian higher education," *Asian Social Sci.*, vol. 10, no. 8, p. 210, 2014, doi: 10.5539/ass.v10n8p210.
[41] *Internet Security Threat Report 2011 Trends*, Symantec, Mountain View, CA, USA, 2012.
[42] R. Broadhurst and L. Y. C. Chang, "Cybercrime in Asia: Trends and challenges," in *Handbook of Asian Criminology*. 2012, pp. 1–26.
[43] B. W. Pudjianto and Z. Hangjung, "Factors affecting e-government assimilation in developing countries," in *Proc. 4th Commun. Policy Res.*, 2009, pp. 1–14.
[44] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 62–72.
[45] W. Hong and K. Zhu, "Migrating to Internet-based e-commerce: Factors affecting e-commerce adoption and migration at the firm level," *Inf. Manage.*, vol. 43, no. 2, pp. 204–221, 2006.
[46] B. L. Ingerman and C. Yang, "Top-ten IT issues, 2011," *Educ. Rev.*, vol. 46, no. 3, pp. 24–26, 2011.
[47] W. Baker *et al.*, "2011 data breach investigations report," Verizon RISK Team Rep., 2011, pp. 1–72.
[48] R. Richardson, "CSI computer crime and security survey," *Comput. Secur. Inst.*, vol. 1, pp. 1–30, Nov. 2008.
[49] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Inf. Manag. Comput. Secur.*, vol. 8, no. 1, pp. 31–41, 2000.
[50] I. Ajzen, "From intentions to actions: A theory of planned behavior," in *Action Control*. Springer, 1985, pp. 11–39.
[51] S. L. Albrecht and K. E. Carpenter, "Attitudes as predictors of behavior versus behavior intentions: A convergence of research traditions," *Sociometry*, vol. 39, no. 1, pp. 1–10, 1976.
[52] P. M. Bentler and G. Speckart, "Models of attitude–behavior relations," *Psychol. Rev.*, vol. 86, no. 5, p. 452, 1979.
[53] S. Weihua, N. Shambare, and J. Wang, "The adoption of Internet banking: An institutional theory perspective," *J. Financial Services Marketing*, vol. 12, no. 4, pp. 272–286, 2008.
[54] K. R. Williams and N. G. Guerra, "Prevalence and predictors of Internet bullying," *J. Adolescent Health*, vol. 41, no. 6, pp. 14–21, 2007.
[55] W. Heirman and M. Walrave, "Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behavior," *Psicothema*, vol. 24, no. 4, pp. 614–620, 2014.
[56] I. Ajzen, "Constructing a TpB questionnaire: Conceptual and methodological considerations," *Time*, pp. 1–13, 2002.
[57] I. Ajzen, "Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior," *J. Appl. Soc. Psychol.*, vol. 32, no. 4, pp. 665–683, 2002.
[58] W. M. Al-Rahmi, A. M. Zeki, N. Alias, and A. A. Saged, "Social media and its impact on Academic performance among University students," *Anthropologist*, vol. 28, nos. 1–2, pp. 52–68, 2017, doi: 10.1080/09720073.2017.1317962.
[59] M. Y. Li, I. Frieze, and C. S.-K. Tang, "Understanding adolescent peer sexual harassment and abuse: Using the theory of planned behavior," *Sexual Abuse*, vol. 22, no. 2, pp. 157–171, 2010.
[60] T. L. Webb and P. Sheeran, "Mechanisms of implementation intention effects: The role of goal intentions, self-efficacy, and accessibility of plan components," *Brit. J. Soc. Psychol.*, vol. 47, pp. 373–395, Sep. 2008.
[61] C. J. Armitage and M. Conner, "Efficacy of the theory of planned behaviour: A meta-analytic review," *Brit. J. Soc. Psychol.*, vol. 40, no. 4, pp. 471–499, 2001.
[62] N. B. Ellison, C. Steinfield, and C. Lampe, "The benefits of Facebook 'friends:' Social capital and college students' use of online social network sites," *J. Comput. Commun.*, vol. 12, no. 4, pp. 1143–1168, 2007.
[63] S. Livingstone, "Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression," *New Media Soc.*, vol. 10, no. 3, pp. 393–411, 2008.
[64] A. Lenhart *et al.*, "Teens, kindness and cruelty on social network sites: How American teens navigate the new world of digital citizenship," Pew Res. Center, Washington, DC, USA, Tech. Rep., 2011, pp. 1–86.
[65] M. O. Lwin, B. Li, and R. P. Ang, "Stop bugging me: An examination of adolescents' protection behavior against online harassment," *J. Adolescence*, vol. 35, no. 1, pp. 31–41, 2012.
[66] J. Wolak, K. J. Mitchell, and D. Finkelhor, "Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts," *J. Adolescent Heal.*, vol. 41, no. 6, pp. S51–S58, 2007.
[67] T. B. Q. Li, "Cyber-harassment: A study of a new method for an old behavior," *J. Educ. Comput. Res.*, vol. 32, no. 3, pp. 265–277, 2005.
[68] W. M. Al-Rahmi and A. M. Zeki, "A model of using social media for collaborative learning to enhance learners' performance on learning," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 29, no. 4, pp. 526–535, Oct. 2017, doi: 10.1016/j.jksuci.2016.09.002.
[69] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "The role of social media for collaborative learning to improve academic performance of students and researchers in Malaysian higher education," *Int. Rev. Res. Open Distrib. Learn.*, vol. 16, no. 4, Nov. 2015.
[70] T. E. Bosch, "Using online social networking for teaching and learning: Facebook use at the University of cape town," *Communication*, vol. 35, no. 2, pp. 185–200, 2009.
[71] E. J. Appel, *Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence*. Boca Raton, FL, USA: CRC Press, 2014.
[72] I. Byrnside, "Six clicks of separation: The legal ramifications of employers using social networking sites to research applicants," *Vand. J. Ent. Tech. L*, vol. 10, p. 445, 2007.
[73] S. Rothberg. (2008). *Do Employers Really Hire Candidates From Facebook and MySpace? FurstPerson/Sprint Does*. Accessed: May 3, 2008. [Online]. Available: http://www.collegerecruiter.com/weblog/2008/04/do_employers_re.php#more
[74] M. F. Plattner, "The global context," *J. Democracy*, vol. 22, no. 4, pp. 5–12, 2011.
[75] G. Hull, H. R. Lipford, and C. Latulipe, "Contextual gaps: Privacy issues on Facebook," *Ethics Inf. Technol.*, vol. 13, no. 4, pp. 289–302, 2011.
[76] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *Proc. WWW*, 2009, pp. 551–560.
[77] J. Peluchette and K. Karl, "Examining students' intended image Facebook: 'What were they thinking?!'" *J. Educ. Bus.*, vol. 85, no. 1, pp. 30–37, 2009.
[78] H. Haron and F. B. M. Yusof, "Cyber stalking: The social impact of social networking technology," in *Proc. Int. Conf. Educ. Manage. Technol.*, Nov. 2010, pp. 237–241.
[79] S. Hinduja and J. W. Patchin, "Bullying, cyberbullying, and suicide," *Arch. Suicide Res.*, vol. 14, no. 3, pp. 206–221, 2010.
[80] F. A. Moafa, K. Ahmed, W. M. Al-Rahmi, N. Alias, and M. A. Obaid, "Factors for minimizing cyber harassment among University students: Case study in kingdom of Saudi Arabia (KSA)," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 6, pp. 1606–1618, 2018.
[81] F. A. Moafa, K. Ahmed, W. M. Al-Rahmi, N. Yahaya, Y. Kamin, and M. M. Alamri, "Cyber harassment prevention through user behavior analysis online in kingdom of Saudi Arabia (KSA)," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 6, pp. 1732–1746, 2018.
[82] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "The effectiveness of using e-learning in Malaysian higher education: A case study Universiti Teknologi Malaysia," *Medit. J. Soc. Sci.*, vol. 6, no. 5, pp. 625–637, 2015, doi: 10.5901/mjss.2015.v6n5s2p625.
[83] L. Kohlberg, "The cognitive-developmental approach to moral education," *Phi Delta Kappan*, vol. 56, no. 10, pp. 670–677, 1975.
[84] L. Floridi and J. W. Sanders, "Mapping the foundationalist debate in computer ethics," *Ethics Inf. Technol.*, vol. 4, no. 1, pp. 1–9, 2002.
[85] R. V. Krejcie and D. W. Morgan, "Determining sample size for research activities," *Educ. Psychol. Meas.*, vol. 30, no. 3, pp. 607–610, 1970, doi: 10.1177/001316447003000308.
[86] Y.-S. Wang, "Assessment of learner satisfaction with asynchronous electronic learning systems," *Inf. Manage.*, vol. 41, pp. 75–86, Oct. 2003.
[87] S. S. Liaw, "Understanding computers and the Internet as a work assisted tool," *Comput. Hum. Behav.*, vol. 23, no. 1, pp. 399–414, 2007.
[88] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Exploring the factors that affect student satisfaction through using e-learning in Malaysian higher education institutions," *Medit. J. Social Sci.*, vol. 6, no. 4, pp. 299–310, 2015.
[89] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," *J. Marketing Theory Pract.*, vol. 18, no. 2, pp. 139–152, 2010.

[90] M. Chow, D. K. Herold, T.-M. Choo, and K. Chan, "Extending the technology acceptance model to explore the intention to use second life for enhancing healthcare education," *Comput. Educ.*, vol. 59, no. 4, pp. 1136–1144, 2012.
[91] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Marketing Res.*, vol. 18, no. 1, pp. 39–50, 1981.
[92] W. M. Al-Rahmi, N. Alias, M. S. Othman, V. I. Marin, and G. Tur, "A model of factors affecting learning performance through the use of social media in Malaysian higher education," *Comput. Educ.*, vol. 121, pp. 59–72, Jun. 2018.
[93] W. M. Al-Rahmi *et al.*, "Use of e-learning by University students in Malaysian higher educational institutions: A case in Universiti Teknologi Malaysia," *IEEE Access*, vol. 6, pp. 14268–14276, 2018.
[94] T. Kaya and H. Bicen, "The effects of social media on students' behaviors; Facebook as a case study," *Comput. Hum. Behav.*, vol. 59, pp. 374–379, Jun. 2016.

FAHAD ABDULLAH MOAFA received the B.Sc. degree from King Abdul-Aziz University and the M.Sc. degree from Cairo University. He is currently pursuing the Ph.D. degree with the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia. He was a Lecturer of information science with the King Fahd Naval Academy, Saudi Arabia.

KAMSURIAH AHMAD received the B.Sc. degree from Flinders University, the STM degree from UK Malaysia, and the Ph.D. degree from UPM Malaysia. She is currently the Head of the Center for Software Technology and Management, Strategic Information System Research Group, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia. She is also an Associate Professor.

WALEED MUGAHED AL-RAHMI received the Ph.D. degree from the Faculty of Computing–Information Systems, Universiti Teknologi Malaysia. He has teaching experience with the Department of Computer Science, Hodeidah University, for eight years. He was a Teaching Assistant with the Faculty of Computing, Universiti Teknologi Malaysia, for 2.5 years. He held a post-doctoral position with the Faculty of Information and Communication Technology, International Islamic University Malaysia. He currently holds a post-doctoral position with the Faculty of Science, Universiti Teknologi Malaysia. His research interests are information system management, human–computer interaction, implementation process, impact of social media networks, collaborative learning, e-learning, knowledge management, massive open online course, and statistical data analysis (IBM SPSS, AMOS, NVIVO, and SmartPLS). He received the Best Student Award, excellent academic achievement in conjunction with the 56nd Convocation Ceremony, from the Universiti Teknologi Malaysia, in 2016.

NORAFFANDY YAHAYA is currently an Associate Professor with the Department of Educational Science, Mathematics and Creative Multimedia, Faculty of Education, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.

YUSRI BIN KAMIN is currently an Associate Professor with the Department of Technical and Engineering Education, Faculty of Education, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.

MAHDI M. ALAMRI received the B.A. degree from King Saud University, Saudi Arabia, the M.Sc. degree from King Faisal University, Saudi Arabia, the master's degree in educational technology in Saudi Arabia, and the Ph.D. degree from the Education Faculty, La Trobe University, Australia. He is currently an Assistant Professor with the Educational Technology Department and the Vice Dean of Scientific Research Deanship, King Faisal University. He is interested in blended learning, online learning, and special education programmers.