Psychometric Properties of a Digital Citizenship Questionnaire

Mohamad Sahari Nordin¹, Tunku Badariah Tunku Ahmad¹, Ainol Madziah Zubairi¹, Nik Ahmad Hisham Ismail¹, Abdul Hamid Abdul Rahman², Fuad A. A. Trayek¹ & Mohd Burhan Ibrahim¹

¹ Faculty of Education, International Islamic University Malaysia, Malaysia
² Prestariang Systems Sdn. Bhd., Lingkaran Cyber Point Barat, Selangor, Malaysia

Correspondence: Tunku Badariah Tunku Ahmad, Faculty of Education, International Islamic University Malaysia, Jalan Gombak, Kuala Lumpur, 53100 Malaysia. Tel: 603-6196-5380. E-mail: tbadariah@iium.edu.my

Received: August 30, 2015   Accepted: September 30, 2015   Online Published: February 24, 2016

doi:10.5539/ies.v9n3p71 URL: http://dx.doi.org/10.5539/ies.v9n3p71

Abstract

The purpose of this study was twofold, i.e. to examine the extent to which students’ self-reported use of digital technology constituted meaningful and interpretable dimensions of the digital citizenship construct, and to test the adequacy of the construct in terms of its reliability, convergent validity, discriminant validity, and measurement equivalence for male and female students. The sample consisted of 391 undergraduates from 15 institutions of higher education in Malaysia. The data were collected using a self-reported 17-item questionnaire measuring university students’ digital citizenship behaviours. The results of the study supported and extended the results of previous work on students’ behaviors when using digital technology. The study found evidence that students’ digital citizenship is a valid and reliable multidimensional construct, and the measurement is gender-invariant. The findings are useful in making evidence-informed decisions in choosing and developing instructional interventions to produce ethical and responsible technology users, and in informing future research in the area.

Keywords: digital citizenship, ethical use of technology, digital etiquette, confirmatory factor analysis, structural equation modeling, confirmatory factor analysis

1. Introduction

1.1 Digital Citizenship

Digital citizenship refers to “the norms of [acceptable] behavior with regard to technology use” (ISTE, 2011, p. 2). It is a rising concern among educators as digital technology and the Internet pervade every aspect of students’ lives. Recent research shows that students are becoming increasingly reliant on digital gadgets and Web-based applications for learning and communicating. According to a 2012 survey involving 500 higher education students, 73% could not study without digital technology; 91% used email to communicate with professors; 74% used digital content; 72% utilized learning management systems; 70% took lecture notes using digital pens and tablets; 65% used digital devices to create class presentations; 55% made use of smart phones; and 53% recorded their lectures (CourseSmart, 2011). A majority were reported to use social media (e.g. Facebook, Twitter and Instagram) on a daily basis (Gosper, Malfroy, McKenzie, & Rankine, 2011). Henderson, Selwyn, Finger and Aston (2015) aptly summarize that digital devices and applications are now central to the ways in which students experience their lives and studies at the university.

At the other end of the spectrum, students’ growing use of and dependence on digital technology have led to myriad abuses and misuses. Occurrences of cyber bullying (e.g. Selkie, Kota, Chan, & Moreno, 2015; Donegan, 2012), sexting (e.g. Perkins, Becker, Tehee, & Mackelprang, 2014; D’Antona, Kevorkian, & Russom, 2010), texting during lectures (e.g. Fried, 2008), and Internet plagiarism (e.g. Smith, 2013) are common among college and university students. With digital technology and the Internet playing such a central role in university learning and in students’ lives, and with the likelihood of abuse and misuse hovering in the background, teaching students digital citizenship becomes foundational and non-negotiable (Hudani, 2014).

1.2 Characteristics of Ethical Digital Citizens

Ribble et al. (2004) developed a 9-dimension framework that is useful to teachers in assessing and helping students to use digital technology appropriately and responsibly. The framework also serves as an informative
guide to research into students’ use of digital technology as it facilitates the identification of researchable issues and concerns within digital citizenship (Isman & Gungoren, 2014). The framework consists of the following interrelated dimensions:

1) **Etiquette**: electronic standards of conduct or procedure;

2) **Commerce**: electronic buying and selling of goods;

3) **Responsibility**: electronic responsibility for actions and deeds;

4) **Safety**: physical safety in a digital technology world;

5) **Security (self-protection)**: electronic precautions to guarantee safety

6) **Rights**: those freedom extended to everyone in a digital world;

7) **Communication**: exchange of information;

8) **Education**: the process of teaching and learning about technology and use of technology;

9) **Access**: full electronic participation in society.

Since digital citizenship is a multidimensional construct, the “topics [of concern] within digital citizenship are wide and varied” (Ribble et al., 2004, p. 7). Thus, particular researchers may focus on specific contents or dimensions in order to add further understanding about the phenomenon. The last four elements (i.e. rights, communication, education, and access), however, primarily are not within the realm of individual students' responsibility. Sincar (2013) indicates that these four components involve higher levels of accountability for technology, which are the concern of policy makers, community leaders, technology leaders, and teachers. Specifically, it is the technology leaders’ duty to formulate rules and policies pertaining to citizens’ rights, accessibility, and electronic exchange of information. Educational leaders and teachers, on the other hand assume the tasks to facilitate the teaching and learning of appropriate use of technology.

As suggested by Ribble et al. (2004), these elements “may be of more concern to technology leaders while others may be of more concern to teachers” (p. 7). Nevertheless, students should be made responsible users of digital technology in many aspects. A good digital citizen is one who acts dutifully in his or her digital community, in that he or she consistently and civily demonstrates normal etiquette as well as responsible, safe, and self-protecting online behaviors (Westheimer & Kahne, 2004). Such a digital citizen is more likely to possess critical literacy and civic responsibility in using digital technology (O’Brien, 2008; Salpeter, 2008). He or she is better-prepared to respond to legal-ethical-moral issues such as cyber-bullying, sexting, intellectual property rights, privacy and protecting of information, unscrupulous electronic commerce, and physical and psychological wellbeing when using technology.

The present study focused on the first five elements of Ribble’s framework as the factors underlying students’ digital citizenship behaviors. Conceptually, these five elements also overlap with many of the behaviors in the other four digital citizenship elements:

**Etiquette**: When online, cultured digital citizens display acceptable etiquette. They observe the customary rules, norms and expectations of the virtual world appropriately, most of which are unwritten (Hollandsworth, Dowdy, & Donovan, 2011; Lenhart & Madden, 2007). Sensible digital citizens communicate and interact politely to the extent that they are likely to state their reasons when disagreeing with something online, do not encourage online fights when they encounter one, and obey mobile phone bans.

**Commerce**: Careful consumers are cognizant of the correct processes for online buying and selling (Mossberger, Tolbert, & Hamilton, 2012). Students are easy preys in online commerce unless they know how to protect themselves from scams and unwarranted debts. Reflective digital citizens are aware of, and protect themselves against the e-predators (Nuccetelli, 2011). To make online purchases, security-concerned customers would “pay attention to currency in use and the total price of the goods and services being paid for” and “note the sellers’ name, address, email, and phone number.” Such preventive behaviors would shield them against identity theft and commercial rip-offs (Ribble, 2011).

**Responsibility**: Law-abiding users of digital technology take responsibility for their online actions and deeds. They know what is right and what is wrong, and what the appropriate and inappropriate behaviors are when engaging in online activities (Curran, 2012; Oxley, 2010). They are also aware of the legal consequences of violating related rules and laws. Hollandsworth et al. (2011) assert that responsible digital citizens are likely to “agree that network administrators have the authority to monitor students’ computer and Internet usage,” “have awareness of copyright infringement,” and “be aware of the AUP (Acceptable Use Policy) of the web.”
Safety: Caring users of digital technology are likely to care about their physical wellbeing (Ohler, 2011) when using computers and digital gadgets. For example, when working on a PC, they are likely to “use an adjustable chair,” “make sure [their] eyes are parallel to the computer screen and keep the computer at a proper distance,” and “make sure [their] forearms are horizontal and wrists are straight.” These are safe ergonomic behaviors (Hollandsworth et al., 2011) that reduce the risks of developing lasting eyestrains, poor postures, pain, numbness and other nerve-related disorders resulting from computer use.

Security (self-protection): Informed users of digital technology exercise electronic precautions to safe-guard their wellbeing (Ribble et al., 2004; Ribble & Bailey, 2005; Ribble, 2011). Such users would likely “install and update antivirus software,” “install and update antispy software,” and “turn on the firewall.” These actions are important in protecting digital information from being stolen or corrupted, in particular those sensitive data which may cost other people’s safety and comfort.

Based on Ribble’s framework and the foregoing assertions on digital citizenship behaviors, we hypothesized that:

H1 Students’ self-reported digital citizenship behaviors consist of five major interrelated factors, which are etiquette, commerce, responsibility, safety, and security.

H2 The five-factor digital citizenship questionnaire is psychometrically sound in terms of reliability, convergent validity, and discriminant validity.

H3 The measurement model is an adequate measure of digital citizenship across gender.

1.3 Statement of the Problem

The literature is replete with information about digital technology use and misuse among students, but there is scanty information on the measurement of students’ digital citizenship behaviors (i.e. the responsible, ethical and safe use of digital technology). Research into digital citizenship is an important one as it would enable university authorities to understand the phenomenon at a deeper, more meaningful level, and thereafter, design curriculum content that befits an instructional intervention to produce digital citizens among their campus populace. Of the limited works on the measurement of digital citizenship behaviors, that of Isman and Gungoren (2014) offers some empirical support for a multidimensional digital citizenship construct. They surveyed digital citizenship behaviors among 229 prospective teachers to examine the underlying dimensions that explained the variability of the undergraduates’ responses to a set of 34 digital citizenship items. The results substantiated the likelihood of a valid and reliable 9-factor structure of digital citizenship. Thus, it is imperative to expand the effort to construct-validate of the measure of digital citizenship.

1.4 Purpose of the Study

This research was thus framed within the notion that the measurement of digital citizenship is an important underpinning of the construct, an essential antecedent to knowledge expansion in the area, and to the formulation of fitting intervention strategies for the inculcation of digital citizenship among university students. Given its importance, ample research should be directed into exploring and validating the quality of the instrument that measures digital citizenship behaviors. Set within this framework, the primary goal of the present study was to construct-validate the factor structure of the questionnaire that measures digital citizenship behavior. In other words, the study primarily aimed to establish whether students’ self-reported use of digital technology constituted meaningful and interpretable dimensions of digital citizenship. Secondly, the study aimed to examine the adequacy of the construct in terms of its reliability, convergent validity, and discriminant validity. Finally, the study sought to provide evidence of the measurement equivalence for the male and female samples involved, which could support the prospect of a gender-invariant measure, and hence, the efficacy of the newly developed digital citizenship questionnaire.

2. Method

2.1 Sample

The sample consisted of 391 undergraduate students from 15 higher education institutions in Malaysia, with female students making up about 73%. The sample was representative of the gender composition commonly found in Malaysian universities. A large majority (80%) were degree seeking students, while the remaining 20% comprised polytechnic undergraduates. The sample size was deemed adequate to address the research objectives (Byrne, 2010; Kline, 2011) and to fulfil the requirements for running a confirmatory factor analysis (CFA).

2.2 Instrument

To collect the data, we used a self-reported 17-item questionnaire measuring university students’ digital
citizenship behaviors. The items were primarily drawn from an extensive review of literature on digital citizenship, especially from the work of Mike Ribble and his colleagues (Ribble, Bailey, & Ross, 2004; Ribble & Bailey, 2007; Ribble, 2011). The items were first content-validated by experts prior to being selected for the present study. The ordering of the items in the questionnaire was in keeping with the expectation that they are indicators of the five sub-constructs of digital citizenship, namely digital etiquette (3 items), digital commerce (3 items), digital responsibility (4 items), digital wellbeing/safety (3 items), and digital security (4 items). Students self-rated their digital behaviors on 5 response categories, i.e. “Never,” “Once in a While,” “Sometimes,” “Frequently” and “All the Time.”

2.3 Procedures of Data Analysis

The study first tested two measurement models of digital citizenship: a one-factor model and a five-factor model. The five-factor model was tested to establish the adequacy of the hypothesized measurement model, while the one-factor confirmatory factor analysis aimed to validate the multidimensional nature of the construct. The expected multidimensionality of digital citizenship measure is compromised if the one-factor model yielded better fit, while a superior one-factor model would undermine the credibility of a multidimensional digital citizenship questionnaire (Bentler & Bonett, 1980; Hoyle & Panter, 1995). Hence, the procedure undertaken addressed the issue of common method bias, an apparent effect of using a single questionnaire to collect and analyze self-reported data of what is supposed to be independent, albeit related, constructs (Podsakoff, MacKenzie, & Podsakoff, 2003). An ill-fitting one-factor CFA of digital citizenship suggests the lack of threats of common method bias, which would enhance the quality of the results.

A CFA using the AMOS (version 20) model-fitting program was applied to validate the two measurement models of digital citizenship. The models were estimated on the basis of the covariance matrix derived from the data. The maximum likelihood estimation procedure was adopted to produce estimates of defensible properties. Preliminary analysis indicated that the assumption of univariate normality was tenable (Byrne, 2010; Kline, 2011). Second, the adequacy of each model was assessed using the widely used standards for a good-fit CFA, which are the: (i) consistency of the measurement model with the data, and (ii) reasonableness of the parameter estimates. The analysis used the relative chi-square ($\chi^2/df$), CFI (comparative fit index), and RMSEA (root mean square error of approximation) as the fit indexes. Arbuckle and Wothke (1995) suggest that the CMIN/df with a value of between 2 and 5 is considered acceptable, while a CFI value close to 1 demonstrates a good fit. Finally, a value of RMSEA of .06 or less shows a reasonable error of estimation.

Third, the study examined the psychometric properties of the models by assessing the components of construct validity, which are convergent validity and discriminant validity. The internal consistency of each sub-construct was measured through composite reliability and Cronbach’s alpha. Finally, a multigroup analysis was conducted to ascertain that the digital citizenship questionnaire is gender-invariant. To test a gender-invariant measure, a two-step simultaneous analysis on both the male (n1 = 104) and female (n2 = 287) groups was conducted, first without constraining the factor loadings, intercepts, residual errors; the results derived a baseline Chi-square value. Second, all loadings, intercepts and residual errors were constrained to be equal in the two samples (Wu, Li, & Zumbo, 2007).

3. Results

Table 1 shows the descriptive statistics of the items included in the confirmatory analysis. The maximum possible score for each item is 4; the mean score of all items distributed above the hypothetical mean of 2.0. The value of each Cronbach’s alpha, which is the internal consistency index of the responses to the related items was reasonably high. The minimum value of the reliability index was .79, and it exceeded the critical cut-score of .70 for a reliable measure.
Table 1. Digital citizenship dimensions and item statistics

<table>
<thead>
<tr>
<th>Code</th>
<th>Dimension/Sub-Construct</th>
<th>Mean</th>
<th>SD</th>
<th>Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>etq1</td>
<td>I state my reasons when I disagree with something.</td>
<td>2.74</td>
<td>.89</td>
<td>.79</td>
</tr>
<tr>
<td>etq2</td>
<td>I don’t encourage online fights even if I encounter one.</td>
<td>2.76</td>
<td>1.06</td>
<td></td>
</tr>
<tr>
<td>etq3</td>
<td>I obey mobile phone bans.</td>
<td>2.56</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>r1</td>
<td>I agree that network administrators have the authority to monitor computer and Internet usage.</td>
<td>2.87</td>
<td>.90</td>
<td>.84</td>
</tr>
<tr>
<td>r2</td>
<td>I use the computer within the timeline given by the instructor.</td>
<td>2.80</td>
<td>.89</td>
<td></td>
</tr>
<tr>
<td>r3</td>
<td>I am aware of copyright infringement.</td>
<td>2.75</td>
<td>.98</td>
<td></td>
</tr>
<tr>
<td>r4</td>
<td>I am aware of the AUP (Acceptable Use Policy) of the web</td>
<td>2.69</td>
<td>.98</td>
<td></td>
</tr>
<tr>
<td>h1</td>
<td>I use a footrest and an adjustable chair that supports my back when working on a computer.</td>
<td>2.70</td>
<td>.99</td>
<td>.84</td>
</tr>
<tr>
<td>h2</td>
<td>I make sure my eyes are parallel to the computer screen and keep them at a proper distance from the screen.</td>
<td>2.87</td>
<td>.91</td>
<td></td>
</tr>
<tr>
<td>h3</td>
<td>I place my keyboard properly and make sure my forearms are horizontal and my wrists are straight.</td>
<td>2.67</td>
<td>.97</td>
<td></td>
</tr>
<tr>
<td>c1</td>
<td>When shopping online, I pay attention to the currency in use and the total price of the goods and services being paid for.</td>
<td>2.97</td>
<td>.90</td>
<td>.80</td>
</tr>
<tr>
<td>c2</td>
<td>I noted the sellers’ name, address, e-mail and phone number.</td>
<td>2.80</td>
<td>.97</td>
<td></td>
</tr>
<tr>
<td>c3</td>
<td>I make sure that I get a copy of the transaction.</td>
<td>2.99</td>
<td>.94</td>
<td></td>
</tr>
<tr>
<td>sc1</td>
<td>I update the browser on my PC.</td>
<td>2.68</td>
<td>1.04</td>
<td>.86</td>
</tr>
<tr>
<td>sc2</td>
<td>I install and update the antivirus software on my PC.</td>
<td>2.97</td>
<td>.99</td>
<td></td>
</tr>
<tr>
<td>sc3</td>
<td>I install and update the antispy software on my PC.</td>
<td>2.71</td>
<td>1.17</td>
<td></td>
</tr>
<tr>
<td>sc4</td>
<td>I turn on the firewall on my PC.</td>
<td>2.74</td>
<td>1.13</td>
<td></td>
</tr>
</tbody>
</table>

3.1 Validity of Multidimensional Digital Citizen Questionnaire

To test the validity of the digital citizenship questionnaire, two confirmatory factor analyses (CFAs) were applied on the data. The results of the first CFA indicated that the one-factor structure of digital citizenship was inadequate to represent the data (Figure 1).
The goodness-of-fit of the model fell short of the minimum standards deemed critical for an adequate solution; \( \chi^2/df = 7.42; \) CFI = .78; RMSEA = .128. These statistics suggest that the measurement model of digital citizenship was not consistent with the data. In other words, there was no evidence to support the validity of a common factor that influences the variability of the sample’s responses to the 17-item questionnaire. Furthermore, the lack of fit of the one-factor models means that the common factor bias was not a threat to the quality of the digital citizenship questionnaire. The second CFA, which tested the hypothesized five-factor digital citizenship model yielded the expected results (Figure 2). The measurement model fitted the variance-covariance matrix; \( \chi^2/df= 2.28; \) CFI = .96; RMSEA = .057. The population RMSEA for the digital citizen model distributed between .048 and .067, with 90% confidence. All parameter estimates were substantial and statistically significant; the direction and magnitude of the factor loadings behaved as expected.

Figure 1. Results of one-factor confirmatory factor analysis

Figure 2. Results of five-factor confirmatory factor analysis
3.2 Psychometric Properties of Digital Citizenship Questionnaire

The results provide evidence to support the psychometric properties of the digital citizenship instrument in terms of its convergent validity and discriminant validity (Table 2). The statistics along the diagonal, which register the average amount of variation (AVE) that a construct is able to explain through its indicators, denote the levels of convergent validity of the measurement. Since the value of the AVE of each construct was larger than the threshold of 0.5, each construct showed sufficient property of convergent validity.

In addition, the measure of digital citizenship adequately satisfied the properties of discriminant validity since most of the AVEs were larger than the values of the corresponding shared variances (values above the diagonal). Furthermore, the moderate inter-factor correlations indicated that digital citizenship was a multidimensional construct consisting of distinct but inter-related dimensions. Finally, the data indicated that the composite reliability of each construct ranged between .78 (etiquette) and .86 (security).

Table 2. Inter-factor correlations, shared variance, average variance extracted, and construct reliability among the constructs of digital citizenship behaviors

<table>
<thead>
<tr>
<th>Dimension/Construct</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Etiquette</td>
<td>0.55</td>
<td>0.48</td>
<td>0.32</td>
<td>0.50</td>
<td>0.27</td>
</tr>
<tr>
<td>Responsibility</td>
<td>0.69</td>
<td>0.57</td>
<td>0.67</td>
<td>0.61</td>
<td>0.45</td>
</tr>
<tr>
<td>Wellbeing</td>
<td>0.57</td>
<td>0.82</td>
<td>0.66</td>
<td>0.53</td>
<td>0.35</td>
</tr>
<tr>
<td>Commerce</td>
<td>0.71</td>
<td>0.78</td>
<td>0.73</td>
<td>0.57</td>
<td>0.44</td>
</tr>
<tr>
<td>Composite Reliability</td>
<td>0.78</td>
<td>0.84</td>
<td>0.85</td>
<td>0.80</td>
<td>0.86</td>
</tr>
</tbody>
</table>

Note. Shown diagonally are the average variance extracted (AVEs) of each sub-construct; below the diagonal is the correlation matrix; above the diagonal is the shared variance matrix.

3.3 Gender-Invariant of Digital Citizenship

Another objective of this study was to examine the factorial invariance of digital citizenship across gender. The estimation of the constrained measurement model produced another Chi-square value, which was then tested against the baseline value for statistically significant differences. Finally, the change in the CFIs and the value of RMSEA of the restricted model were verified against the cutscores of .001 and .05, respectively (Cheung & Rensvold, 2002).

Table 3. Results of the gender-invariant analysis

<table>
<thead>
<tr>
<th></th>
<th>Unconstrained</th>
<th>Constrained</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-Square</td>
<td>422</td>
<td>456</td>
<td>34</td>
</tr>
<tr>
<td>Degree of freedom</td>
<td>218</td>
<td>249</td>
<td>31</td>
</tr>
<tr>
<td>CFI</td>
<td>.943</td>
<td>.943</td>
<td>.000</td>
</tr>
<tr>
<td>RMSEA</td>
<td>.049</td>
<td>.046</td>
<td>.003</td>
</tr>
</tbody>
</table>

The invariance test across the male and female groups resulted in a statistically insignificant change in the Chi-square value, Chi-square (df = 31) = 34, p > .005 (Table 3). In other words, the increase in the Chi-square values from the unrestricted model to the constrained model did not produce a poorer model. Furthermore, while the restricted model maintained the value of CFI at .943, the value of RMSEA was changed by merely .003.

4. Discussion

The study supported the results of previous work on students’ use of digital technology and extended current understanding about the digital citizenship construct in several ways. First, the study offers additional evidence that digital citizenship is in fact a multidimensional construct. The results suggest that the measurement model of digital citizenship did generate the covariance matrix, in that it was consistent with the data. In sum, the CFA results offer evidence that supported the multifactor nature of students’ self-reported digital citizenship behavior.
The citizenship structure comprises five dimensions, namely etiquette, commerce, responsibility, safety, and security. Thus, it is justifiable to use the five-dimension questionnaire to systematically measure students’ digital citizenship behaviors when using digital technology. The CFAs of the two measurement models found the absence of the threat of common method bias since the one-factor solution failed to fit the data; the five-factor structure adequately represented the observed data (Podsakoff et al., 2003). These dimensions are in keeping with the prevailing digital citizenship framework (Ribble & Bailey, 2007; Isman & Gungoren, 2014). Unlike Isman and Gungoren’s work, however, the present study focused on digital citizenship behaviors which are within the realm of individual students’ responsibility, thus involving only five of the nine components of Ribble et al. (2004) digital citizenship framework.

The second objective of this study was to assess the reliability and validity of the five digital citizenship dimensions. The scores from each dimension showed sufficient levels of internal consistency. The analysis showed the reliability indexes to range between $\alpha = .79$ (etiquette) and $\alpha = .86$ (security). Interestingly, Isman and Gungoren (2014) found similar pattern of reliability. The data of the present study also supported the convergent validity and discriminant validity of the digital citizenship questionnaire. The AVE of each dimension exceeded the threshold of importance and moderate inter-correlations among the sub-constructs of digital citizenship. The current study was able to demonstrate that the 17-item questionnaire functions well in measuring students’ responses to digital citizenship behaviors. It is reasonable to conclude that the questionnaire satisfactorily explained the meaning and variability of a five-dimension digital citizenship behavior among students of higher education institutions.

Thirdly, the study addressed the validity of responses across gender. The results of multiple group CFA indicated that measurement of digital citizenship behavior did not systematically vary between males and females. These results suggest that the measure of digital citizenship is configurally and metrically valid on the basis of the results of strict invariant analysis, in that the measure did not vary significantly across gender. It is justifiable then to conclude that gender was not a moderating variable; it did not interact with the underlying dimensions to influence students’ responses to the digital citizenship questionnaire. Regardless of gender, students with similar true scores will indicate the same observed responses (Wu et al., 2007). The study had provided evidence of strong invariance of the questionnaire. The finding suggests that the measurement of digital citizenship behavior is applicable to both male and female students, especially since the gender gap in the use of digital technology among male and female users has been found insubstantial (Ahmad et al., 2010).

5. Conclusion and Recommendations
One of the practical contributions of the study to educational practice is the usefulness of the brief 17-tem digital citizenship questionnaire. It is an adequate tool to assess students’ use of digital technology. Policy makers, community leaders, technology leaders, and teachers should use the instrument to diagnose and evaluate the degree to which students are behaving responsibly, safely, and ethically online. In particular, the examination of students’ self-reported responses to three of the dimensions, namely etiquette, responsibility and security, would help teachers and educators to help students to function as good digital citizens. These seem to be the most relevant dimensions of digital citizenship behavior which would determine students’ appropriate use or misuse of digital technology. The use of the current questionnaire is promising in terms of facilitating future research, and helping educators and teachers plan prevention and treatment programs.

The results notwithstanding, the study is limited in several important matters. First, it did not cover the whole spectrum of online behaviors, which collectively are a function of the constantly evolving digital technology. As time passes by, the validated questionnaire may contain dated indicators of digital citizenship. For example, one may find some items in the security dimension irrelevant as new security features are added to smart phones, tablets, and laptops. Therefore, periodic content-validation of questionnaire is warranted. Second, the sample of the study was a group of homogenous students who were undertaking post-secondary education in Malaysia. The results may differ with users of technology from different populations and cultures. Future studies involving varied student samples may offer useful insights on the comparability of the instrument across age group and culture. Finally, the study did not address the likely causal link between digital citizenship behaviors and misuse and abuse of computer technology, in light of the multifactor nature of digital citizenship. This concern warrants a systematic examination, the results of which may enable the inculcation and teaching of digital citizenship to be improved.

In conclusion, the study has instilled further understanding about the meaning and nature of students’ digital citizenship. The data generated from the study are very useful in informing ongoing efforts in planning and conducting instructional intervention towards producing digital citizens among students. Such efforts are
warranted to help students to develop the attributes of safe, responsible, and ethical users of digital technology.

References


Mossberger, K., Tolbert, C. J., & Hamilton, A. (2012). Broadband adoption| measuring digital citizenship:


**Copyrights**

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).