Towards an Evaluation of Cyber Risks and Identity Information Sharing Practices in e-Learning, Social Networking, and Mobile Texting Apps

Yair Levy
Nova Southeastern University, USA
levyy@nova.edu

Michelle M. Ramim
Middle Georgia State University, USA
michelle.ramim@mga.edu

Abstract

With the growing dependency for online connectivity, the use of Information and Communication Technologies (ICTs) to share identity information surged substantially. Students are constantly sharing where they go, how they feel, and even pieces of identity information such as their age, address, personal pictures, etc. Pieces of identity information are bits of information that, if combined, provide a larger picture of the identity of an individual. Such identity information may enable criminals to obtain financial benefits under the victims' identity, or be utilized for stalking, bulling, or other harassments. The use of different ICTs such as mobile texting, social networking, and e-learning among students, while most of them are not aware that their digital communication is not encrypted, exposes them to increased risk of identity theft. Given that students spend majority of their connectivity time with school related contacts, the focus of this exploratory study is to measure if there are significant differences on the frequency of identity information pieces they share, who do they willing to allow access to their personal profiles, and what is the level of identity protection risks they report compared between three ICTs (e-learning systems, social networking sites, & mobile texting apps). Preliminary results and discussions are provided.

Keywords: Student risks in cybersecurity, identity information sharing, risk in online learning, risk in social networking, risk in mobile texting, risk of identity theft

Introduction

Identity theft is one of the most growing crimes in the 21st century with one million individuals victimized daily, most are not even aware that their identity was stolen (Verizon, 2015). The central focus of this exploratory study is to assess if there are significant differences on the frequency of identity information that high-school and university students share when using e-learning systems, social networking sites, and mobile texting. Moreover, we assess students' disclosure about whom they are willing to allow access to their personal profile on all three Information and Communication Technologies (ICTs), along with their reported identity protection risk level. Sharing personal information over ICTs increases significantly the risk of identity theft. Identity theft is defined as "the illegal and unauthorized acquisition of personal identity in order to engage in unlawful acts" (Shareef & Kumar, 2012, p. 30). There are two main ways at which cyber criminals are obtaining personal identifiable information (PII) for the purpose of identity theft (Hong, 2014). The first is via cyber breaches, where criminals use the Internet to gain illegal and unauthorized access to servers and obtain employees', customers', or other patrons' PIIs (Hovav & Gray, 2014). Such cyber breaches have been documented in recent years with substantial increase in frequency and losses resulting from it (IBM, 2015). The second method used is by "tapping" on non-encrypted communication where sharing of PII can be captured. Such threat vector is the focus of this study, especially investigating it in the

context of educational institutions, where students appear to share constantly PIIs without knowing the risks associated with it.

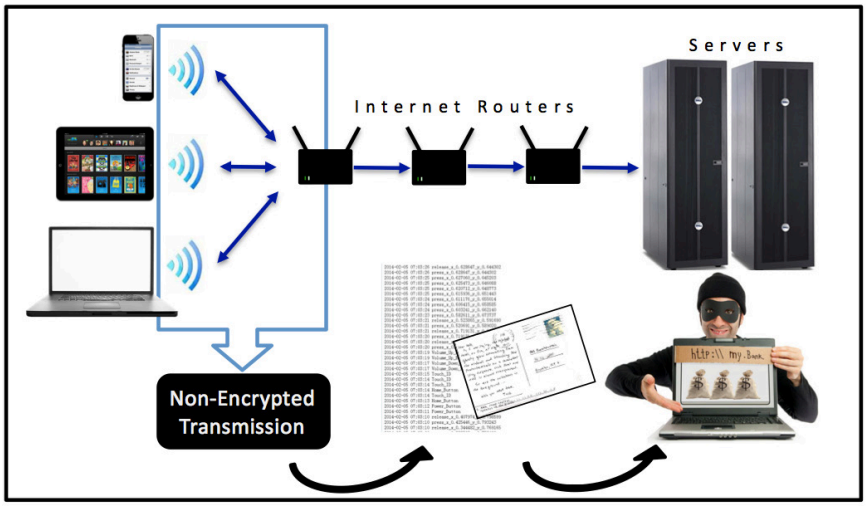

Figure 1. Common Cyber Vulnerability of Identity Information via Non-Encrypted Transmission over WiFi

It appears that there is some underlying cultural and cognitive aspect behind sharing in general, and sharing of information, PII among it, in particular. Specifically, in some cultures where young kids are being constantly reminded of the importance of sharing their toys, belongings, and other items with others, something that usually combines with the age-old phrase of "sharing is caring", which was incorporated into children popular television shows such as 'Sesame Street' (Taylor, 2011). By implanting this cultural and cognitive perspective on sharing, the same young children appear to grow to believe that when they are teenagers and posses a mobile device, tablet, or laptop, it is a positive endeavor to share with everyone they are connected with on social network, mobile texting, and via e-learning systems various personal information. While sharing toys and items is valuable for development of a healthy adolescent who cares for others (Hong, 2014), when it comes to sharing personal identity information, the potential for self-inflicting harm is significant (Ball, Ramim, & Levy, 2015). Specifically, the risk of identity theft is significantly higher when it comes to sharing PII via ICTs, especially via non-encrypted applications. Figure 1 illustrates a typical process at which cyber criminals are using "free" WiFi access points to capture information transmitted via non-encrypted applications. In such typical case, cyber criminals set up a "free" WiFi access point at a coffee shop, airports, schools, universities, or other public locations. They enable "free" connectivity to the Internet and name their WiFi access points similar to the location they are at (i.e. "Free_Starbucks_WiFi", "Free_Airport_WiFi", "Guest_University_WiFi", etc.) deceiving the victims to believe their "free" WiFi access points are legitimate. Once connected, they are able to either implement malware on the victim's device for future identity information capturing, or just "listen" to all communications done by the victim. All non-encrypted communication is equivalent to a postcard, where every individual handling the routers throughout the transmission can see and read whatever information is transmitted. If such communication contains PIIs, the cyber criminals capture the information, and use it for monetization of the information by committing identity theft of the victim. High-school and university students appear to be major consumers of Internet bandwidth, with 97% of them (in the United States (U.S.)) using the Internet on a daily basis, and represent the population that will comprise the workforce in the next few years (Pew Research Center, 2014). They engage in constant digital communication, and are continuously seeking free WiFi, so they are able to connect to the Internet faster, share information, and also reduce their boredom (White & Levy, 2013). Therefore, the three research questions that this study is focused on are:

RQ1: Are there significant differences on the *frequency of identity information* that high-school and university students share between e-learning systems, social networking sites, and mobile texting apps?

RQ2: Who (i.e. friends, family, classmates, & strangers) are high-school and university students *willing to allow access* to their personal profile on e-learning courses, social networking sites, and mobile texting apps?

RQ3: Are high-school and university students aware of the *inherent risks* associated with sharing identity information when using e-learning systems, social networking sites, and mobile texting app?

Methodology

In this exploratory study, we have adopted the approach used by Stutzman (2006) and Carroll (2013) for the assessment of PII sharing in social networking, for the e-learning environment. Our main focus is to empirically assess if there are significant differences on the frequency of PIIs high-school and university students share during e-learning courses, via social networking sites, and mobile texting. Stutzman (2006) assessed the amount of PIIs shared on Facebook™ from 20 undergraduate and 18 graduate students in the eastern U.S. He found that students shared 26 different pieces of PII, were the most shared items were: full name, academic classification, gender, e-mail address, personal picture, birthdate, and hometown. Using a group of five Subject Matter Experts (SMEs), we have provided them the list of PIIs, and asked to evaluate their validity in the context of PII sharing in e-learning courses, via social networking sites, and mobile texting. Table 1 provides an overview of the technologies students in this study experienced as part of the three ICT types.

Table 1: The Three ICT Types and Specific Technology/Website/App Used by Learners

Type	Technology/Website/App
E-Learning Systems	Blackboard, D2L, Edmodo, ReadingPlus, Khan Academy, etc.
Social Networking Sites	Facebook, MySpace, LinkedIn, Google+, etc.
Mobile Texting Apps	iMessage, What'sApp, ChatOn, Facebook Messenger, Viber, Skype, Google+ Hangouts

Following the feedback from the SMEs, we developed a Web-based survey using 24 relevant pieces of PII to be assessed on the 7-Likret scale ranging from (1) 'never' shared, to (7) shared 'every time' used the technology or app (See Section 1 in Appendix A). On the recommendation of the SMEs, we have adjusted the four questions used by Stutzman (2006) that pertains to the group of individuals (i.e. friends, family, classmates, & strangers) that high-school and university students are willing to allow access to their personal profile on e-learning courses, social networking sites, and mobile texting app (See Section 2 in Appendix A). Moreover, we have used the four questions adopted from Stutzman (2006) on assessing the level of identity protection risk that high-school and university students are reporting when using e-learning systems, social networking sites, and mobile texting app (See Section 3 in Appendix A).

Study participant population included high-school and undergraduate university students from several institutions across the southeastern U.S. The 'snowball' approach following Baltar and Brunet (2012) was used in study to collect data by sending the request to complete the Web-based survey instrument to random selection of science department chairs at high-schools in the South Florida region, as well as several instructors of undergraduate courses at the three universities in Florida and Georgia, Therefore, the data collection is still ongoing, however, some interesting results already emerged from the 31 records collected (13 high-school, & 18 university students).

Preliminary Results

A total of 31 survey submissions have been collected so far. Table 2 provides the demographic distribution of the learners participated so far. As noted earlier, and we expect to obtain more data in the next few weeks.

Table 2: Demographics of Study Participants (N=31)

	Frequency (#)	Precentage (%)
Gender		
Female	16	51.6%
Male	15	48.4%
Age		
<14	0	0.0%
14-16	7	22.6%
17-18	6	19.4%
19-24	9	29.0%
25-29	2	6.5%
29-34	7	22.6%
35-39	0	0.0%
40-44	0	0.0%
45-49	0	0.0%
50-54	0	0.0%
55-59	0	0.0%
60+	0	0.0%
Current Academic Level		
Freshman (High-School)	1	3.2%
Sophomore (High-School)	2	6.5%
Junior (High-School)	5	16.1%
Senior (High-School)	5	16.1%
Freshman (College)	3	9.7%
Sophomore (College)	2	6.5%
Junior (College)	6	19.4%
Senior (College)	7	22.6%

In efforts to provide preliminary results in addressing RQ1, we have calculated the mean scores of all the 24 identity information assessed across all the three ICTs. Figure 2 provides the preliminary results. We have observed some interesting differences in the frequency of identity information that students share with some major differences between what is shared via the three ICTs. Specifically, it is interesting to see that identity information such as hometown, birthdate, personal photos, affiliations, sexual orientations, relationships, religions, and favorites (music, books, movies, & TV shows) were self-reported to be shared more on social media and mobile texting, compared with e-learning, although sharing it on all types of ICTs poses the risk of identity theft. Given that we have three groups, a one-way Analysis of Variance (ANOVA) using Statistical Package for Social Sciences (SPSS) (ver. 23) was conducted to compare the means.

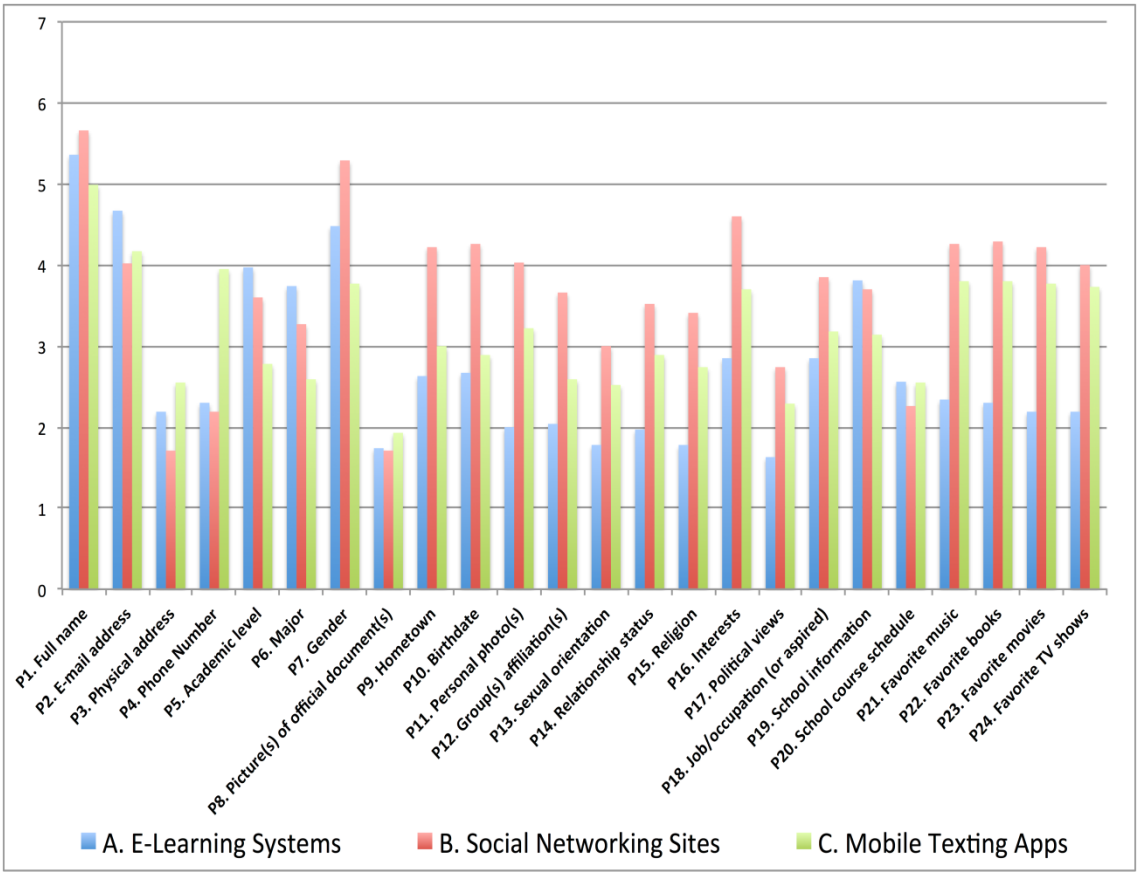

Figure 2. Average frequency of the 24 disclosed pieces of identity information shared via three ICTs assessed (N=31)

In order to focus the preliminary findings, we have selected two separate groups: (a) low sharing - all identity information that were found to have mean below 3.5; and (b) high sharing - all that have a mean of 3.5 or higher. Figure 3 represents the two groups and it is clear that, by and large, identity information is shared much less via e-learning.

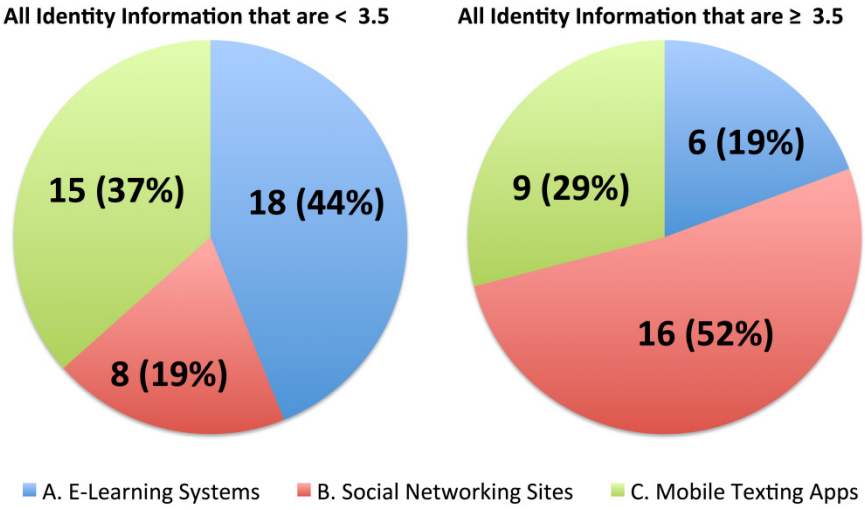

Figure 3. Distribution of number of identity information pieces shared (Low, μ<3.5 & High, μ≥3.5)

Additionally in addressing RQ2, we have asked the participants to disclose if they are OK to share their (A) e-learning system, (B) social networking, or (C) mobile texting personal profile with (1) friends, (2) family, (3) classmates, and (4) strangers. Figure 4 indicates our preliminary results where interestingly students don't perceive classmates as strangers, rather more closely to their friends and family, although some of the classmates they may not know and may even be strangers to them.

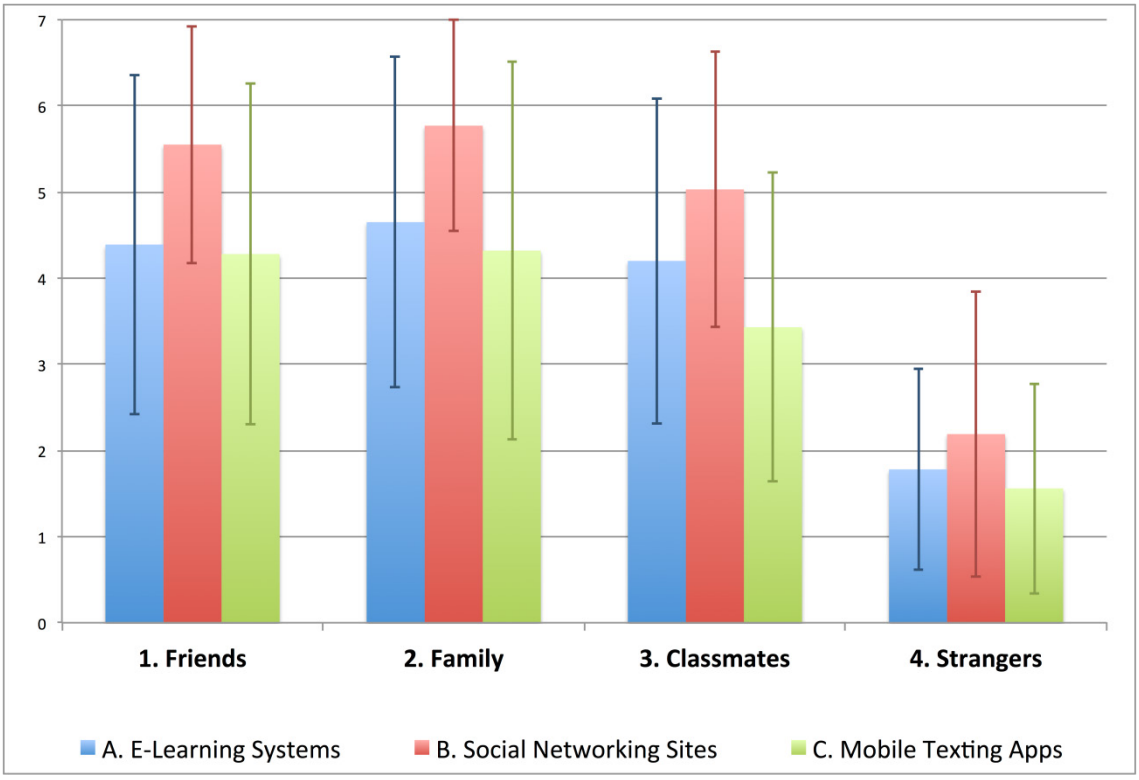

Figure 4. Students' disclosure to whom they are OK to have access to their personal profile per technology

Our preliminary results also provide some indication for addressing RQ3. Figure 5 provides the mean levels of awareness of the *risks* associated with sharing identity information that high-school and university students are reporting when using e-learning systems, social networking sites, and mobile texting app. While it was clear from all prior reporting that students share significant volume of identity information over the Internet, they appear to contradict themselves with a mean score for e-learning systems (M_{ELS}=5.21, $Std.DV_{ELS}$=1.45), Social Networking Sites (M_{SNS}=5.22, $Std.DV_{SNS}$=1.58), and Mobile Texting apps (M_{MTA}=5.37, $Std.DV_{MTA}$=1.60) for indication that they are not likely to share identity information over the three ICTs. Another interesting result is that students appear to consider their identity information more protected in e-learning (M_{ELS}=4.19, SD_{ELS}=1.57) than in social networking (M_{SNS}=3.26, SD_{SNS}=1.87) or mobile texting (M_{MTA}=3.52, SD_{MTA}=1.80), although clearly from previous results they tend to share much more over these two ICTs.

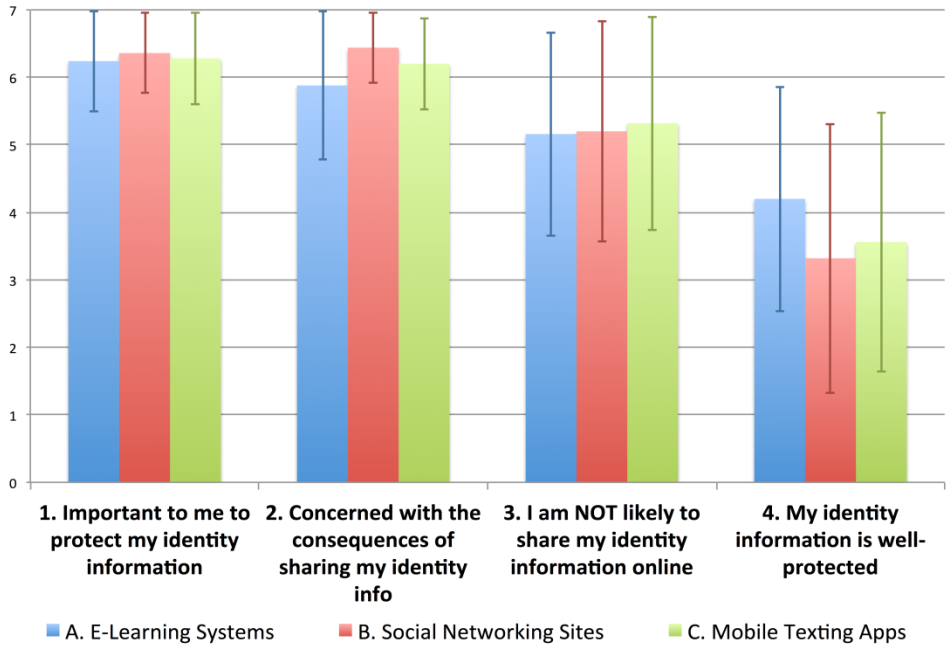

Figure 5. The level of identity protection concerns that students report per technology

Table 3 provides the one-way ANOVA results for all 24 identity information assessed, the declared level of which students willing to allow access to their personal profile, and the awareness level of students on the risks associated with sharing identity information compared across the three ICTs.

Table 3: Mean Scores, Standard Deviation, and One-Way ANOVA Results across all Three ICTs

No.	A. E-Learning System Mean	SD	B. Social Networking Sites Mean	SD	C. Mobile Texting Apps Mean	SD	One-Way ANOVA F	Sig.	
P1	5.36	1.75	5.66	1.75	4.99	2.24	0.95	0.391	
P2	4.67	1.67	4.02	2.11	4.17	2.16	0.89	0.416	
P3	2.19	1.75	1.71	1.41	2.55	1.68	2.12	0.126	
P4	2.30	1.43	2.19	1.46	3.95	2.04	10.82	***0.000***	***
P5	3.97	1.74	3.60	1.79	2.78	1.87	3.53	***0.033***	*
P6	3.74	1.87	3.27	1.80	2.59	1.72	3.20	***0.046***	*
P7	4.48	2.07	5.29	2.06	3.77	2.23	4.00	***0.022***	*
P8	1.74	1.38	1.71	1.61	1.93	1.63	0.19	0.830	
P9	2.63	1.77	4.22	2.02	3.00	1.97	5.83	***0.004***	**
P10	2.67	1.55	4.26	2.04	2.89	1.85	6.92	***0.002***	**
P11	2.00	1.03	4.03	2.01	3.22	2.04	10.49	***0.000***	***
P12	2.04	1.20	3.66	2.08	2.59	1.76	7.15	***0.001***	**
P13	1.78	1.47	3.00	2.18	2.52	2.01	3.22	***0.045***	*
P14	1.97	1.56	3.52	2.09	2.89	2.02	5.20	***0.007***	**
P15	1.78	1.60	3.41	2.16	2.74	1.98	5.58	***0.005***	**
P16	2.85	1.52	4.60	1.94	3.70	2.05	6.88	***0.002***	**
P17	1.63	1.10	2.74	1.71	2.29	1.55	4.45	***0.014***	*
P18	2.85	1.65	3.85	1.77	3.18	1.61	2.85	0.063	
P19	3.81	2.02	3.70	1.88	3.14	1.82	1.12	0.332	
P20	2.56	1.81	2.26	1.71	2.55	1.74	0.29	0.748	
P21	2.34	1.65	4.26	1.74	3.80	2.05	9.37	***0.000***	***
P22	2.30	1.69	4.29	1.84	3.80	2.11	9.34	***0.000***	***
P23	2.19	1.65	4.22	1.83	3.77	2.09	10.10	***0.000***	***
P24	2.19	1.65	4.00	1.75	3.73	2.19	8.38	***0.000***	***
OK1	4.39	1.97	5.55	1.38	4.28	1.98	4.30	***0.016***	*
OK2	4.65	1.92	5.77	1.22	4.32	2.19	4.99	***0.009***	**
OK3	4.20	1.89	5.03	1.60	3.43	1.80	6.33	***0.003***	**
OK4	1.78	1.16	2.19	1.65	1.56	1.22	1.71	0.186	
IDP1	6.22	0.76	6.32	0.65	6.26	0.73	0.09	0.917	
IDP2	5.89	1.10	6.34	0.62	6.19	0.80	1.20	0.305	
IDP3	5.21	1.45	5.22	1.58	5.37	1.60	0.10	0.907	
IDP4	4.19	1.57	3.26	1.87	3.52	1.80	2.30	0.106	

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$

Discussions and Conclusions

In this exploratory research, we are investigating three aspects of identity information sharing as it pertains to risk related to identity theft. The first, relates to the assessment of what identity information do high-school and university students share via e-learning systems, social networking sites, and mobile texting app. The second relates to what type of individual (i.e. friends, family, classmates, & strangers) are students willing to allow access to their personal profile on all three ICTs. Moreover, the third aspect we are assessing, the level of identity protection, concerns that the students are reporting when using the three ICTs. We believe that our study provides novel perspectives on student risks in cyberspace, and contributes to information security theory. Such contribution is significant, as prior research has focused primarily on generic identity information pieces shared over the Internet without specific type of ICT (Lankton, Wilson, & Mao, 2010; Polites, & Karahanna, 2012) or only within social networking sites (Acquisti & Gross, 2006), while our study focused on comparing three different cyber environments that the same individuals are using to share identity information pieces. Our results are interesting as they provide indications that e-learning is somewhat considered different than social networking and mobile texting in the pieces of identity information that students are reporting to disclose, specifically with less items and less frequency. As we continue to collect more data, we will update the results appropriately.

References

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing and privacy on the Facebook. *Privacy Enhancing Technologies, 4528*, 36-58.

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management, 3*(1), 180-207.

Baltar, F., & Brunet, I. (2012). Social research 2.0: Virtual snowball sampling method using Facebook. *Internet Research, 22*(1), 57-74.

Carroll, T. J. (2013). *Perceptions of identity theft in college age individuals*. Masters Thesis, Utica College, New York. (UMI No. 1550258).

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81. doi:10.1145/2063176.2063197

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Associations for Information Systems, 34*(Article 50), 893-912.

IBM Global Technology Services, Managed Security Services. (2015). *IBM security services 2015 cyber security intelligence index*. Retrieved from http://www-03.ibm.com/security/data-breach/2015-cyber-security-index.html

Lankton, M. K., Wilson, E. V., & Mao, E. (2010). Antecedents and determinants of information technology habit. *Information & Management, 47*(6), 300-307.

Pew Research Center (2014). Internet user demographics. Retrieved from http://www.pewinternet.org/data-trend/internet-use/latest-stats/

Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: the inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly, 36*(1), 21-42

Shareef, M. A., & Kumar, V. (2012). Prevent/control identity theft: Impact on trust and consumers' purchase intention in B2C EC. *Information Resources Management Journal, 25*(3), 30-60.

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *International Digital and Media Arts Journal, 3*(1), 10-18.

Taylor, J. (2011). *Your children are listening: Nine messages they need to hear from you*. The Experiment LLC: New York, NY.

Verizon (2015). The 2015 data breach investigations report (DBIR). Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Appendix A. Survey Instrument Items

SECTION 1: INFORMATION SHARING	
No.	Identity Information Piece
P1.	Full name
P2.	E-mail address
P3.	Physical address
P4.	Phone Number
P5.	Academic level
P6.	Major
P7.	Gender
P8.	Picture(s) of official document(s) (Student ID, Driver License, etc)
P9.	Hometown
P10.	Birthdate
P11.	Personal photo(s)
P12.	Group(s) affiliation(s)
P13.	Sexual orientation
P14.	Relationship status
P15.	Religion
P16.	Interests
P17.	Political views
P18.	Job/occupation (or aspired job/occupation)
P19.	School information
P20.	School course schedule
P21.	Favorite music
P22.	Favorite books
P23.	Favorite movies
P24.	Favorite TV shows
SECTION 2: ALLOWING OTHERS TO ACCESS OR SEE YOUR PROFILE	
No.	Item Description
OK1.	I am OK with friends seeing my [e-Learning System/SNS/Mobile Texting app] profile
OK2.	I am OK with family seeing my [e-Learning System/SNS/Mobile Texting app] profile
OK3.	I am OK with classmates seeing my [e-Learning System/SNS/Mobile Texting app] profile
OK4.	I am OK with strangers seeing my [e-Learning System/SNS/Mobile Texting app] profile
SECTION 3: IDENTITY PROTECTION	
No.	Item Description
IDP1.	It is important for me to protect my identity information on [e-Learning Systems/SNS/Mobile Texting app]
IDP2.	I am concerned with the consequences of sharing identity info in [e-Learning Systems/SNS/Mobile Texting app]
IDP3.	I am NOT likely to share my identity information online in the future via [e-Learning Systems/SNS/Mobile Texting app]
IDP4.	I believe my identity information is well-protected in [e-Learning Systems/SNS/Mobile Texting app]