An Analysis on the Perceptions of High School Teachers in Manila, Philippines Towards Student Data Privacy and Its Legal Implications

Juan Carlo Zamora, De La Salle University, The Philippines
Madeleine Tan, De La Salle University, The Philippines
Sharon Albacete, St. Paul University-Manila, The Philippines
Rosemin Canulo, De La Salle University, The Philippines

The Asian Conference on Education 2018
Official Conference Proceedings

Abstract
Information and communication technology (ICT) has been making its way into our lives since the invention of Internet and its applications, including the daily usage of internet social media. In recent years, it has conquered the education industry, providing school administrators and teachers a more challenging, yet effective and practical way of managing school operations. Teachers have been using technology-enhanced data collection and analysis as tools to aid their schools in planning, and implementing personalized, student-centered learning experiences for their students. While there are numerous positive effects, it goes without notice that privacy of students is being sacrificed. The Philippines enacted its privacy law, the Data Privacy Act of 2012 to protect its people from the growing use of data. As the law is relatively new, the researchers investigated the perceptions of high school teachers from public and private schools in Manila, Philippines towards data privacy and its legal implications. The methods used in obtaining the perception of the teachers were through an online survey using convenience sampling. The survey used a Likert scale in asking the perception of the teachers regarding potential lawsuits and data usage activities. Analysis administered for the perception are descriptive statistics, validity and reliability using Cronbach's alpha, and correlation of perception against different demographic profiles. Results show that the perception of the teachers show significance in age group and awareness of the data privacy law.

Keywords: Philippines, Data Privacy, High School

Introduction

Schools of today are making the most out of the use of technology. The prevalence and use of computers, the Internet, and social media are continuously evolving and expanding; and concomitantly so are the legal, ethical, and practical implications in the employment sector and beyond (Cavivo, Majtaba, Muffler, & Samuel, 2013). As of the end of 2017, there were approximately 4.2 billion Internet users around the world, and Asian countries take approximately 2 billion Internet users (Internet World Stats, 2018). According to the National Association of Secondary School Principals (n.d.), school administrators and teachers have been using technology-enhanced data collection and analysis as tools to aid their schools in planning, and implementing personalized, student-centered learning experiences for their students. Though it seems that current technology has made access to data much easier and reliable, there are pitfalls to it and one is the increasing trend of sharing private student information (Bloom and Attai, 2016). This student information not only includes personal demographic information, but also student abilities, strengths and weaknesses, and habits and routines.

The rapid increase in data production and collection in schools have the potential to make students targets of cybercrime; which includes fraud, cyberbullying, and theft. In the past decade, several countries have produced data protection law to protect its citizens. In the Philippines, the 'Data Privacy Act of 2012 (DPA)' is a safeguard enacted by the government to such pitfall. According to the DPA, their main goal is to *"protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth"*. As it is relatively new, this research would like to gather and compare perceptions of teachers from private and public high schools in Manila, Philippines on the act.

In this research paper, the group aims to provide answers an explanationtothefollowing research questions: RQ1. Do teachers know the rights of the students' personal data? RQ2. Do teachers respect and protect the personal data of the students? RQ3. How does the teachers perceive legal threats in their role of data management? These questions inquire about the privacy concerns with the usage of social media and usage of personal data for academic use.

Review of Related Literature

Privacy is a right (MacCarthy, 2014). According to Yang and Wang (2014), it is the *"desire of people to choose freely under what circumstances, and to what extent, they will expose themselves, their attitude, and their behavior to others"*. In other words, a person chooses what information of his could be shared, disclosed, and used. There are rules created on privacy, with consideration to the context, because these *"govern the transmission of information and serve to protect the integrity of the context",* as stated in MacCarthy (2014). With access to information just a click away, how can one be protected?

Data Privacy Systems

Data privacy is a common issue in today's technology-plagued society. Free speech is integrated into different social media platforms. Social media has been consuming

countless minutes of our everyday life and it is one of the primary sources of personal information, such as Facebook and Twitter, especially for the youth (Clemons and Wilson, 2015). An ethical problem revolving around sociology may occur whenever technology companies source data, in which a person may not be fully aware on the usage of their personal human data. User- generated media is rapidly increases and it is impossible for any human to scrutinize all of the data to see which media affects privacy (Smith, Szongott, Henne & Von Voigt ,n.d.). In 2014, an estimate of 2.5 quintillion bytes of data are created each day (Amihan, 2017).

The internet provides its users the opportunity to communicate with people around the globe, research and share information, and conduct podcasts, classes, and videos to name a few; and any of such connection to the internet could potentially be utilized in collecting and/or accessing data (NASSP, n.d.). These modes of communication through the internet transmit the littlest of information that is being uploaded into the web or in other words, whatever is inputted, can be retrieved and used.

Technology-enhanced data collection and analysis have *"the power to transform teaching and learning by helping educators identify and provide supports to all students, assisting teachers and school leaders in improving their instructional practices, and informing schoolwide improvement activities"* (NASSP, n.d.); Furthermore, these data can be used as reference and support in creating activities that can improve the educational system. According to Strauss (2015), most of the student data gathered in schools are through students' online usage or the information provided by teachers, staff, and parents; and this information may be composed of the student's demographics, school and discipline records, disabilities, medical history and records, and Individual Education Plan to name a few.

While having online database systems has its many advantages, it comes with its comparable responsibilities. Schools have collected student data which they had created, used, and stored over the years, through different means; and with this comes the obligation of keeping student information private (Bloom and Attai, 2016).

There have been recent controversies involving such obligation that took down at least two well-known companies namely 23andm3 and inBloom, the latter being a $100-million non-profit corporation backed up by the Bill and Melinda Gates Foundation and Carnegie Corporation of New York (Boyd and Metcalf, 2014). The said corporation's mission is to personalize learning through the collection of student data and store these in a cloud for teachers to be able to track, customize lessons in real time, and share the records with educational tool developers for better and more effective construction of resources (Singer, 2013). However, a few months later, controversies arose which led to the company to shut down for reasons that there are no policies on the security of information and the amassing increase of information about the students that are stored, leading parents, school board members, and privacy lawyers to gravely object (Singer, 2013).

School administrators and teachers have it easier today when it comes to collecting and analyzing data at the school level because of technology (National Association of Secondary School Principals, n.d.). With the benefits and loopholes of online database systems, there must be safeguards to the usage of these data. School administrators must have policies, besides those of the government, to govern who can access

student information, how these should be stored, and what information can only be shared to private companies such as third-party vendors (Singer, 2013). Legal contracts and agreements must be clearly discussed, and the partner vendors are well-aware of the privacy laws on such as well (Bloom and Attai, 2016). As a provider of education, a school has the responsibility to protect its staff, stakeholders, and students, be it in physical form or through information systems, and how these are being managed within its environment (Aston, 2017). They are accountable as to what is being done to the information.

For students, each of them has personal, identifiable information in a school's database, for whatever purpose; and therefore, for their protection, there must be movements towards student data privacy as to present the *"legal and ethical limitations on the collection, use, sharing, and handling of student personal identifiable information"*. (Bloom and Attai, 2016). In our technology-dependent society today, laws must be made to govern such handling of private information.

Free Speech Rights of Teachers

The credibility of teachers is affected by their social media content, in which the perception of the students show that teacher credibility affects whether it is acceptable for a teacher to have Facebook profile (Wang, Z., et. al., 2015). In light of this, teachers are believed to be disciplined whenever students' profiles are being monitored by educators, even when the profile is publicly accessible, since the students have rights over the information posted (Folger, T. S., et. al., 2009). Educational institutions might create strict rules for the use of social media by teachers and students if there is encouragement in the use of social media, whatever the medium. On the other hand, if there is discouragement or banning of the use of social media, the development of their innovative creativity may hinder (Folger, T. S., et. al. 2009).

Legal Implications of the Data Privacy Act of 2012

In the Philippines, with the rapid increase in internet usage, an act was passed to address 21st century crimes, specifically the concern on internet and information. This Act is known to be RA 10173 or otherwise known as the "Data Privacy Act of 2012".

The National Privacy Commission (n.d.) states that the Act *"(1) protects the privacy of individuals while ensuring free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through National Privacy Commission (NPC)"*. It is the country's first comprehensive data protection law.

Based from Nicolas and De Vega Law Offices (2016), *"Data Privacy Act of 2012 protects all forms of information that are personal, private or privileged. It covers all persons, whether natural or juridical, with particular emphasis to companies or juridical entities involved in the processing of protected information",* though it is

worth noting that the law only protects private information, not of which are publicly accessible. Wapp (2017) defines private personal information as being:

- *About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;*
- *About an individual's health, education, genetic or sexual life of a person, or to any proceeding or any offense committed or alleged to have committed;*
- *Issued by government agencies "peculiar" (unique) to an individual, such as social security number;*
- *Marked as classified by executive order or act of Congress.*

When personal, private, or privileged data are to be collected and processed, the purpose must first be specified, legitimate, transparent, legal, and reasonable (Amihan, 2017; Wapp, 2017). Certain circumstances have been identified though as exceptions when it comes to processing of such data and Wapp (2007) stated these:

- *Consent of the data subject;*
- *Pursuant to law that does not require consent;*
- *Necessity to protect life and health of a person;*
- *Necessity for medical treatment;*
- *Necessity to protect the lawful rights of data subjects in court proceedings, legal proceedings, or regulation.*

Second, the consented information can be shared to only the agreed recipient. The information, kept accurate and relevant, must be used only for the stated and agreed upon purposes and kept for as long as reasonably needed (Amihan, 2017). Third parties, most especially, who process personal information must have and utilize contracts or other reasonable means that align with the Act's implementing rules and regulations (IRR) to *"ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and otherwise comply with the law"* (Parsons, M. and Crawford, L., 2016). When unauthorized person has acquired any sensitive personal information or information that may be used to commit identity fraud, the personal information controllers must notify NPC within 72 hours as mandatory breach notification (Parsons, M. and Crawford, L., 2016).

Third, when the personal information is no longer needed, it must be securely discarded. It must not be visible and accessible to unauthorized parties (Amihan, 2017). When handled improperly, the Act states that one is punishable for up to six (6) years in prison or up to five million pesos (PHP 5,000,000), depending on the nature and degree of the violation (Amihan, 2017).

National Privacy Commission

A commission was created to enforce the R.A. 10173 or the Data Privacy Act of 2012. The National Privacy Commission is assigned to check and validate whether companies are compliant with the element stated in the republic act. The five (5) elements, as discussed in Amihan (2017), are:

1. Appointing a Data Protection Officer
2. Conducting a privacy impact assessment
3. Creating a privacy knowledge management program
4. Implementing a privacy and data protection policy
5. Exercising a breach reporting procedure

According to Amihan (2017), the Data Privacy Act of 2012 requires companies with at least 250 employees or have access to personal and identifiable information of at least 1,000 people to register with the National Privacy Commission and comply with the Act. Furthermore, as it is relatively new, many are still unaware that they are affected by the law (Amihan, 2017).

Research Methodology

The survey was developed and pretested on the respondents of private schools and public high schools, also known as government schools, in Manila, Philippines. Participants were collected through convenience sampling, in which the researchers sent survey request through the principals of the schools around Manila. Participants must be currently employed as a teacher full-time teacher in a government accredited school. The survey is voluntary, the teachers from each school were not forced by the principal to answer the survey. Out of 534 survey requests only 44 returned to answer the survey. The personal information gathered through this survey is kept intimate and is treated with utmost respect.

The survey, which consists of 25 questions, inquires about the online behavior of teachers, and perceived legal threats. The composition of the survey consists of 6 questions on demographic, 6 technical data, and 13 questions on perceptions, which are divided into three parts.

The questions on perceptions were initially 25 questions, but were then modified to and reduced to 13 questions. The reason for the decrease in questions is to maintain a good score on the reliability test using Cronbach's alpha. Then, perception questions were divided into three parts. The first two categories of questions about perceptions are adapted from information security and education literature, specifically the survey items related to Privacy Concern for Communication Tools, and Risk and Severity of exposing others were adapted from study of James, T. L. et al (2017) and Dhir (2016). The questions about legal implications are developed by the researchers with the assistance of lawyer specializing in education and working as a full-time professor in a university in the Philippines, and it is also based on the current Philippine laws about data privacy and cybercrime. These questions are on a Likert scale from 1 (Highly Disagree) to 7 (Highly Agree).

Table 1.
Sources of Survey Items

Constructs	Items Adapted From:
Privacy Concern for Communication Tools (PC)	Dhir (2016); James (2017)
Risk and Severity of Exposing Others (RS)	Dhir (2016); James (2017)
Perceived Legal Threats (PL)	Scale Developed by Authors

The framework of this research is based on the hypothesis that if the teachers are not efficient and knowledgeable about technology and data, then they are more likely to perceive threats. The researchers made four hypotheses to answer the research questions. Specifically, the first hypothesis (H1) connects that Privacy Concern of Communication tools is positively associated with Risk and Severity of Exposing Others; second hypothesis (H2) is about Risk and Severity of Exposing Others having a significant influence on Perceived Legal Threat; and lastly the last hypothesis (H3), which answers the main inquiry, is about Perceived Legal Threats have a significant difference between technical aspects and demographic profiles of the teachers.

Using the SPSS as a statistical tool, the researchers tested the measures of central tendency, with mean and standard deviation for the analysis of the Likert scale. Validity, reliability, and discriminant validity were measured for the sub constructs items in the survey.

Results and Discussion

As seen in Table 2, it can be observed that most of the teachers are females. Most of the age group comes from the Millennial generation, which was defined by Dimock (2018). Most of the teachers comes from private institutions. The teaching experience of the teachers range highly from 3-4 years, while the next large population comes from those who have though for more than 5 years. The teachers are taking graduate studies and have taken graduate degree exceeds those who only continue to teach with educational attainment of a bachelor's degree.

From the data, it can be inferred that the teachers are experienced teaching and handling students. Furthermore, the professional qualifications of the teachers relating to education are substantial. For most of the teachers, they have most likely have been exposed to the Data Privacy Act from its conception to its implementation by the time they started their teaching profession.

Table 2.
Demographic Profile of Teachers

Demographics	Category	Frequency (Percentage)
Sex	Male	11 (25)
	Female	33 (75)
Age Group	Generation Z (Born in 1997 – 2012)	2 (4.5)
	Millenials (Born in 1980 – 1996)	38 (86.4)
	Generation X (Born in 1965 – 1980)	4 (9.1)
School Type	Private	34 (77.3)
	Public	10 (22.7)
Undergraduate degree is in Education	Yes	31 (70.4)
	No	13 (29.6)
Highest Educational Attainment	Graduate Degree	12 (27.3)

	Some Master's Units	17 (38.6)
	Undergraduate	15 (34.1)
Years of Teaching	1-2 years	9 (20.5)
	3-4 years	23 (52.3)
	5-10 years	7 (15.9)
	>10 years	5 (11.4)

The questions asked for the technical knowledge of teachers related to the potential data breach of information that the teacher may accidentally release. Teachers could accidentally release students' information without warning, and thus they must be trained for data protection practices (Chou & Chou, 2016; Chou & Chen, 2016). The data Risk of Data Breach shows that there is a potential that the personal data of the students may be stored in a teacher's possession without the approval of the school.

The final count for the technical knowledge of the teachers are presented in Table 3. Majority of the teachers have knowledge about the laws covering data privacy in the Philippines. The researchers believe that if the teachers are knowledgeable in the laws regarding the rights of every person in the Philippines and their perceive legal threats is present in their mindset. This also answers **RQ1**, in which teachers know their rights and the rights of the students. Thus, it cannot be dismissed that the teachers are not apathetic to the laws protecting everyone when it comes to handling sensitive data. **RQ2** can also be answered in the information below, in which the teachers may have shared the data or have kept confidential data that can be potentially distributed. Respecting and protecting the data of the students may differ in definition for each teacher and having the ability to protect these data may also differ in terms of efficiency and use of different instruments.

Table 3.
Technical Knowledge of Teachers

Technical Aspect	Items	Answer	
		Yes	No
Risk of Data Breach	I keep the records of my students in my personal computer	32	12
	I save the records of my students in different tools (Drobox, flashdrive, email, Google drive, etc.)	35	9
	I have access to my students' personal data without signing any consent forms on disclosure	24	20
Knowledge About Philippine Laws	I have at least read basic information in Data Privacy Act of 2012	27	17
	I have at least read basic information in the Cybercrime Prevention Act of 2012	33	11
	I have at least read the Philippine 1987 Constitution	38	6

A good reliability of the Cronbach's alpha is greater than 0.7 (Peterson, 1994). The Cronbach's alpha of all the final survey items were greater than 0.7. As can be seen in Table 4, the survey items show a good indicator of reliability. Additionally, the

average for the PC and RS leans on the agreement that there is a threat to certain behaviors and activities that they perceive to be happening.

Table 4.
Reliability of Survey Items

Item	Cronbach's Alpha	Mean	Std. Dev.
Privacy Concern for Communication Tools (PC)	0.71	5.15	1.28
Risk and Severity of Exposing Others (RS)	0.73	5.43	1.33
Perceived Legal Threats (PL)	0.81	4.32	1.24

The final items in the survey, along with the means and standard deviations of each item are provided in Table 5. For each item in the PC, it can be observed that most of the answers tend to agree with the communication tools have some privacy concerns. As for items in RS, teachers can be seen to agree that their behavior may risk of exposing others. This can be seen to be related to the items in Table 3. As for PL, the perception of teachers is leaning towards being more on the neutral when it comes to their legal threats.

The role of the teachers in answering RQ3, could be initially identified by the results in the individual means of each item under PL. It seems that the teachers perception of legal threats is not high as opposed to the expectations of the researchers, in which it is expected to lean towards the scale of agreement.

Table 5.
Descriptive Statistics of Perception Items

Item Indicator	Item	Mean	Std. Dev.
PC1	Through social media, I can get Information	5.73	1.68
PC2	Through social media, I can share information	5.50	1.52
PC3	Others may experience leaks of personal information because of what I do on social media	4.45	2.19
PC4	If I use social media, it is likely that the personal information of some other people may be posted.	4.82	2.06
PC5	It is possible that other people's personal information may be shared by my use of social media.	4.59	1.85
RS1	If I shared somebody's personal information through social media, it could be harmful for that other person.	6.00	1.75
RS2	It could be unfortunate for a person if his or her personal information was spread by my social media activity.	6.14	1.41
RS3	Posting the grade of my students in a social media group or online education platform is not tolerable	4.42	2.04
PL1	It is acceptable that a teacher loses its license if they were put on trial for data privacy	4.41	2.15
PL2	I am vulnerable to lawsuits for my practice in handling student data	4.41	1.99
PL3	I think that my employer is responsible for potential lawsuits regarding student data, and I may pose as an	5.45	1.45

	accessory to such lawsuits		
PL4	Being unaware to some data privacy definitions makes me worried for my legal safety	3.41	1.74
PL5	I see the Data Privacy Act can harm me in the current situation	4.41	2.15

(7-point Likert scale; 1 = Strongly Disagree to 7 = Strongly Agree)

In testing the three hypotheses, the results of different perceptions together with the technical and demographic data are correlated with each other. The results for the correlation of PC and RS were insignificant ($p>0.05$), thus rejecting H1, which then it can be inferred that the perceived behavior for the privacy concern does not affect the risk and severity of exposing others. The results show that is not similar to the study by James (2017), in which there is a significance for similar items of RS and PC.

As for RS correlating with PL shows that they are positively significant (H2: 0.467; $p<0.01$), in which that there is a reason to believe that there is a legal threat if there is a high risk of exposing others.

Lastly, Table 6 shows significance are age, years of teaching, and have read the Data Privacy Act of 2012. This result is straightforward, in which it can be interpreted that as legal threats may come easily to teachers who have aged more and had taught more throughout years of teaching and work experience. The correlation for reading the data privacy law is set at 1 for those who have answered Yes, thus it can be inferred that those who have read the law about data privacy are much more concerned for legal threats. The results for the significance of some demographics and some technical knowledge does not fully supports the totality of H3. The results could be improved by reinforcing different options in the perceptions on legal threats.

Table 6.
Summarized Results for Correlation

Category	Perceived Legal Threats (PL)	
	Pearson Correlation	Sig. (2-tailed)
Age	0.629	0.000**
Years of Teaching	0.475	0.001**
I have at least read basic information in Data Privacy Act of 2012	0.352	0.019*

*Correlation is significant at: ($p<0.05$); Correlation is significant at **($p<0.01$)

Conclusion and Recommendation

It can be inferred that teachers in this study are more likely to perceive threats if they are aware of the potential lawsuits applicable to them based on their behavior. Overall, the threats of inhibiting the freedom of the teachers are near to neutral, and it can be implied that they may not see that potential lawsuits are imminent. Perhaps, due to the relatively new implementation of multiple data privacy laws, issues of lawsuits are not entirely visible to the teaching community. The perceptions on the privacy concern for the use of communication tools and risks of exposing others

shows that teachers could have potentially made minor breach in privacy of student data but shows little concern if there would be legal ramifications in the future.

Despite these findings, our study is without its limitations. There are numerous rooms for improvements and opportunities that can be explored. Perhaps, future research could dive into topics that involve a holistic environment of the school setting, where administrators, and the student body are involved. Aside from instruction, the professional and social environment among different countries would be potentially good for exploration. The study was done on a limited scope involving only the city of Manila in the Philippines, in which the results may differ dramatically to other regions of the country or differ from different countries.

Nevertheless, our study has investigated the legal perceptions of the teachers through the Philippine context. We believe that there is a wide potential for research in teacher behavior and data privacy. Our study introduces the different concepts of data privacy in the Philippine context, and it could serve Filipino educators well for building on the growing knowledge of data privacy and the views on its legal implications.

Acknowledgements

We would like to thank our professor Atty. Jocelyn Cruz, faculty and former dean of De La Salle University's (DLSU) College of Law, for encouraging us in making this research. We would also like to express gratitude to all of our colleagues, friends, and fellow teachers who have helped in gathering data. This research would not also be possible without the guidance of Dr. Ferdinand Pitagan, former chair of Educational Leadership and Management Department of DLSU, for his wisdom in being productive in research writing.

References

Amihan. (2017, July 10). The beginner's guide to ra 10173 (data privacy act of 2012). Retrieved from https://amihan.net/2017/07/10/beginners_guide_to_ra_10173/

Aston, J. (2017, November 10). How the data protection act affects schools. Retrieved from https://www.stonegroup.co.uk/data-protection-act-affects-schools/

Belanger, F., Collignon, S., Enget, K., & Negangard, E. (2011). User resistance to the implementation of a mandatory security enhancement. *IFIP WG8. 11/WG11*, *13*.

Bloom, A., & Attai, L. (2016, December 12). The abcs of student data privacy for administrators. McGrawhill Education. Retrieved from https://www.districtadministration.com/content/abcs-student-data-privacy-administrators

Boyd, D., & Metcalf, J. (2014, November 10). Example "big data" research controversies. Retrieved from https://bdes.datasociety.net/council-output/example-big-data-research-controversies/

Cavivo, F.J., Majtaba, B. G., Muffler, S. C., & Samuel, M. (2013): Social Media and the Workplace: Legal, Ethical, and Practical Considerations for Management. Journal of Law, Policy and Globalization, Vol.12, 2013

Chou, H.-L., & Chen, C.-H. (2016). Beyond identifying privacy issues in e-learning settings–Implications for instructional designers. Computers & Education, 103, 124–133.

Chou, H., & Chou, C. (2016). Computers in Human Behavior An analysis of multiple factors relating to teachers ' problematic information security behavior. *Computers in Human Behavior*, *65*, 334–345. https://doi.org/10.1016/j.chb.2016.08.034

Clemons, E. K., & Wilson, J. S. (2015). Family preferences concerning online privacy, data mining, and targeted ads: regulatory implications. *Journal of Management Information Systems*, *32*(2), 40-70. doi:10.1080/07421222.2015.1063277

Dimock, M. (2018, March 1). *Defining generations: Where Millennials end and post-Millennials begin.* Retrieved from http://www.pewresearch.org/fact-tank/2018/03/01/defining-generations-where-millennials-end-and-post-millennials-begin/

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information systems research, 17(1), 61-80.

DLA Piper. (2018, January). Law - dla piper global data protection laws of the world. Retrieved from https://www.dlapiperdataprotection.com/index.html?t=law&c=TH

Foulger, T. S., Ewbank, A. D., Kay, A., Popp, S. O., & Carter, H. L. (2009). Moral spaces in MySpace: Preservice teachers' perspectives about ethical issues in social networking. *Journal of Research on Technology in Education*, *42*(1), 1-28.

InternetWorldStats (2016). Retrieved from http://www.internetworldstats.com/

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. Information and Management, 54(7), 851–865. https://doi.org/10.1016/j.im.2017.01.001

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

MacCarthy, M. (2014). Student privacy: harm and context. *International Review of Information Ethics*, *21*, 11-24. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093299

National Privacy Commission. (n.d.). Data privacy act primer. Retrieved from https://privacy.gov.ph/data-privacy-act-primer/

Nicolas and De Vega Law Offices. (2016). Data privacy in the philippines. Retrieved from http://ndvlaw.com/data-privacy-in-the-philippines/

Sarapin, S. H., & Morris, P. L. (2015). Faculty and Facebook friending: Instructor–student online social communication from the professor's perspective. *The Internet and Higher Education*, *27*, 14-23.

Smith, M, Szongott, C., Henne, B. & Von Voigt, G. (n.d.): Big Data Privacy Issues in Public Social Media

Singer, N. (2013, October 5). Deciding who sees students' data. Retrieved from http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html

Strauss, V. (2015, November 12). The astonishing amount of data being collected about your children. Retrieved from https://www.washingtonpost.com/news/answer-sheet/wp/2015/11/12/the-astonishing-amount-of-data-being-collected-about-your-children/?utm_term=.59d456ce1ad1

Parsons, M., & Crawford, L. (2016, September 9). Philippines finalizes data privacy act implementing rules. Retrieved from https://www.hldataprotection.com/2016/09/articles/international-eu-privacy/philippines-finalizes-data-privacy-act-implementing-rules/

Peterson, R. A. (1994). A meta-analysis of Cronbach's coefficient alpha. *Journal of consumer research*, *21*(2), 381-391.

Wapp, A. (2017, April 27). Philippines data privacy act and implementing regulations. Retrieved from https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/

Wang, Z., Novak, H., Scofield-Snow, H., Traylor, S., & Zhou, Y. (2015). Am I disclosing too much? Student perceptions of teacher credibility via Facebook. *The Journal of Social Media in Society*, *4*(1).

Yang, F., & Wang, S. (2014). Students' perception toward personal information and privacy disclosure in e-learning questionnaire. *PsycTESTS Dataset*, *13*(1). doi:10.1037/t44647-000

Contact email: juan_carlo_zamora@dlsu.edu.ph
madeleine_rose_tan@dlsu.edu.ph
sharon_albacete@dlsu.edu.ph
rosemin.laguerta@dlsu.edu.ph