POTENTIAL THREATS OF INFORMATION DISCLOSURE IN SOCIAL MEDIA: A SYSTEMATIC LITERATURE REVIEW

Budi Yulianto[1]; Fredy Purnomo[2]; Evaristus Didik Madyatmadja[3]; Meyliana[4]; Harjanto Prabowo[5]

[1,2] Computer Science Department, School of Computer Science, Bina Nusantara University,
[3,4,] Information Systems Department, School of Information Systems, Bina Nusantara University,
[5] Management Department, School of Business Management, Bina Nusantara University,
Jln. K.H. Syahdan No 9, Jakarta Barat, DKI Jakarta, 11480, Indonesia
[1]laboratory@binus.ac.id; [2]fpurnomo@binus.edu; [3]emadyatmadja@binus.edu; [4]meyliana@binus.edu; [5]harprabowo@binus.edu

ABSTRACT

Along with the growth of social media, a variety of potential threats to users is also increasing. These kinds of threats often occur because the users accidentally or unknowingly disclose their information or identity on social media. Threats resulted from the disclosure of information are needed to be known so that the users can understand the risks that arise and take precautions. This research was aimed to summarize the potential threats arising from the information disclosure in social media. The research method used was a systematic literature review to explore and summarize the literatures that discuss the specific topic. The research results show that the potential threats are mostly social threats and identity theft.

Keywords: *social media, information disclosure, systematic literature review, social threat, identity threat*

INTRODUCTION

Social media is an online interaction and communication media that allows the communities forming (Gangopadhyay & Dhar, 2014), content sharing (Guo, 2008), and collaboration (Rouse, 2015). Social media are providing interaction channel for their users (Acquisti & Gross, 2006) and appearing as a potentially addictive 'toy' that fills the social vacuum in people's lives and produces the ongoing sensation (Turel & Serenko, 2012). Most users typically use social media for fun and spending time rather than gathering information (Fogel & Nehmad, 2009).

Currently, the popular social media are Facebook, Twitter, LinkedIn, Pinterest, Google+, Tumblr, and Instagram (Ebizmba, 2016; Elmaghraby & Losavio, 2014). Facebook, a social media that was built in 2004, is now becoming the most popular social media with 1.5 billion users (Figure 1) and revenue of $3.7 billion per year (Factslides, 2015). Thus a large number of communities have made Facebook as the online 'state' with the densest number of 'residents' even outnumbering the population of China. Along with the growth of Facebook, a variety of threats to users is also increasing (Shullich, 2012; Jones & Soltren, 2005; Acquisti & Gross, 2006). About 122 million Facebook users use fake accounts, and there are 600.000 hacking attacks attempted every day. Other data said that 1 of 3 Facebook users feel disappointed, sad, and intimidated after accessing Facebook.

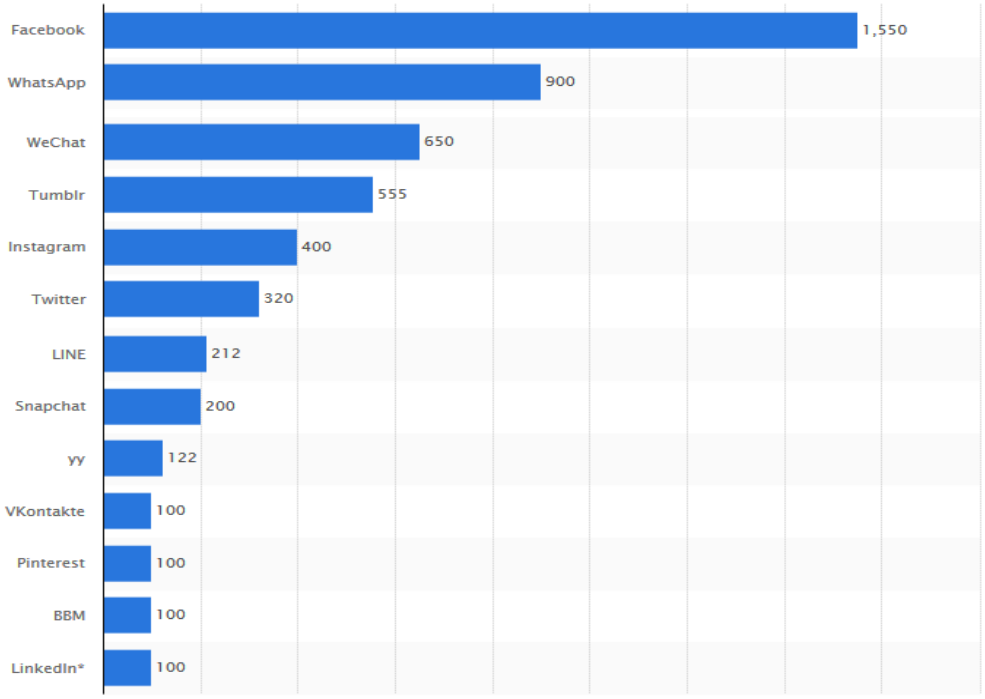

Figure 1 Social Media Active Users in Million per January 2016 (Statista, 2016)

Many threats and dangers are growing in line with the growth of social media (Figure 2). A 14-year-old boy who loved gaming, was groomed online and murdered in 2014 (Moore, 2016). In 2015, a 19-year-old girl had been kidnapped after getting contact with a fake account by promising a job at Amazon (McMillan, 2015). In 2016, a 13-year-old girl had been kidnapped and murdered after getting contact in social media (Riley, 2016). There is also a list of death for trivial matters in social media. A man killed his friend for "poking" his girlfriend, a wife was killed for changing status to single, a man used social media to lure his ex-girlfriend into a death trap, and a 17-year-old girl killed herself after being cyberbullied (Milam, 2016).

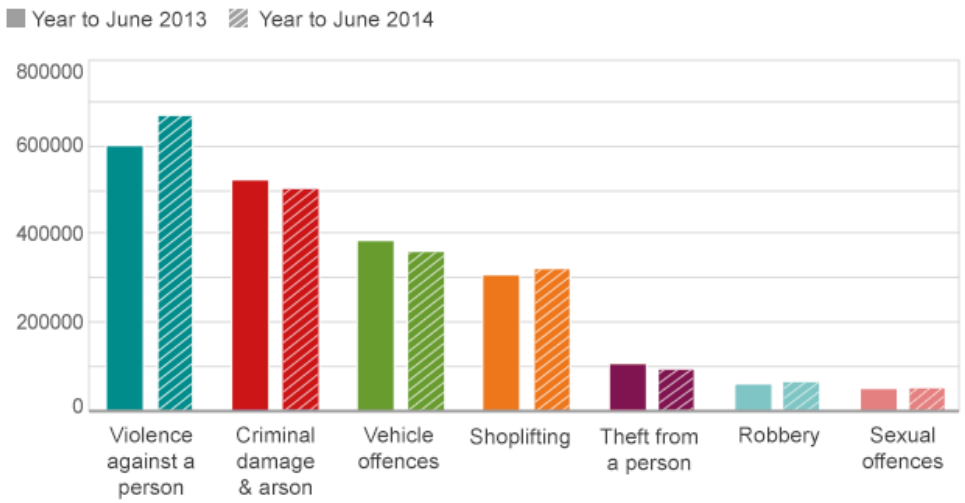

Figure 2 Social Media Crime Reported Statistics (BBC, 2014)

Bishop (2013) and Krasnova *et al.* (2009) divided the potential threats in social media into three categories, namely identity, social, and technology threat. Identity threat is activities of user's information or identity theft. Social threat includes (1) cyberbullying, ridicule or bullying activities that annoy users by either textual or visual, (2) cyber crime, criminal activities that generally lead to fraud or financial theft (Lawstuff, 2015), and (3) sexual predator, sexual crimes in the form of ridiculement, visual, to unwanted sexual act. These threats often occur because the users accidentally or unknowingly disclose their identity information in social media (Christofides *et al*., 2010; Acquisti & Gross, 2006), poorly understood default sharing mechanism, or intentional use of user data by social media provider for marketing purposes (Lucas & Borisov, 2008).

This research is conducted to answer a research question "What are the potential threats arising from information disclosure in social media?". Through systematic literature review (SLR) research method, researchers will explore and summarize journals that discuss the topic. Expected result of this study is to contribute to the community of the potential threats caused by information disclosure in social media, either as precaution or exhortation to the users.

METHODS

This research method is Systematic Literature Review (SLR) approach that includes determining the research questions, source of the journal, organizing keywords to search journals, data extraction, and analyzing the result to answer the research question (Ridley, 2012). SLR is currently a trend research method because it summarizes the essence of the journals those are growing rapidly in number. The summary is necessary to accelerate other researchers in conducting further researches.

Sources of journal on this study include three major publishers, namely (1) ACM Digital Library (dl.acm.org), (2) Science Direct (www.sciencedirect.com), (3) Springer Link (link.springer.com), and several other sources that will be presented in this article. Keywords used to search the journals in answering research question are by the combination of Boolean operators: AND, and OR. There are two pairs certain keywords used namely the first is danger, threat or crime, information or privacy, and social media or social network as for the second pair is namely danger, threat or crime, and social media or social network.

Keywords are inserted into each web publisher, and hundreds to thousands of journal titles are displayed. The titles of journals that appropriate to answer the research question are categorized as 'studies found'. After that, the abstract from each journal are read, and that correspondingly answers the research question are categorized as 'candidate studies'. Last, the journals are downloaded and read in detail, and that appropriate to answer the research question are categorized as 'selected studies' (Figure 3).

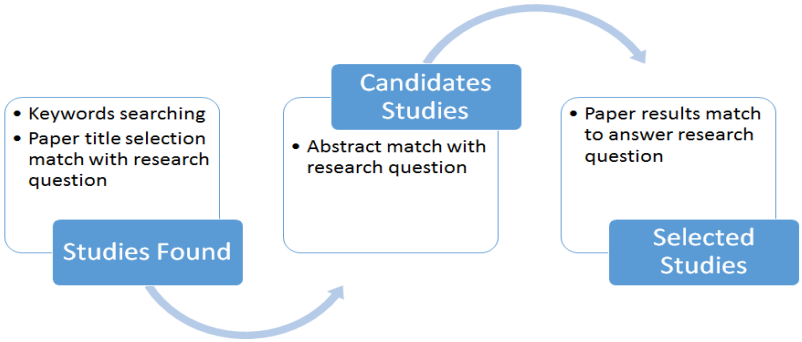

Figure 3 Steps for Selecting Journal

Journals published before 2005 are not used in order to preserve the up-to-date research results. Year 2005 is determined based on one year after the launch of current popular social media, Facebook. Determination of 1 year is based on the possibility of the publication of journals that discuss the threats of information disclosure in Facebook already began to be studied by researchers. Nevertheless, this study does not only examine Facebook but also other social media. The next stage is the process of extracting the data (Table 1).

Table 1 Data Extraction

Source	Studies Found	Candidate Studies	Selected Studies
ACM	53	32	10
ScienceDirect (ScDr)	76	33	12
Springer (Spr)	61	25	8
Other (Oth)	49	14	6
TOTAL	239	104	36

RESULTS AND DISCUSSIONS

Those 36 journals are obtained to answer the research question (Table 2, sorted by journal title). Year of publication, researcher name, and journal/conference name of each journal can be seen on References chapter at the end of this journal.

Table 2 List of Journals

No	Journal Title and Citation
1	A Regulatory Model for Personal Data on Social Networking Services in the UK (Haynes et al., 2016)
2	An Empirical Analysis of Users' Privacy Disclosure Behaviors on Social Network Sites (Li et al., 2015)
3	College Students' Consumption, Contribution, and Risk Awareness Related to Online Mapping Services and Social Media Outlets: Does Geography and GIS Knowledge Matter? (Mathews et al., 2013)
4	Cyber Security Challenges in Smart Cities: Safety, Security and Privacy (Elmaghraby & Losavio, 2014)
5	Disclosure of Information by Children in Social Networking—Not Just a Case of "You Show Me Yours and I'll Show You Mine" (De Souza & Dick, 2009)
6	Facebook: Threats to Privacy (Jones & Soltren, 2005)
7	Facebook's Privacy Trainwreck (Boyd, 2008)
8	Flybynight: Mitigating the Privacy Risks of Social Networking (Lucas & Borisov, 2008)
9	Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook (Acquisti & Gross, 2006)
10	Improving Content Privacy on Social Networks Using Open Digital Rights Management Solutions (Marques & Serrão, 2013)
11	Individual Information Security, User Behaviour and Cyber Victimisation: An Empirical Study of Social Networking Users (Saridakis et al., 2016)
12	Inferring Privacy Information from Social Networks (He et al., 2006)
13	Information Revelation and Privacy in Online Social Networks (The Facebook Case) (Gross & Acquisti, 2005)
14	Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns (Fogel & Nehmad, 2009)
15	Is lurking an Anxiety-Masking Strategy on Social Media Sites? The Effects of Lurking and Computer Anxiety on Explaining Information Privacy Concern on Social Media Platforms (Osatuyi, 2015)
16	LotusNet: Tunable Privacy for Distributed Online Social Network Services (Aiello & Ruffo, 2012)
17	Network and Device Forensic Analysis of Android Social-Messaging Applications (Walnycky et al., 2015)

Table 2 List of Journals (continued)

No	Journal Title and Citation
18	Obscurity by Design: An Approach to Building Privacy into Social Media (Stutzman & Hartzog, 2012)
19	On Privacy and Security in Social Media–A Comprehensive Study (Kumar et al., 2016)
20	On the Leakage of Personally Identifiable Information Via Online Social Networks (Krishnamurthy & Wills, 2009)
21	Overview of the Special Issue on Trust and Veracity of Information in Social Media (Papadopoulos et al., 2016)
22	Perceived Risks and Risk Management of Social Media in an Organizational Context (Munnukka & Järvi, 2014)
23	Privacy Concerns and Identity in Online Social Networks (Krasnova et al., 2009)
24	Proactive Insider Threat Detection Through Social Media: the YouTube Case (Kandias et al., 2013)
25	Risk-Taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors (Jia et al., 2015)
26	Social Media for Mental Illness Risk Assessment, Prevention and Support (De Choudhury, 2015)
27	Social Media Use and High-Risk Sexual Behavior Among Black Men Who Have Sex with Men: A Three-City Study (Broaddus et al., 2015)
28	Social Networking and The Exchange of Information (Wise & Shorter, 2014)
29	Social Networking Sites and Privacy Issues Concerning Youths (Gangopadhyay & Dhar, 2014)
30	Stranger Danger and the Online Social Network (Guo, 2008)
31	The Benefits and Dangers of Enjoyment with Social Networking Websites (Turel & Serenko, 2012)
32	The Privacy Jungle: On the Market for Data Protection in Social Networks (Bonneau & Preibusch, 2010)
33	The Relationship Between Online Social Network Use, Sexual Risk Behaviors, and HIV Sero-Status Among a Sample of Predominately African American and Latino Men Who have Sex with Men (MSM) Social Media Users (Chiu & Young, 2015)
34	Undergraduate Student Perceptions of Personal Social Media Risk (Rivera et al., 2015)
35	Understanding Member Use of Social Networking Sites from a Risk Perspective (Chena & Sharma, 2013)
36	You Are What You Say: Privacy Risks of Public Mentions (Frankowski et al., 2006)

The journals come from 48 institutions spread across 14 countries. The most contributing institutions are Carnegie Mellon University (3 journals) and University of California, Los Angeles (2 journals). The most contributing countries are USA (24 journals) and UK (4 journals). USA is also the highest Facebook users (about 170+ million users) in the world (Khan, 2015). Contribution of each country is shown in Table 3 and distribution of publication year is shown in Table 4. Most journals are also published in recent years (2015).

Table 3 Contributing Countries

Country	# Journals	Country	# Journals
Australia	1	India	2
Austria	2	Italy	2
Canada	1	Netherlands	1
China	1	Portugal	1
Finland	1	UAE	1
Germany	1	UK	4
Greece	2	USA	24

Table 4 Publication Years

Year	#	Year	#
2005	2	2012	3
2006	3	2013	4
2008	3	2014	4
2009	4	2015	9
2010	1	2016	3

Based on the extraction results from the journals, researchers found 28 potential threats that are grouped into five types and three categories that have been discussed previously. 28 potential threats are shown in Table 5. Mapping of five types and three categories of threat against publishers are shown in Table 6. Science Direct is the most prolific publisher that presents the threats. Identity theft and cyber crime are the most common threats.

Table 5 Potential Threats

No	Potential Threat	Threat Type	Threat Category
1	Absence of Guardianship	Identity Theft	Identity Theft
2	Accessible Target	Identity Theft	Identity Theft
3	Attitude	Cyber Bullying	Social Threat
4	Blackmailing	Cyber Crime	Social Threat
5	Bullying	Cyber Bullying	Social Threat
6	Character Assassination	Cyber Bullying	Social Threat
7	Cyber Attack Risk	Cyber Crime	Social Threat
8	Digital Notes	Identity Theft	Identity Theft
9	Embarrassment	Cyber Bullying	Social Threat
10	General Accessibility (HR check)	Identity Theft	Identity Theft
11	Home Life	Cyber Bullying	Social Threat
12	Identity Theft	Identity Theft	Identity Theft
13	Internet Risk	Cyber Crime	Social Threat
14	Motivated Offender	Cyber Bullying	Social Threat
15	Online Harassment (Pestering)	Cyber Bullying	Social Threat
16	Online Victim	Cyber Crime	Social Threat
17	Personal Life	Identity Theft	Identity Theft
18	Reidentification (Demographic, Face)	Identity Theft	Identity Theft
19	Sexual Harassment	Sexual Predator	Social Threat
20	Sexual Predator	Sexual Predator	Social Threat
21	Social Life	Cyber Bullying	Social Threat
22	Stalking	Identity Theft	Identity Theft
23	Transportation (Position)	Identity Theft	Identity Theft
24	Unencrypted Data	Technology Threat	Technology Threat
25	Using Public WIFI	Cyber Crime	Social Threat
26	Value of Privacy	Identity Theft	Identity Theft
27	Vendor Trust	Technology Threat	Technology Threat
28	Work Life	Cyber Bullying	Social Threat

Table 6 Mapping of (a) Threat Type and (b) Category to Each Publisher

(a)

No	Threat Type	Publisher				Total
		ScDr	ACM	Spr	Oth	
1	Identity Theft	12	13	8	5	38
2	Cyber Bullying	3	2	2	4	11
3	Cyber Crime	11	2	0	1	14
4	Sexual Predator	2	0	2	2	6
5	Technology Threat	2	0	0	0	2
	TOTAL	30	17	12	12	71

(b)

No	Threat Category	Publisher				Total
		ScDr	ACM	Spr	Oth	
1	Identity Theft	12	13	8	5	38
2	Social Threat	16	4	4	7	31
3	Technology Threat	2	0	0	0	2
	TOTAL	30	17	12	12	71

CONCLUSIONS

Analysis of the results showed that identity theft is the most common threat. Identity theft includes personal data, photo, activity (stalking), and position (Wise & Shorter, 2014). Employee candidates' data and daily activities checking by HRD (recruiters) of a company in social media before hiring can also be categorized as identity theft (Frankowski *et al.*, 2006). The police or authorities also often use social media to re-identify perpetrator through either history or photo (Boyd, 2008). Another common threat is social threat that includes ridicule or bullying activities (cyber bullying), disrupt or harm activities (blackmailing, photo editing, advertising), and online fraud (cyber crime) such as the spread of viruses, account theft, and financial fraud (Chena & Sharma, 2013).

Threats less likely to happen are online sexual disruption or taunt (sexual harassment) and sexual abuse (sexual predator) that occur in the real world because of identity fraud or personal identity manipulation to deceive victim (Gangopadhyay & Dhar, 2014). Although there is less case of sexual harrasment, the threat often appears in the news because of the visible complaint from the victim (Guo, 2008). Identity theft is very rarely posted because of difficulty to trace, the victim is not aware, and the impact obtained is not rapidly felt (Walnycky *et al.*, 2015).

Social media is still playing an important role in human life as a community forming and communication media that is fast, easy, and inexpensive (Turel & Serenko, 2012). Along with the widespread use of social media by the community (Gross & Acquisti, 2005), the threats also increase (Lucas & Borisov, 2008; Fogel & Nehmad, 2009). Users are advised to be more selective to open information (Koehorst, 2013; Saridakis *et al.*, 2016), and the role of parents and educators are also needed to guide the use of social media wisely (Jia *et al.*, 2015). Various studies, media coverages, and the public's attention are expected to encourage the development of more secure social media for users (Gross & Acquisti, 2005). The government is also expected to provide legal laws to protect users (Elmaghraby & Losavio, 2014) and to punish perpetrators of online crime (US Dept. of Justice, 2013).

REFERENCES

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies*, *4258*, 36-58. doi: 10.1007/11957454_3

Aiello, L. M., & Ruffo, G. (2012). Lotus Net: Tunable privacy for distributed online social network services. *Computer Communications*, *35*(1), 75-88. doi: 10.1016/j.comcom.2010.12.006

BBC. (2014). *Rapes increase by 29% as overall crime falls in England and Wales*. Retrieved in March, 2016 from http://www.bbc.com/news/uk-29642455

Bishop, E. (2013). *5 Threats To Your Security When Using Social Media*. Retrieved in October, 2015 from http://www.adweek.com/socialtimes/5-social-media-threats/493325

Bonneau, J., & Preibusch, S. (2010). The privacy jungle: On the market for data protection in social networks. *Economics of Information Security and Privacy*, 121-167. doi: 10.1007/978-1-4419-6967-5_8

Boyd, D. (2008). Facebook's Privacy Trainwreck. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13-20. doi: 10.1177/1354856507084416

Broaddus, M. R., DiFranceisco, W. J., Kelly, J. A., Lawrence, J. S. S., Amirkhanian, Y. A., & Dickson-Gomez, J. D. (2015). Social media use and high-risk sexual behavior among black men who have sex with men: a three-city study. *AIDS and Behavior*, *19*(2), 90-97. doi: 10.1007/s10461-014-0980-z

Chena, R., & Sharma, S. K. (2013). Understanding Member Use of Social Networking Sites from a Risk Perspective. *Procedia Technology*, 9, 331-339. doi:10.1016/j.protcy.2013.12.037

Chiu, C. J., & Young, S. D. (2015). The relationship between online social network use, sexual risk behaviors, and HIV sero-status among a sample of predominately African American and Latino men who have sex with men (MSM) social media users. *AIDS and Behavior*, *19*(2), 98-105. doi: 10.1007/s10461-014-0986-6

Christofides, E., Desmarais, S., & Muise, A. (2010). *Privacy and Disclosure on Facebook: Youth and Adult's Information Disclosure and Perceptions of Privacy Risks*. Retrieved in October, 2015 from https://www.ontariosciencecentre.ca/Uploads/researchlive/documents/OPC-FinalReport-FacebookPrivacy.pdf

De Souza, Z., & Dick, G. N. (2009). Disclosure of information by children in social networking—Not just a case of "you show me yours and I'll show you mine". *International Journal of Information Management*, *29*(4), 255-261. doi: 10.1016/j.ijinfomgt.2009.03.006

De Choudhury, M. (2015). Social Media for Mental Illness Risk Assessment, Prevention and Support. *Proceedings of the 1st ACM Workshop on Social Media World Sensors*, 1-1. doi: 10.1145/2806655.2806659

Ebizmba. (2016). *Top 15 Most Popular Social Networking Sites*. Retrieved in March, 2016 from http://www.ebizmba.com/articles/social-networking-websites

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, I(4), 491-497. doi: 10.1016/j.jare.2014.02.006

Factslides. (2015). *Facebook Facts*. Retrieved in October, 2015 from http://www.factslides.com/s-Facebook

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior*, *25*(1), 153-160. doi: 10.1016/j.chb.2008.08.006

Frankowski, D., Cosley, D., Sen, S., Terveen, L., & Riedl, J. (2006). You are what you say: privacy risks of public mentions. *Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval*, 565-572. doi: 10.1145/1148170.1148267

Gangopadhyay, D. S., & Dhar, M. D. (2014). Social Networking Sites and Privacy Issues Concerning Youths. *Article-2 Global Media Journal-Indian Edition*, *5*(1).

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 71-80.

Guo, R. M. (2008). Stranger danger and the online social network. *Berkeley Technology Law Journal*, *23*(1), 617-644.

Haynes, D., Bawden, D., & Robinson, L. (2016). A regulatory model for personal data on social networking services in the UK. *International Journal of Information Management*, *36*(6), 872-882.

He, J., Chu, W. W., & Liu, Z. V. (2006). Inferring privacy information from social networks. *International Conference on Intelligence and Security Informatics*, 154-165.

Jia, H., Wisniewski, P. J., Xu, H., Rosson, M. B., & Carroll, J. M. (2015). Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 583-599. doi: 10.1145/2675133.2675287

Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. *Project MAC: MIT Project on Mathematics and Computing*, *1*, 1-76.

Kandias, M., Stavrou, V., Bozovic, N., & Gritzalis, D. (2013). Proactive insider threat detection through social media: The YouTube case. *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, 261-266. doi: 10.1145/2517840.2517865

Khan, I. (2015). *Top 10 most Facebook User Country in the World*. Retrieved in March, 2016 from http://worldknowing.com/top-10-most-facebook-user-country-in-the-world/

Koehorst, R. H. G. (2013). *Personal information disclosure on online social networks: an empirical study on the predictors of adolescences' disclosure of personal information on Facebook*. Retrieved in March 2016 from http://essay.utwente.nl/63797/1/MSc_Ruud_H.G._Koehorst.pdf

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39-63. doi: 10.1007/s12394-009-0019-1

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Proceedings of the 2nd ACM workshop on Online social networks*, 7-12. doi: 10.1145/1592665.1592668

Kumar, S., Saravanakumar, K., & Deepa, K. (2016). On Privacy and Security in Social Media–A Comprehensive Study. *Procedia Computer Science*, 78, 114-119. doi: 10.1016/j.procs.2016.02.019

Lawstuff. (2015). *Cyber Bullying*. Retrieved in October, 2015 from http://www.lawstuff.org.au/sa_law/topics/bullying/cyber-bullying

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management*, *52*(7), 882-891.

Lucas, M. M., & Borisov, N. (2008). Flybynight: mitigating the privacy risks of social networking. *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, 1-8. doi: 10.1145/1456403.1456405

Marques, J., & Serrão, C. (2013). Improving content privacy on social networks using open digital rights management solutions. *Procedia Technology*, 9, 405-410. doi: 10.1007/s12243-013-0388-1

Mathews, A. J., Lu, Y., Patton, M. T., Dede-Bamfo, N., & Chen, J. (2013). College students' consumption, contribution, and risk awareness related to online mapping services and social media outlets: does geography and GIS knowledge matter?. *Geo Journal*, *78*(4), 627-639. doi: 10.1007/s10708-012-9456-8

McMillan, R. (2015). *Man arrested for using social media to lure, kidnap teen*. Retrieved in March 2016 from http://abc7.com/news/man-arrested-for-using-social-media-to-lure-kidnap-teen/546961/

Milam, W. (2016). *The 15 Craziest Deaths Caused by Social Media*. Retrieved in March 2016 from http://www.ranker.com/list/the-13-craziest-deaths-caused-by-social-media/whitney-milam

Moore, A. (2016). *I couldn't save my child from being killed by an online predator*. Retrieved in March, 2016 from http://www.theguardian.com/lifeandstyle/2016/jan/23/breck-bednar-murder-online-grooming-gaming-lorin-lafave

Munnukka, J., & Järvi, P. (2014). Perceived risks and risk management of social media in an organizational context. *Electronic Markets*, *24*(3), 219-229. doi: 10.1007/s12525-013-0138-2

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior*, *49*(C), 324-332. doi: 10.1016/j.chb.2015.02.062

Papadopoulos, S., Bontcheva, K., Jaho, E., Lupu, M., & Castillo, C. (2016). Overview of the Special Issue on Trust and Veracity of Information in Social Media. *ACM Transactions on Information Systems* (TOIS), *34*(3), 14. doi: 10.1145/2870630

Ridley, D. (2012). *The literature review: A step-by-step guide for students*. Sage Publications Asia-Pacific.

Riley, N. S. (2016). *Don't downplay the dangers of social media to kids*. Retrieved in March 2016 from http://nypost.com/2016/02/07/dont-downplay-the-dangers-of-social-media-to-kids/

Rivera, J. C., Di Gangi, P. M., Johnston, A., & Worrell, J. L. (2015). Undergraduate student perceptions of personal social media risk. *Information Security Education Journal, 2*(2), 49-57.

Rouse, M. (2015). *Social Media*. Retrieved in Oct, 2015 from http://whatis.techtarget.com/definition/social-media

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320-330. doi: 10.1016/j.techfore.2015.08.012

Shullich, R. (2012). *Risk Assessment of social media*. Retrieved in October, 2015 from https://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940

Statista. (2016). *Leading social networks worldwide as of January 2016, ranked by number of active users (in millions)*. Retrieved in March, 2016 from http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Stutzman, F., & Hartzog, W. (2012). *Obscurity by design: An approach to building privacy into social media*. Retrieved in October, 2015 from http://fredstutzman.com/papers/CSCW2012W_Stutzman.pdf.

Turel, O., & Serenko, A. (2012). The benefits and dangers of enjoyment with social networking websites. *European Journal of Information Systems*, *21*(5), 512-528. doi: 10.1057/ejis.2012.1

US Dept. of Justice, Global Justice Information Sharing Initiative, & United States of America. (2013). *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*. Retrieved in March 2016 from https://it.ojp.gov/GIST/132/File/Developing%20a%20Policy%20on%20the%20Use%20of%20Social%20Media%20in%20Intelligence%20and%20Investigative%20Activities_compliant.pdf

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. *Digital Investigation*, *14*(1), S77-S84. doi: 10.1016/j.diin.2015.05.009

Wise, E. K., & Shorter, J. D. (2014). Social networking and the exchange of information. *Issues in Information Systems*, *15*(2), 103-109.