# Cyber Awareness and Social Media Scams Among Users

**J.Preetha[1*], K.Lokeshwaran[2], D. Asha[3] ,K.Bashkaran[4]**

## Abstract

Human behavior and interactions on social media have remained extremely dynamic real-time social systems that accurately express individual social awareness at fine spatial, temporal, and digital resolutions. By utilizing a social media aggregator, hackers will gain easy access to all social media platforms that are linked together. Social media users' lack of security awareness exposes them to a variety of cybercrime operations. Numerous countermeasures are being considered, including improving social media privacy settings, limiting social media authorization, and increasing social media users' security awareness. We discuss how social media spreads information, the multifaceted consequences of social media, and some real-world examples. On the one hand, social media has aided in the prediction of human dynamics across a broad range of domains, including public health, emergency response, decision-making and social justice promotion. Social networking sites can be used to facilitate data exchange. As a result, our study emphasized the users' awareness of social networking sites.

**Key Words:** Social Network, Security, Awareness, Human dynamics

**DOI Number: 10.14704/nq.2022.20.8.NQ44243** **NeuroQuantology 2022; 20(8):2209-2216**



## Introduction

In today's technology-driven world, social networking sites have become a vehicle for retailers to reach a broader audience with their marketing initiatives. The American Marketing Association describes social media marketing as a "link between brands and consumers, providing a personal channel and currency for user-centered networking and social interaction." With the advent of social media, the tools and tactics for connecting with customers have shifted dramatically; as a result, businesses must learn how to use social media in a way that is compatible with their business strategy. This is especially true for businesses seeking a competitive edge. This review evaluates the current body of knowledge regarding the development and usage of social media as an extension of a retailer's marketing strategy. While social media marketing is a well-researched subject, it has only been studied experimentally and theoretically; studies never accurately identify the benefits retailers receive from this marketing approach. After studying a profusion of multidisciplinary literature, it became obvious that studies are primarily concerned with defining social media marketing and examining the aspects that influence customer behaviour in relation to social networking. Despite early advances by scholars, advancement in this field of study has been slow. The research has to be expanded to provide a more complete picture of the long-term promotional benefits retailers derive from social media marketing. Additionally, more organized investigations are required to advance beyond hypothesized or expected effects and gather understanding about real-world applications. This review of the literature discusses the limitations in current social media marketing research and emphasizes the importance of future studies examining the benefits of marketing on social networking sites, particularly for small retailers.

**Corresponding author:** J.Preetha
**Address:** [1]Department of Computer Science and Engineering, Muthayammal Engineering College Autonomous, Rasipuram-637408, Tamil Nadu, India, [2]Associate Professor, C. Abdul Hakeem College of Engineering and Technology, [3]Assistant professor Jeppiaar institute of technology, [4]Department of BioMedical Engineering, Kongunadu College of Engineering and Technology Autonomous, Tholurpatti, Thottiam- 621215, Tamil Nadu, India
E-mail: psgpreetha@gmail.com[1] , k.lokeshwaran@gmail.com[2], asha@jeppiaarinstitute.org[3], bashkarank@kongunadu.ac.in[4]

Numerous individuals utilize social media platforms to communicate or spread "news" or knowledge with their social circles or with other social media users. Typically, these platforms are online social networking websites like Facebook and Instagram. Individuals' behaviour is influenced by information shared on social media, which is why social media is utilized for a variety of purposes—product marketing, political campaigning, and information dissemination, to name a few. For instance, businesses looking to market new products could advertise on social media by obtaining a large number of likes and comments on their online posts. Existing or prospective customers might then "follow" the companies' aggregated news in order to obtain additional information about them or their products.

This lack of awareness is exacerbated when the same information is delivered to an individual multiple times via various media outlets. Known as a "echo chamber," this type of circumstance increases the possibility that folks believe the phoney news is true. This occurs primarily on social media platforms as a result of the filter bubble effect of the website's algorithm. Many individuals may perceive a piece of news to be true without properly analyzing it, and this "bias perception" leads individuals to seek out similar information to bolster their opinions. These folks would therefore believe just those pieces of information that corroborate their own positions. As a result, the spread of bogus news on social media continues to grow. Typically, and consciously, social movements are created around agreed objectives, rules, and identities. Social movements are sometimes characterized by collective protests, such as those opposing a government decision or an environmental concern. Members of such social movements typically come from disparate social groups, political parties, and so on, but they share a common desire to effect change and hence affiliate themselves with the movement or group behind the movement. Individuals are encouraged to participate in collective action by the notion that it will be easier to attain a desired outcome if they work collaboratively rather than individually. As a group, there is a shared sense of identity and a greater chance of achieving the common goal. However, many individuals may join a movement without having a complete comprehension of it. Human actions and interactions in the digital realm, as well as regular status updates, might emerge as highly dynamic real-time social systems, allowing governments to create appropriate policies for relevant groups and targeted communities. The electronic footprints and perceptions left by users of social media and derivatives of complex social networks can be used to improve the design of location-based services. As a result of the growing need for mapping and analysing social media data, more new conceptual and technological breakthroughs in visual and computational methodologies are required. These research difficulties and opportunities may pave the way for a paradigm shift in larger social scientific disciplines as a result of this new data landscape.

**Figure 1. Social Media Awareness**

Social media communications can illustrate the interrelated patterns and links between cyberspace and real space, as well as be rapidly broadcast to a huge number of users worldwide who may be members of various virtual groups. The use of enormous computer-mediated communication in emergency response and disaster management has piqued the public's and policymakers' curiosity. Social media enables rapid interpersonal communication during crises through information dissemination, early warnings, environmental awareness, and public participation in disaster-affected areas, allowing emergency responds to respond more quickly and effectively, argue experts. "This growing use of social media during crises provides new information sources from which the appropriate authorities can enhance emergency situation awareness," they argue. Survivors in disaster-affected areas can provide on-the-ground reports about what they see, hear, and information during natural catastrophes. Residents in the immediate vicinity can contribute near-real-time views of disaster events, such as aerial shots and photographs."



## Literature Review

Social media platforms can be utilized to help contain the spread of pandemics and the worry that accompanies them. Through identifying, tracking,

andvisualizing users' behaviour patterns, scholars have employed sentiment analysis and spatial analysis to examine how social media communication distributes information about dangerous and infectious diseases and warns the public. For example, we examined public health-related rumour during disease outbreaks and evaluated how negative media framing affects the quality of disease outbreak detection and prediction, utilizing the spread of Ebola rumour in social media networks as a case study. Ordinary citizens and social media users have a relatively limited understanding of how contagious diseases spread across time and place, as well as their associated consequences. As a force in health communication, social media data could be used to define the infection's temporal scope and create a spatial database of disease reports. Additionally, social media data can be utilized to track and forecast the appearance and spread of infectious diseases, as well as their geographic and temporal distribution.

We can use public information resources such as news stories and public knowledge resources such as Wikipedia and Freebase to model the real world. These resources cover a broad range of topics spanning multiple facets of life. Additionally, they are updated in near real time as a result of recent advancements in publication technology, promoting these public information resources as a digital equivalent to the physical world. As a result, we may establish a link between social media data and the real world via the mirrored world of publicly available information resources. The primary technical problems in establishing this connection are the ability to autonomously extract events from those public resources (e.g., news stories) and the ability to connect the information in social media to the properly detected events. Such issues would necessitate a thorough examination of the semantics of the information supplied in both (e.g., posts on social media and events in public resources) in order to accurately identify the events and linkages. Fortunately, artificial intelligence research in areas such as natural language processing, computer vision, graph modelling, and machine learning is actively investigating deep semantic understanding of such information. For example, numerous recent research have demonstrated that events in news stories may be efficiently curated using deep learning approaches, a subset of machine learning capable of autonomously inducing underlying representations for data in order to achieve high extraction performance.

One user may share content about another user or party on social media. While this approach facilitates the efficient distribution of content across networks, it necessarily poses a significant danger of privacy breach. For instance, your pals may share a photo you shared of you and another buddy in a restaurant. Without your approval, photo sharing may be done without your knowledge and may inadvertently reveal your location or other private information that you do not like to share with anybody outside of your friend list. To combat such privacy violations, social media administrators have established ways for users to lodge complaints and request that content be removed from the networks. However, before the information can be examined and revoked, it may have had some adverse effects on users. It would be more effective if the spread of such content was vetted from the start. Addressing the issue of user-user privacy needs collaboration between experts from diverse fields, including computer scientists, geographic information scientists, and psychologists. For example, a hybrid negotiation architecture with a reciprocity mechanism was examined to simulate social responsibility in reality, and a credit system was utilized to incentive agents/users to respect others' privacy in social media.



Ye et al. (2017) used vote tweets over a California water bond to demonstrate location-based situational awareness. Convention and tourist bureaus may concentrate their efforts on 'hot button' issues in specific areas of their cities or regions. These data may provide operational indicators regarding the most often frequented or favourite sites by visitors, which can be used to inform marketing efforts for these locations. Local governments might study social media communications to ascertain whether the public would support a planned construction project or whether other proposed projects would be viewed positively by their voters.

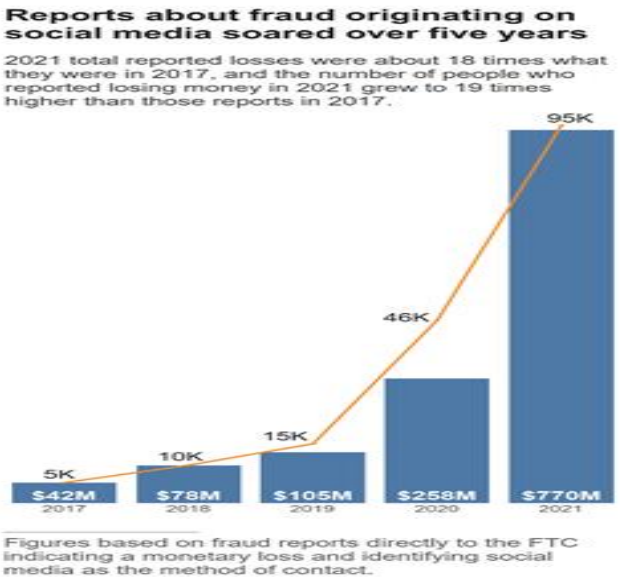
## Social Media Scams

In recent times social media has become the home of scammers. They perform different kind of scams in social media and people are falling to it. In recent times Facebook and Instagram have become the market place for small-business sellers, it is good to encourage the small-business owners but sometimes someone who claims to be a small-business owner is not actually a legit person he is a scammer. The Scammers performs the scam so legit that even a well-educated person couldn't find him. They will list the products with cheap prizes in their pages after people try to buy the product with the given link the page will have a Cash on Delivery option and if the victim proceeds to buy the product they website will display a message like "Due to the Covid-19 Pandemic the Cash On Delivery is not currently available" most people will think this as a legit reason and they will proceed to buy with their credit or debit card, after doing this they will get a tracking id, acknowledgement and everything that they would expect from a legit website but after some days if the victim try to open the website link there will be no such website exists and if the user try to go to the Social Media page where he found the link the page will also be disappeared and there will be no sign of this page again. The Scammer will come back with a new name and new website. The victim will be left helpless as he could do nothing other than complaining to Cybercrime. So, before you make a purchase in any unauthorized website make sure to verify that it is a legit website or not. Don't try to save money and fall on scams, if a product has a fixed price then the price variation must be somewhere around it but if you see the same product on social media listed for a very cheaper price then understand that it is a Scam!. Even the developed countries like USA also faces many online scams in recent times.

## The Online Scam Report Submitted By The Federal Trade Commission (Ftc) Usa

Social media permeates the lives of many people – we use it to stay in touch, make new friends, shop, and have fun. But reports to the FTC show that social media is also increasingly where scammers go to con us. More than one in four people who reported losing money to fraud in 2021 said it started on social media with an ad, a post, or a message. In fact, the data suggest that social media was far more profitable to scammers in 2021 than any other method of reaching people. More than 95,000 people reported about $770 million in losses to fraud initiated on social media platforms in 2021. Those losses account for about 25% of all reported losses to fraud in 2021 and represent a stunning eighteen fold increase over 2017 reported losses. Reports are up for every age group, but people 18 to 39 were more than twice as likely as older adults to report losing money to these scams in 2021.

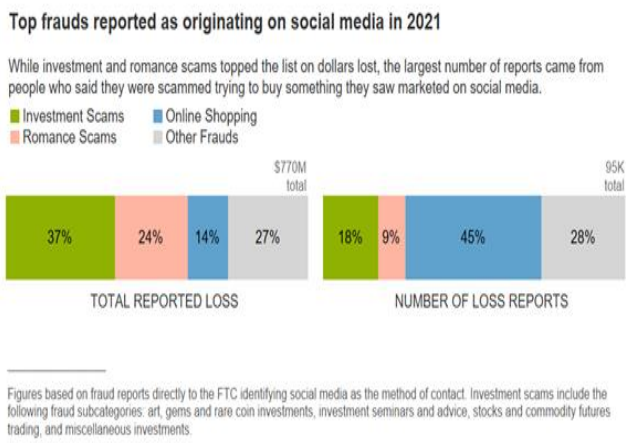
For scammers, there's a lot to like about social media. It's a low-cost way to reach billions of people from anywhere in the world. It's easy to manufacture a fake persona, or scammers can hack into an existing profile to get "friends" to con. There's the ability to fine-tune their approach by studying the personal details people share on social media. In fact, scammers could easily use the tools available to advertisers on social media platforms to systematically target people with bogus ads based on personal details such as their age, interests, or past purchases.




Reports make clear that social media is a tool for scammers in investment scams, particularly those involving bogus cryptocurrency investments — an area that has seen a massive surge in reports. More than half of people who reported losses to investment scams in 2021 said the scam started on social media. Reports to the FTC show scammers use social media platforms to promote bogus investment opportunities, and even to connect with people directly as supposed friends to encourage them to invest. People send money, often cryptocurrency, on promises of huge returns, but end up empty handed.

After investment scams, FTC data point to romance scams as the second most profitable fraud on social media. Losses to romance scams have climbed to

record highs in recent years. More than a third of people who said they lost money to an online romance scam in 2021 said it began on Facebook or Instagram. These scams often start with a seemingly innocent friend request from a stranger, followed by sweet talk, and then, inevitably, a request for money. While investment and romance scams top the list on dollars lost, the largest number of reports came from people who said they were scammed trying to buy something they saw marketed on social media. In fact, 45% of reports of money lost to social media scams in 2021 were about online shopping. In nearly 70% of these reports, people said they placed an order, usually after seeing an ad, but never got the merchandise. Some reports even described ads that impersonated real online retailers that drove people to lookalike websites. When people identified a specific social media platform in their reports of undelivered goods, nearly 9 out of 10 named Facebook or Instagram.




Together, investment scams, romance scams, and online shopping fraud accounted for over 70% of reported losses to social media scams in 2021. But there are many other frauds on social media too, and new ones popping up all the time. Here are some ways to help you and your family stay safe on social media:

Limit who can see your posts and information on social media. All platforms collect information about you from your activities on social media, but visit your privacy settings to set some restrictions.

Check if you can opt out of targeted advertising. Some platforms let you do that.

If you get a message from a friend about an opportunity or an urgent need for money, call them. Their account may have been hacked – especially if they ask you to pay by cryptocurrency, gift card, or wire transfer. That's how scammers ask you to pay.

If someone appears on your social media and rushes you to start a friendship or romance, slow down. Read about romance scams. And never send money to someone you haven't met in person.

Before you buy, check out the company. Search online for its name plus "scam" or "complaint."

## Awareness On Cheating Scam ( By The Cyber Cell Delhi India)

In this type of scam, the sender, generally through an email, requests help in facilitating the transfer of a substantial sum of money. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request that money be sent to pay for some of the costs associated with the transfer. Once money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems with the transfer.

In such matters the victims normally allege that they have received emails from unknown sources wherein they have been informed that:

• Either they have won a lottery worth millions of dollars; or

• Their help is required for transferring of illegal money from some African Country; or

• They have been selected for an overseas job, generally a hotel job in some European/American country; or

• Goods are offered at throwaway prices; or

• In some cases, the victim's address book in her emailing list is compromised and emails sent to all her contacts from her ID asking for money to bail out from a perilous situation;

The victims are trapped in a phased manner and are generally made to deposit a huge amount of money either as money transfer fee, payment of taxes or transportation cost.

The victims apparently receive a spam email and respond to the same and ends up paying money to some unknown persons for a nonexistent purpose.

Such crimes are generally carried out from foreign locations. Money is either deposited in offshore accounts or in some courier account in India.

## Preventive Measures/Precautions

1. Do not chat with strangers over net. Fraudsters and scammers prowl on the internet looking for victims.

2. Never send money or give credit card details, online account details or copies of personal

documents to anyone you don't know or trust and never by email.
3. Avoid any arrangement with a stranger who asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.
4. Do not agree to transfer money for any unknown person. Money laundering is a criminal offence.
5. Verify the identity of the contact by calling the relevant organization directly – find them through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you.
6. Check credentials of foreign enteties through the concerned Embassies and High Commissions, Counselates etc.
7. Do an internet search using the names or exact wording of the letter/email to check for any references to a scam – many scams can be identified this way.
8. If you think it's a scam, don't respond — scammers will use a personal touch to play on your emotions to get what they want.
9. Remember there are no get-rich-quick schemes: if it sounds too good to be true it probably is a trap.

## Research Methodology

The study's main objective is to connect the quantitative system with a specific end goal of spuriously investigating the social information of potential users and acquiring the much-needed details about the responds, such as demographic data, temporal data, and user profile. This study took a quantitative method. The questionnaire was the primary instrument used in the data collection process.

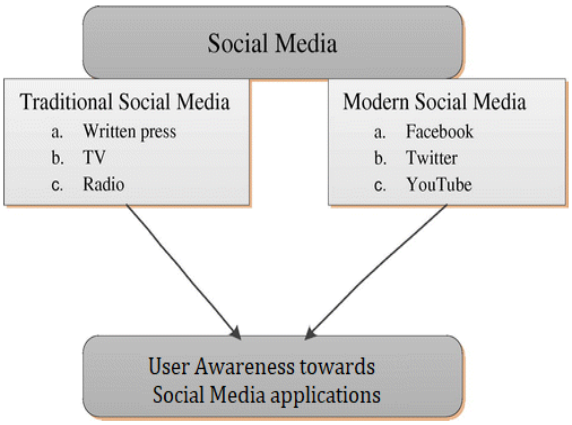



**Figure 2. Methodology**

The respondents were 100 users with social media accounts. In this study, a simple random sample procedure was applied. The Statistical Package for Social Sciences (SPSS) software was used to analyse the obtained data. Through the use of frequency distribution and percentage techniques, descriptive analysis was performed on the respondents' demography to ascertain the total number of respondents tested by gender, age, and educational level. The mean and standard deviation were used to determine the level of knowledge and awareness of the threat of cyber security as a result of social media use for questions in parts II, III, and IV.

**Table 1. Questionnaire part**

| No. | Component | Parts of Questions |
|---|---|---|
| 1 | User's Profiles | General Profiles of Users |
| 2 | Information on Social Media | Information on social media used |
| 3 | Awareness Level | Knowledge and awareness about social media |
| 4 | Awareness about cyber security | Knowledge and awareness about cyber security and its threat |



The destinations of social network sites work to enforce privacy settings. Facebook and other long-distance social communication destinations place a premium on security as a default setting. It is critical for customers to access their client settings and modify their security preferences. These places, for example, Facebook, enable clients to conceal personal information, for example, their conception date, email address, telephone number, and business status. For those who choose to incorporate this content, Facebook allows users to restrict access to their profile to just those they identify as "companions." Even with this level of secrecy, one of those companions may save a snapshot to their own PC and post it elsewhere. Regardless, fewer social media site clients have restricted their profiles as of late.

## Results & Discussion

The findings are classified into three categories: basic understanding of social networking usage awareness; technical awareness for secure social networking; advocacy for social networking awareness; and reactivity to occurrences and suspicious profiles on such sites. The findings are

evaluated according to the respondents' gender and academic background. The sub-sections that follow discussed the outcomes for each category.

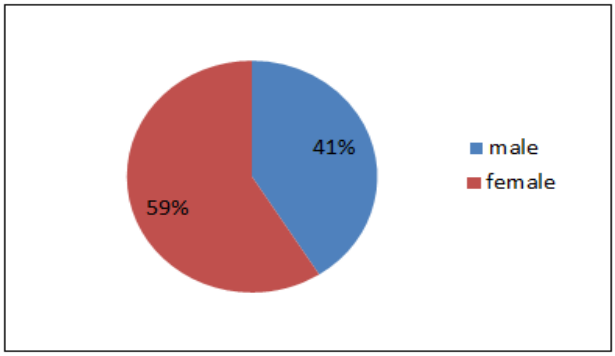



**Figure 3. Users Composition based on gender**

Female respondents, on average, have a higher level of security awareness than male respondents, at 59% versus 41%. Women, as defined, are more inclined to put an emphasis on the surroundings in order to accomplish their goals. The objective of Path is to ensure that users keep a level of privacy that is regarded appropriate for women. The emphasis on achieving objectives in this regard is on the use of social media Paths that allow for privacy protection.

As illustrated in figure 4, respondents with a Bachelor's degree or higher had the highest level of security awareness (43%). Basic Awareness has a flat - the highest average percentage for all academic backgrounds with specifics on the percentage of Advocacy has the lowest level of security awareness for respondents with a high school intellectual background (35 percent ) Additionally, highly educated individuals get sufficient information and are receptive to novel ideas. (The information contained above may pertain to an individual's level of awareness on information security).

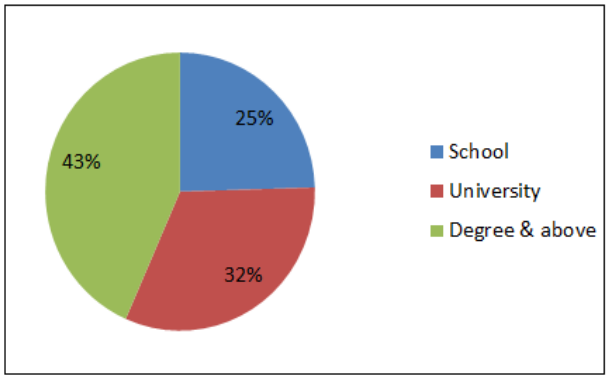



**Figure 4. Users Composition based on academic background**

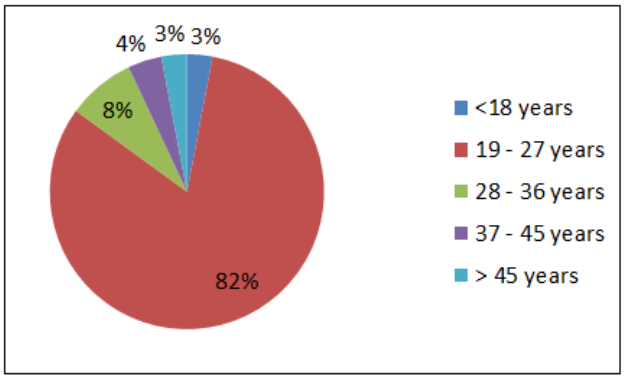



**Figure 5. Users Composition based on age**

Respondents aged 19-27 years demonstrate the greatest level of security awareness, with an average of 82 percent. Meanwhile, respondents aged > 45 years have the lowest level of security awareness, at 3%. The succession of ages from the highest to the lowest level of security awareness is depicted in Figure 5. As customers' willingness and abilities (in this case, their use of social media, particularly their attitude toward security awareness) change with age.

## Conclusion

The primary aim of this article was to assess security awareness about the use of social networking sites. As a result, as a social media user, we must always verify the validity of information before disseminating it in order to prevent being a victim of fraud. Individuals must exercise caution when receiving information from official sources or vice versa. If the information is not verified, it should not be distributed, as distributing false information can have a harmful effect on the individual, society, and nation. We must always keep in mind the phrase "Uncertain, Do Not Share." Authorities must play their part by taking necessary action against those who create or distribute misleading information on social media. Each individual must utilizesebenarnya.my as a means of determining the veracity of information at all times. However, there are some students who only use the internet for educational purposes. In summary, mobile technology use includes a number of benefits and drawbacks. As such, as a responsible community, we must exercise caution in preventing the spread of misleading information that could jeopardize the country's wealth and well-being.

## References

Nguyen TM, Nguyen TH (2019) One for all: neural joint

modeling of entities and events. In: The association for the advancement of artificial intelligence (AAAI), arXiv.org >cs>

Kekulluoglu D, Kokciyan N, Yolum P (2017) Preserving privacy as social responsibility in online social networks. ACM Trans Internet Technol 18(4):1–22

Ye X, Li S, Sharag-Eldin A et al (2017) Geography of social media in public response to policy-based topics. In: Ye X, Li S, Sharag-Eldin A et al (eds) Geospatial data science techniques and applications. CRC Press, Boca Raton, US, p 221–232

Zadeh AH, Zolbanin HM, Sharda R et al (2019) Social media for nowcasting flu activity: spatiotemporal big data analysis. InfSyst Front 21(4):743–760.

James, P., Lawler, John C. Molluzo, 2010. A survey of First Year College Student Perceptions of Privacy in Social Networking. Journal of Computer Sciences in Colleges., 26(3): 36-41. Consortium of Computing Sciences in Colleges. USA.http://dl.acm.org/citation.cfm?id=1859168 (Accessed on July 10, 2012)

BasilisaMvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networ king service users, and motivation prediction from observable features. Computers in Human Behavior, Dec 2014; 4(c):20-34.

Helen Streck., 2011. Social Networks and Their Impact on record and Information Management. ARMA International Educational Foundation. Pennsylvania,USA.http://www.armaedfoundation.org/pdfs/Social_Networks_Impact_on_RIM_Streck. pdf (Accessed on July 8, 2012).

Choo, K.-K.R., 2009. Online child grooming:a literature review on the misuse of social networking sites for grooming children for sexual offences. Retrieved 7 August, 2012 from, http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf. Australian Institute of Criminology, Canberra (Accessed on July 8, 2012).

Mitchell, K.J., D. Finkelhor, L.M. Jones, J. Wolak, 2010. Use of Social Networking Sites in Online Sex Crimes Against Minors: an Examination of National Incidence and Means of Utilization. Journal of Adolescent Health. Vol. 42(2), pp. 183-190 Elsevier.http://www.ncbi.nlm.nih.gov/pubmed/20638011. (Accessed on March 3, 2012).

Young, A.L., A. Quan-Haase, 2009. Information Revelation and Internet Privacy Concernson Social Network Sites: A Case Study of Facebook. Proceedings of the 4th International Conference on Communities and Technologies, pp. 265-274.http://dl.acm.org/citation.cfm?id=1556499 (Accessed on August 3, 2012).

Kozinets, R. V., Belz, F. M., & McDonagh, P. (2012). Social media for social change. In D. G. Mick, S. Pettigrew, C. Pechmann, & J. L. Ozanne (Eds.), Transformative consumer research for personal and collective well-being (pp. 205–223). New York, NY: Taylor and Francis.

Madge, C., Meek, J., Wellens, J., & Hooley, T. (2009). Facebook, social integration and informal learning at university: 'It is more for socialising and talking to friends about work than for actually doing work'. Learning, Media and Technology, 34, 141–155.10.1080/17439880902923606.

Nalewajek, M., & Macik, R. (2013). The role of social media in building awareness of responsible consumption. In Active Citizenship by Knowledge Management & Innovation. Proceedings of the Management, Knowledge and Learning International Conference 2013 (pp. 837–844). Zadar: ToKnowPress.