UNIVERSITY OF
GLOUCESTERSHIRE

This is a peer-reviewed, final published version of the following document, ©2021 The Authors. and is licensed under Creative Commons: Attribution 4.0 license:

Viana, Thiago ORCID logoORCID: https://orcid.org/0000-0001-9380-4611, Hemns, Jessica and Paterson, Julie (2021) Towards a Multidimensional Model to Represent Human Behaviour on Online Social Networks. International Journal of Cyber-Security and Digital Forensics, 10 (3). pp. 91-99.

EPrint URI: https://eprints.glos.ac.uk/id/eprint/10736

Disclaimer

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.

The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.

The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

PLEASE SCROLL DOWN FOR TEXT.

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 10(3): 91-99

The Society of Digital Information and Wireless Communications (SDIWC), 2021 ISSN: 2305-0011

Towards a Multidimensional Model to Represent Human Behaviour on Online Social Networks

T. Viana, J. Hemns and J. Paterson
School of Computing and Engineering
University of Gloucestershire
tviana1@glos.ac.uk, jesshemns@glos.ac.uk, jpaterson@glos.ac.uk

ABSTRACT

Online social networks have been growing exponentially. Everyday loads of new users are immersed into this environment, sharing and interacting using many different methods, tools and devices. However, this ever-growing environment leads to a variety of security and privacy concerns. Addressing this challenge, this paper proposes a discussion on risks and issues that arise from user behaviours on OSNs. To this end, a multidimensional model is presented to support the identification and analysis of such behaviours. This model comprises of three dimensions, namely, (*depth of*) involvement, (*width of*) perception and (*height of*) action. Furthermore, a list of ten possible disclosure behaviour divided into the three dimensions is presented and discussed. This paper analyses how these behaviours can be transformed into Personal Information Disclosure (PID).

KEYWORDS

Human behaviour, OSN, PID.

1. INTRODUCTION

The growth and proliferation of online social networks (OSNs) have led to a dependency on its usage and the development of an OSN ecosystem. Data collected from OSNs is currently being used on different domains including, but not limited to, commercial, marketing, advertising, market trend analysis, education, criminology and governmental. Due to its increasing popularity, as well as its accessibility, OSNs are being used by people of different ages, ethnicity, cultural, social or economic status.

Amongst the many functions provided by different OSNs, Cavazza [1] has presented a social media landscape, dividing them into six categories, namely, Networking, Publishing, Sharing, Collaborating, Discussing and Messaging. Figure 1 illustrates the landscape proposed and shows Google, Facebook and Twitter in the centre of this OSN ecosystem with other OSNs building their solutions based on and supported by them.

As an extract of this complex and ever-evolving ecosystem, Facebook Messenger and WhatsApp alone handle more than 60 billion messages per day [2][3], approximately 510,000 comments are posted, 293,000 status changes are registered, and 136,000 photos are uploaded on Facebook every 60 seconds, 500 million Tweets are sent every day, 3.5 billion likes/day are taken place on Instagram and 56 million blog posts are published on WordPress every month [2][3].

Figure 1. Social Media Landscape [1]

However, this OSN ecosystem can become an ideal environment for the spread of many privacy and security risks. Current research has shown that, whilst using OSNs, many users have revealed a large amount of personal information about themselves [4]. Due to that, OSNs have become a target for cybercriminals and hackers. As a sample of this problem, a recent data scandal involving

Facebook and Cambridge Analytica hit around 78 million users, exposing the lack of OSNs privacy and security measures [5].

In this scenario, questions arise with regards to the growth of OSNs, particularly, when dealing with issues related to privacy and security. Previous research in the area has demonstrated that individual's behaviour on OSNs plays an important part in addressing these issues [6][7][8][9]. Following this path, this paper proposes to investigate and discuss the different behavioural patterns and related privacy issues over OSNs.

2. DIFFERENT BEHAVIOURAL AND PRIVACY ISSUES

One of the most prevalent behaviours displayed by users over OSN is the Fear of Missing out (FoMo). This behaviour is often ignited by the nature of these social networks, with individuals constantly displaying unrealistic portrayals of their lives to enhance feelings of popularity and a sense of belonging [18]. This fear of missing out is typically triggered in a user once they have seen their peers partaking in enjoyable activities through social media while they are absent, causing them to develop anxieties [10] [11]. A serious behavioural issue that FoMo provokes is a dependency on social media and an obsession that reinforces the tendency to stay in constant contact on OSNs, resulting in excessive use that stems from an increased perception of the importance of the OSN and can lead to addictive and dysfunctional behaviours [19] [20]. This dependency can take a toll on the individuals' mental wellbeing, especially if they are feeling socially excluded from their friends online.

This online social exclusion can evoke feelings of worthlessness and lack of self-esteem which in essence causes users to not express any interest or concern about their online safety, making them more susceptible to cyber-attacks [10]. Individuals may also take part in suspicious activities online or use unstable software if their peers are doing so. The feeling of FoMO replaces the rationality that would normally be prominent in an individual because they are more focused on not missing out and so overlook any privacy or security concerns.

Kramer and Schawel [21] reiterate this, stating that OSN users find it difficult to balance the need to self-disclose with the need to protect their privacy, with the latter often losing out to the former regardless of the risks involved of sharing private information with a wider audience. This in turn led to the term privacy paradox [22].

To illustrate the fear of missing out, consider a scenario between two individuals, Mary, and John. Mary follows John on multiple forms of social media and notices that along with their other mutual friends he is posting photos of a new search engine that Mary has never heard of. Mary then experiences the feeling of FoMO due to being left out by John and downloads the search engine with no prior research. Little to Mary's knowledge the search engine was an elaborate scam, and she has now disclosed all her private information to this malicious third party, putting herself at risk.

The development and implementation of online social networks have nevertheless shaped the future of socialising and communication between individuals. This method of social interaction is often used to fulfil a deep-seated need to belong and a need to be accepted by friends on OSNs. This is also often described as the "fear of being rejected and abandoned by others" [11]. This behaviour breeds within an individual once they have established firm social bonds and felt a strong sense of belongingness on OSNs [11], a behaviour that malicious attackers exploit to their advantage. However, this behaviour can expose the individual to issues which can ultimately harm their online privacy and security. PID, also known as private information disclosure, is the act of giving out personal information to others, either with or without consent. With individuals constantly chasing the need to belong, they will tend to share more information about their life on OSNs such as, photos, date of birth, email address, family members, status updates with geolocation, and even their physical home address [12] with people who are not necessarily trustworthy. The severity of this information disclosure can elicit unwarranted actions such as in-person attacks or identity theft. Although Anaraky et al [23] found that older adults were more likely to consider

associated risks and benefits prior to disclosure than younger adults, both age groups nevertheless share personal information when using OSNs, tagging others to support their need to belong and be accepted by the group.

To illustrate the need to belong behavioural theory, consider a scenario between two individuals, Mary, and John. Mary follows John on Instagram and spots that he has 1000 followers, opposed to Mary's 200. Mary experiences the need to belong and wants to prove to herself and others that she can gain just as many, if not more followers than John. Mary changes her privacy settings on Instagram allowing anybody to see her profile and starts following strangers. However, Mary posts images on her Instagram with her geolocation on and tags her family and close friends in posts. Mary has now disclosed her personal information to strangers online putting her at risk in real life through becoming a victim of private information disclosure (PID).

An individual's behaviour on social networks is heavily influenced by their perceived security and privacy online. Despite OSNs constantly producing guidelines on how to stay safe, a high percentage of users remain naïve about their security online. Naivety in this context can be described as a lack of knowledge, experience or judgement regarding social networks and online privacy. As described by [13] "*Past research has shown that users of online social networks tend to exhibit a higher degree of trust in friend requests and messages sent by other users*". This level of trust, alongside user naivety creates an ideal environment for cyber-attacks on OSNs. As soon as an individual is known as technology-ignorant or naïve online, they will be immediately exploited by social engineers [14]. Social engineering is a form of cyber-attack which manipulates vulnerable people and forces them to hand over their possessions such as money, valuables, or private or sensitive information [14]. Common methods of social engineering attacks can be described as; scamming through fake profiles (also known as catfishing), clickbait links, or phishing scams. Once a naïve individual has fallen victim to these social engineering attacks, they may adapt their behaviour and become more concerned with their online privacy and security. However, [24] and [25] found that even with greater threat awareness, individuals did not significantly change their personal information sharing behaviour to protect themselves. Consequently, it is also common for social engineering victims to fall for these scams a second time and accidentally expose themselves and their data again.

To illustrate naivety in individuals, consider a scenario between two OSN users, Mary, and John. John uses Facebook to mainly keep in touch with his family, but one day he received a friend request from Mary, a stranger. John, being the naïve individual, accepts the friend request allowing Mary to communicate with him. Mary then proceeds to send John a message detailing a fake story about her life which includes a link to an unknown source. Without thinking about the consequences John proceeds to click on the link which then allows Mary to execute her attack and download malware onto John's computer. This malware searches through the computer and steals private data, all unbeknown to John. This example details just one consequence of naivety over online social networks.

3. A MULTIDIMENSIONAL MODEL TO REPRESENT HUMAN BEHAVIOUR AND ISSUES RELATED TO OSNS

Knijnenburg *et al.* [6] has demonstrated that privacy issues, such as disclosure behaviour, can be represented as a multi-dimensional problem and different users will present different behaviours in similar situations. Also, recent literature findings have shown that behaviour in OSN can be organised in four stages, namely, 1. Factors that motivate involvement, 2. Privacy concerns, 3. Individual's behaviour when using OSN and 4. Individual's behaviour when facing privacy and security risks [15].

Building on these ideas, this paper proposes the creation of a multidimensional model to support the analysis of different users' behaviours involving privacy and security on OSNs. The proposed model is based on three different dimensions, namely, (*depth of*) involvement, (*width of*) perception and (*height of*) action (Figure 2).

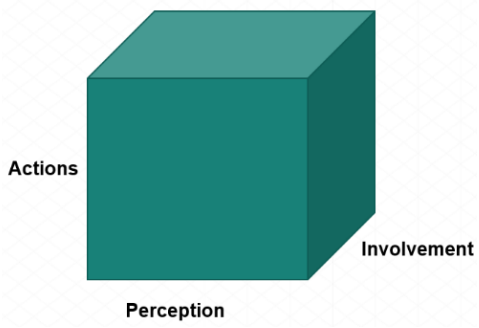

Figure 2. Multidimensional model

More specifically, this model proposes that the usage of such multidimensional representation will be able to support in the identification and analysis of privacy and security issues on OSNs based on different user behaviours.

4. DIFFERENT BEHAVIOURS FOR EACH DIMENSION

Using a multi-dimensional analysis to address the different behaviours displayed by an OSN user it is possible to provide a deeper discussion and evaluation on different triggers and situations that lead to a PID.

For each dimension it is possible to represent different behaviours.

4.1 INVOLVEMENT DIMENSION:

Analysing a user behaviour through the multidimensional model, this dimension represents the depth of involvement that a user has when utilizing a particular OSN. The depth has been chosen to represent the level of involvement a user has with an OSN, the deeper their dependency the less likely their awareness of privacy and security risks will influence their behaviour. As a user digs into his relationship with an OSN, he gets too deep to realise potential dangers, increasing the likelihood of being affected by these issues. Thus, the involvement dimension focuses on the level of involvement a user has when interacting with certain aspects of online social networks.

Therefore, the depth of a user's involvement is likely to affect a user's behaviour and lead to or alternatively prevent a personal disclosure information (PID).

There are many possible behaviours that demonstrated the effect of this dimension. This paper has listed four possible behaviours.

4.1.1 FREE-VALUE FEELING

A common behaviour featured within the involvement dimension is free-value feeling. This behaviour stems from the individual's need to save money or attain a perceived bargin, through for example, using technological software or hardware just because it is free. This behaviour could become problematic if someone values the price of an item over their own security and privacy.

An example of this could be when an individual is deciding to purchase anti-virus software for their device and are debating between a high-end expensive version or a free low-grade option. A user experiencing the free-value behaviour would risk their security by opting for the free version, while a calculated individual would prioritise their privacy and purchase the reliable software.

4.1.2 FOMO (FEAR OF MISSING OUT)

As previously mentioned within this article, the fear of missing out is a prevalent behaviour within the involvement category of the multi-dimensional model. As stated by [10], "*The fear of missing out refers to feelings of anxiety that arises from the realisation that you may be missing out on rewarding experiences*." This anxiety can create a widespread range of issues for an individual, varying from sleep deprivation to personal information disclosure.

One of the most prominent behavioural issues that stems from the fear of missing out is a dependency on technology which can be developed by an individual. This dependency causes the user to value the technological world before their other mental and physical needs such as sleeping, eating, their mental health or their privacy and security. This behaviour can result in an addiction that supersedes all other behavioural patterns to the detriment of the individual. Indeed [26] found that OSN

addiction was related to unhealthy social relationships and reduced life-satisfaction.

4.1.3 NEED TO BELONG

As expressed by [11] the Need to Belong behavioural theory is derived from the "*fear of being rejected and abandoned by others*". This feeling has become more of a concentrated behavioural issue recently due to the uprising of individuals seeking social interaction through technology. As mentioned earlier in this article, the need to belong increases within a user once they have established firm connections and achieved a sense of belongingness with their peers. This can also often be derived from individuals wanting to be part of a society. However, this behaviour can highlight problematic behaviours within an individual including vaguebooking, namely posting potentially alarming messages for attention, which [27] argue can predict suicidal thoughts.

An example of this is, a user compromising their private information through PID (private information disclosure). This can be compromised in multiple ways, but a common example of PID is through using software such as "Find my Friends". This allows users to add themselves and their friends to an application which grants them permission to view where they are at all times. This might have been done to fulfil the need to belong to a social group, but can ultimately cause more harm towards a user.

4.1.4 COLLECTIVE SELF-ESTEEM

Another disclosure behaviour that is a key part of the involvement dimension is an individual's collective self-esteem. This behaviour can be described as, the way someone views themselves based on their role within social groups. These groups can range from different settings such as family members, friends, and online interactions. If an individual has positive interactions within social groups, they may gain a higher level of collective self-esteem, however this may also cause them to attempt to enhance or protect the esteem if ever threatened [16].

On the other hand, a negative social environment may breed a lack of collective self-esteem within a user. This can cause behavioural issues such as low motivation or inadequate mental health.

4.2 PERCEPTION DIMENSION

Analysing user behaviour through the multidimensional model, this dimension represents the width of perception that a user has when utilizing a particular OSN. The width has been chosen to represent the perception as a user's perception can be "*wide*", as in a user being able to see the whole coverage of effects that an OSN can have on his/her privacy and security, or it can be "*narrow*", as in a user not being able to fully comprehend the effects of an OSN on his/her privacy and security.

Therefore, the different ways that a user perceives the same thing is likely to affect a user's behaviour and lead to or prevent a personal disclosure information (PID). There are many possible behaviours that demonstrate the effect of this dimension. This paper has listed three possible behaviours.

4.2.1 PRIVACY AND SECURITY FAÇADE

Transparency is a key principle that should be adopted by everyone, especially in a corporate setting. This establishes trust between the business and customer meaning that users can trust that their data is being handled securely. However, some companies may present a façade regarding how they handle user information.

This tricks the user into thinking that their information is secure, however, the business misleads the individual and has little or no privacy or security measures in place to protect the data. Unbeknown to the user, their private information could be taken from these businesses and stolen by individuals with malintent, creating a vulnerability.

4.2.2 DIFFERENT USES, DIFFERENT PERCEPTIONS

Technology has multiple purposes and can be used for a multitude of activities. An individual's perception of technology can change depending on what they use it for. An example to show this perception behaviour is the type of passwords individuals use for different services online. If a user had to create a password for an online banking account, they may use a secure password, due to the nature of the information stored in that account.

However, the same user could create an insecure password for an account to a bakery webpage as they would assume the nature of the website does not deal with sensitive information. This example demonstrates that an individual's perception of their security changes depending on what they use technology for.

4.2.3 THEY BEFORE ME, COLLECTIVE PERCEPTION

Collective perception is a common behaviour experienced by individuals. This behaviour causes a user's perception to be influenced or changed depending on what their peers believe. Collective perception often overrules a user's individual perception, usually due to the user wanting to please their peers and seeking approval from them.

An example of this is a user downloads kali Linux because all their peers say it's safe, secure, and useful. Although the individual has opposing views, they decide to ignore their own judgement to go with the majority. This collective perception can affect a user's privacy or security as they commonly do not do the research surrounding the item, and blindly trust their peers, who may also not know the potential consequences.

4.3 ACTION DIMENSION

Analysing a user behaviour through the multidimensional model, this dimension represents the height of action that a user has when utilizing a particular OSN. The height has been chosen to represent the action of the user as a user can act differently when presented with similar situations. An action can be "*tall*", as in stronger than needed or "*short*", as in weaker than appropriate for the current situation.

Therefore, the different ways that a user acts or reacts upon the same situation on OSNs is likely to affect a user's behaviour and lead to or prevent a personal disclosure information (PID).

There are many possible behaviours that demonstrate the effect of this dimension. This paper has listed three possible behaviours.

4.3.1 EASY TO USE

Over time individuals have developed a need to find the easiest way to complete tasks and interact with other objects and/or people. In most scenarios, to find the easiest way to interact with something a user will have to potentially sacrifice their privacy or security. This disclosure behaviour is placed within the action dimension of the multidimensional model proposed in this paper because this behaviour stems from actions that individuals make.

An example of this behaviour is the way a user deals with 2 factor authentication (2FA) on social media. An individual might disable 2FA on their device as it is easier to just log onto the application without having to verify their identity. Disabling 2FA may be easier for a user, however it will decrease the amount of security they have protecting their account and all their private data.

4.3.2 PRIVACY SELF-PRESENTATION

A scenario that presents itself within the action dimension is the trade-off between privacy and self-presentation. Self-presentation can commonly be described as how individuals try to present themselves either online or face-to-face to control how others view them. The more information users disclose about themselves, the less privacy they have surrounding their sensitive data.

Since most social interaction between peers is through online social networks, it has revealed a new form of self-presentation, which

can become increasingly damaging to private information [17]. If an individual with a large social media following discloses private information through this method, due to it reaching a wider audience, it can be detrimental to their security and privacy.

4.3.3 PRIVACY LAZINESS

An inherent behaviour displayed within all humans is laziness. An individual's laziness can inadvertently cause them to put their own security at risk. A common example of an action driven by laziness that is shown by individuals online is how they deal with cookies.

Although most individuals experience privacy laziness in their day-to-day life, there is a distinct lack of literature raising awareness on it through technological platforms such as OSNs.

On most web pages nowadays, a pop up will prompt a user to accept or deny cookies being saved. Most users will be too lazy to explore the deny option and will just click accept, without being knowledgeable of the consequences. In other similar situations, the user's laziness and refusal to research small decisions they make could impact their privacy or security.

4.4 SUMMARY

A multidimensional analysis of user behaviours on OSNs is able to support with the identification and understanding of privacy and security issues that lead to PID. Table 1 summarizes a list of different behaviours that can be identified using the three suggested dimensions.

Though this list is not extensive, this multidimensional analysis supports the study on user behaviours and OSNs and how this can play an important part on the discussion of privacy and security related threats in such environments. The model can be used to support research and discussion in the area through the usage of the proposed dimensions and the identified disclosure behaviours.

Table 1. List of different user behaviours leading to PID in each dimension

Dimension	User Behaviour
(*depth of*) Involvement	Free-Value Feeling
	FoMO (Fear of Missing Out)
	Need to Belong
	Collective Self-Esteem
(*width of*) Perception	Privacy and Security Façade
	Different uses, different perceptions
	They before me, collective perception
(*height of*) Action	Easy to Use
	Privacy Self-Presentation
	Privacy laziness

5. CONCLUSION

This paper has discussed different issues related to OSNs and user behaviours. Such behaviours can lead to personal information disclosure (PID) and raise many privacy and security related issues. To support the analysis and understanding of such a problem, this paper has proposed a multidimensional model comprising of three dimensions, namely, (*depth of*) involvement, (*width of*) perception and (*height of*) action. Finally, this paper has catalogued different behaviours that can be analysed and represented on each of the model's dimensions. A total of ten different behaviours have been discussed and analysed based on these three dimensions.

As future works for this research, the proposed multidimensional model will be further analysed through the creation of scenarios and exploratory research on OSNs user's behaviour. Also, the implementation of such a model can be used to predict behaviours that can lead to disclosure and support OSNs users with preventing cyber threats. Also, the model can be used to support research in the area of cyber human factors leading to cyber security risks. Finally, building on this paper, an implementation and test using simulation methods to evaluate the constructs and to access the quality of this behavioural representation.

REFERENCES

1. F. Cavazza, 'Social Media Landscape 2017', *FredCavazza.net*, Apr. 19, 2017. https://fredcavazza.net/2017/04/19/social-media-landscape-2017/ (accessed Oct. 07, 2020).

2. K. Smith, 'Marketing: 96 Amazing social media statistics and facts for 2016', *Retrived from https://www. brandwatch. com/2016/03/96-amazing-social-media-statistics-and-facts-for-2016*, 2016.
3. Zephoria, 'Top 20 Facebook Statistics - Updated August 2020', *Zephoria Inc.*, Aug. 03, 2020. https://zephoria.com/top-15-valuable-facebook-statistics/ (accessed Oct. 07, 2020).
4. M. Aljohani, A. Nisbet, and K. Blincoe, 'A survey of social media users privacy settings & information disclosure', 2016, doi: 10.4225/75/58A693DEEE893.
5. A. Groth, 'Facebook's Data Scandal and Europe's New Data Privacy Rule Have Massive Implications for U.S. Entrepreneurs', *Entrepreneur*, Apr. 02, 2018. https://www.entrepreneur.com/article/311273 (accessed Oct. 07, 2020).
6. B. P. Knijnenburg, A. Kobsa, and H. Jin, 'Dimensionality of information disclosure behavior', *International Journal of Human-Computer Studies*, vol. 71, no. 12, pp. 1144–1162, Dec. 2013, doi: 10.1016/j.ijhcs.2013.06.003.
7. Y. Li, Y. Li, Q. Yan, and R. H. Deng, 'Privacy leakage analysis in online social networks', *Computers & Security*, vol. 49, pp. 239–254, Mar. 2015, doi: 10.1016/j.cose.2014.10.012.
8. R. Shillair, S. R. Cotten, H.-Y. S. Tsai, S. Alhabash, R. LaRose, and N. J. Rifon, 'Online safety begins with you and me: Convincing Internet users to protect themselves', *Computers in Human Behavior*, vol. 48, pp. 199–207, Jul. 2015, doi: 10.1016/j.chb.2015.01.046.
9. J. Angulo and M. Ortlieb, '"WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations', in *Eleventh Symposium On Usable Privacy and Security*, 2015, pp. 19–38.
10. V. Franchina, M. Vanden Abeele, A. J. Van Rooij, G. Lo Coco, and L. De Marez, 'Fear of missing out as a predictor of problematic social media use and phubbing behavior among Flemish adolescents', *International journal of environmental research and public health*, vol. 15, no. 10, p. 2319, 2018.
11. T. L. James, P. B. Lowry, L. Wallace, and M. Warkentin, 'The effect of belongingness on obsessive-compulsive disorder in the use of online social networks', *Journal of Management Information Systems*, vol. 34, no. 2, pp. 560–596, 2017.
12. V. Kisekka, S. Bagchi-Sen, and H. R. Rao, 'Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users', *Computers in human behavior*, vol. 29, no. 6, pp. 2722–2729, 2013.
13. D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, 'Reverse Social Engineering Attacks in Online Social Networks', in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Berlin, Heidelberg, 2011, pp. 55–74. doi: 10.1007/978-3-642-22424-9_4.
14. I. Ghafir *et al.*, 'Security threats to critical infrastructure: the human factor', *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4986–5002, 2018.
15. V. Moustaka, Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. Anthopoulos, 'Enhancing social networking in smart cities: Privacy and security borderlines', *Technological Forecasting and Social Change*, vol. 142, pp. 285–300, May 2019, doi: 10.1016/j.techfore.2018.10.026.
16. J. Crocker and R. Luhtanen, 'Collective self-esteem and ingroup bias.', *Journal of personality and social psychology*, vol. 58, no. 1, p. 60, 1990.
17. S. Mehdizadeh, 'Self-presentation 2.0: Narcissism and self-esteem on Facebook', *Cyberpsychology, behavior, and social networking*, vol. 13, no. 4, pp. 357–364, 2010.
18. Fabris, M.A., Marengo, D., Longobardi, C. and Settanni, M., 2020. Investigating the links between fear of missing out, social media addiction, and emotional symptoms in adolescence: The role of stress associated with neglect and negative reactions on social media. *Addictive Behaviors*, *106*, p.106364.
19. Brand, M., Wegmann, E., Stark, R., Müller, A., Wölfling, K., Robbins, T.W. and Potenza, M.N., 2019. The Interaction of Person-Affect-Cognition-Execution (I-PACE) model for addictive behaviors: Update, generalization to addictive behaviors beyond internet-use disorders, and specification of the process character of addictive behaviors. *Neuroscience & Biobehavioral Reviews*, *104*, pp.1-10.
20. D'Arienzo, M.C., Boursier, V. and Griffiths, M.D., 2019. Addiction to social media and attachment styles: a systematic literature review. International Journal of Mental Health and Addiction, 17(4), pp.1094-1118.
21. Krämer, N.C. and Schäwel, J., 2020. Mastering the challenge of balancing self-disclosure and privacy in social media. Current opinion in psychology, 31, pp.67-71.
22. Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. First Monday.
23. Ghaiumy Anaraky, R., Byrne, K.A., Wisniewski, P.J., Page, X. and Knijnenburg, B., 2021, May. To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-14).
24. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N., 2022. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), pp.82-97.
25. Ortiz, J., Chang, S.H., Chih, W.H. and Wang, C.H., 2017. The contradiction between self-protection and self-presentation on knowledge sharing behavior. Computers in Human Behavior, 76, pp.406-416.
26. Sun, Y. and Zhang, Y., 2021. A review of theories and models applied in studies of social media addiction and implications for future research. Addictive Behaviors, 114, p.106699.

27. Berryman, C., Ferguson, C.J. and Negy, C., 2018. Social media use and mental health among young adults. Psychiatric quarterly, 89(2), pp.307-314.