Privacy and user awareness on Facebook

AUTHORS:
Phillip Nyoni[1]
Mthulisi Velempini[2]

AFFILIATIONS:
[1]Department of Information Systems, North-West University, Mafikeng, South Africa
[2]Department of Computer Science, University of Limpopo, Polokwane, South Africa

CORRESPONDENCE TO:
Mthulisi Velempini

EMAIL:
mvelempini@gmail.com

DATES:
Received: 27 Apr. 2017
Revised: 29 Aug. 2017
Accepted: 07 Dec. 2017
Published: 30 May 2018

KEYWORDS:
social networks; personal data; online profiling; third-party applications; online advertising

HOW TO CITE:
Nyoni P, Velempini M. Privacy and user awareness on Facebook. S Afr J Sci. 2018;114(5/6), Art. #2017-0103, 5 pages. http://dx.doi.org/10.17159/sajs.2018/20170103

ARTICLE INCLUDES:
✓ Supplementary material
× Data set

FUNDING:
North-West University

Users' privacy on social media platforms continues to be important as users face numerous threats to their personal data. Social media sites such as Facebook store large amounts of users' personal data which make such sites prime targets for hackers. Research has shown that users have been subjected to privacy attacks in which hacked personal data are sold to online marketers. These incidents have prompted the need to protect users' privacy against data theft by third parties. We investigated the privacy risks that social media users on Facebook face when online. The privacy awareness of regular users of Facebook was evaluated through the observation of their online activities. Facebook was selected as a case study because it is the largest and most popular social media platform in South Africa. A sample group of Facebook users was selected for this study based on their activeness (or frequency of posting, uploaded or liking) on the site. Findings indicate that users' personal data can be obtained as they are publicly available on Facebook. The implication of this finding is that users lack adequate awareness on protection tools designed to protect their personal data, and as a result, they risk losing their data and privacy.

Significance:

- This study serves as an assessment tool for the privacy and security features of the social media site Facebook. This assessment tool can help users of social media sites to evaluate their own behaviour and usage patterns on Facebook. It can also assist social media site designers in considering the effectiveness of current measures, which are designed to ensure that the privacy and safety of users are protected.

Introduction

I. Social media have attracted robust debate around user privacy as these sites store users' personal data online.[1,2] User-generated content is at the core of Facebook as users share their opinions, personal pictures, location, age or gender.[2] When users share personal data, they do so without an understanding of the risks involved.[2] They assume that Facebook is a trusted computing platform but that is not always the case.[2] For example, hackers can create false accounts or clone user accounts to steal personal data.[3]

II. Third-party applications such as games on Facebook also present a threat to users' personal data.[2,3] These applications can also be used to access sensitive data as they always attempt to access users' Facebook profiles. A users' privacy can then be violated through the third-party application which can publish content using the identity of users which may violate privacy.[4] Third-party applications can profile and track online users' activities.[1]

III. Criminals can also track the movements of users whenever users post their geo-location data on Facebook, and could break into users' properties when they are away on holiday.[5] Facebook has attempted to offer tools for protecting users' privacy but the awareness of users of these tools is still lacking.[2] It is necessary to highlight possible risks associated with such self-disclosure tools.[6] It is envisioned that increased privacy awareness may encourage users to secure their data.[6]

IV. We evaluated users' awareness of their privacy on Facebook. Our aim was to highlight social media privacy risks by using Facebook as a case study. Facebook was selected as it is popular and has been associated with a number of documented incidents of privacy violations. The site also encourages users to search for other users' profiles and add them as 'friends', which may violate their privacy.[3] This open sharing of data is at the heart of this study.

Social media: Facebook

V. Facebook is one of the largest social media sites with 1.28 billion users.[7] There are 50.3 million Facebook users in Africa and 5.5 million users in South Africa – making South Africa the second largest nation of Facebook users in Africa after Egypt (with 13 million users).[8] The site operates by getting users to connect to each other based on their background or shared interests.[2] It also allows them to join groups that have the same likes. Each user signs up for an online profile which contains personal data on the user such as their name and email address.[2] Part of being on Facebook involves users posting status updates which inform others about what they are doing. These updates then appear on their friends' newsfeeds as well as atop the user's feed.[2] These data are available to anyone and are considered to be in the public domain.[9] Because of the type of information posted, it is possible for an attacker to collect and target users based on the personal information they share.[9]

VI. The creator of Facebook has in the past expressed that privacy is not as important as the value that the site offers.[10] Personalised services and targeted advertising on Facebook rely on users' personal information.[10] Tailoring services based on personal information allows companies to segment potential customers and advertise their products.[10]

VII. Previous studies have focused on the usage patterns of university students on Facebook and did not examine the privacy issues faced by these students on Facebook.[9] In this study, we highlight the online privacy issues that users of Facebook encounter and we suggest how these issues may be mitigated.

Personal data and Facebook

VIII. Personal data are data that can be linked to an individual such as location or utility bills.[11] Facebook relies on these data as it needs content that is user generated.[11] Users are willing to disclose very personal aspects of their lives such as holiday trips and recent job promotions.[11] The implications of these data being available include online marketers profiling users or cyber criminals obtaining information on users.[11] Personal data have a high potential for misuse if obtained wrongfully.[11]

IX. A report by the advocacy group Security and Privacy in Online Social Networks[12] in 2015 found that Facebook tracked users' browsing histories, including users who no longer had an account and those who had opted to not be tracked by the site. These direct violations of privacy may lead to users' data being less secure on Facebook[12] and are why it is important for users to be in control of who has access to their data[4].

X. Another scam that has been perpetrated on Facebook involves criminals targeting young teenage users.[13] These young users often share personal details of a trip out of town or a holiday on Facebook (geo-location data)[13]; scammers then call the user's parents pretending to be the police and to have arrested the user in the exact location which they shared on Facebook.[13] The scammers appear to be legitimate as they also provide other information that they have obtained from the user's profile such as age, hometown and school.[13] These scammers then demand money for bail to be sent to a false account. If the parents do not verify their claims, they end up paying and the scam is successful.[13] That such scams are perpetrated using Facebook demonstrates how personal information can be used against users by criminals.[3,5,11]

XI. Data sharing reveals important information about how users interact, which helps third parties to profile users.[11] It is possible for the government to spy on individuals online by accessing their Facebook data.[13]

Data sharing model

XII. An information privacy model developed by Conger[14] lays out the types of relationships that exist between users, website operators (such as Facebook) and third parties (online marketers). This model gives a visual illustration of how personal data can be passed from users to the service provider and then passed onto third parties without user consent.[14] The model is shown in Figure 1.

XIII. Figure 1 shows how privacy can be violated through the sale of their personal data.[1] A lack of awareness of what information is stored about users and how it is used has led to researchers questioning Facebook's approach towards privacy.[14]

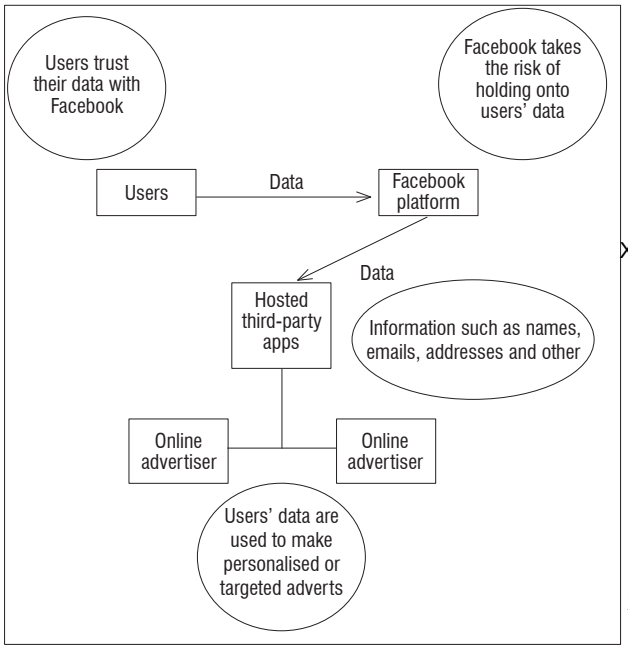

Figure 1: Information privacy model.[14]

Risks users face on Facebook

XIV. Risk is defined 'as a measure of uncertainty of an event happening times the severity of the outcome'[15]. Risk theory has been included here to explain why users may engage in unsafe behaviour online. Users may not be aware of potential threats to the data they post on Facebook. These potential threats include:

- Profiling. Big data analytics can be used against users by marketers or law enforcement agencies to profile them.[15]
- Scams and identity fraud. There have been a number of scams perpetrated on Facebook, from account cloning to users who impersonate officials for the purpose of defrauding individuals.[15]
- Surveillance and cyber bullying. The availability of personal data can be used against users for surveillance or harassment purposes.[15]

XV. Disclosing personal information online has also affected some users in their search for employment.[11] Individuals are subject to background checks before signing employment contracts. These background checks involve reviewing social media accounts such as Facebook. Individuals who post and exhibit online behaviour that a prospective employer finds unprofessional could negatively affect their chances for employment.[11] Those already employed are at risk if they post any negative remarks about their organisation. These risks show how vulnerable personal information is and how users lack awareness of how to protect their personal data.[2] It is also possible that users engage in online self-disclosure as a consequence of ineffective privacy policies.[3]

Defining privacy

XVI. Privacy can be defined in a number of ways, but we adopted the definition provided by Westin[16]. Westin's[16] definition views privacy as the 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'[16]. This definition is supported by Wacks[17] who describes privacy as the desire to be left alone. This view links privacy to the preservation of user identity for individuals.[17] It also highlights the need for users to control their own information, specifically how it is stored and disseminated by service providers.[18] This control can be implemented by giving users options for data minimisation such as a limited data sharing mode.[18] This option would allow users to preserve their privacy and grant them control over their data.[18]

Methodology

XVII. We utilised a mixed-methods approach for data collection. This approach was selected to add depth to the findings.[19] The methodology consisted of an online observation of users on Facebook (which constituted a natural setting). The users were observed using a polling checklist that gathered data from the profiles of users. In addition, a fake account was set up by the researcher to test how easy it is to clone a user's profile. Finally, a short survey was done on users' general awareness of privacy on Facebook. Ethical clearance for this study was given by the North-West University (NWU) Research Ethics Committee (reference number NWU-00212-13-A9).

XVIII. Participants were drawn from NWU stakeholders. The study focused on Facebook because of its wide adoption in Africa and South Africa.[8] It was also considered to be ideal for the study given its publicly available and searchable profiles. The study targeted users who had liked the NWU Facebook page. These users included students, staff, alumni, prospective students, business associates and other stakeholders of the university. NWU was selected as a research site as it has a diverse number of individuals including African students and employees. The international students are approximately 6% of the student body. The findings of the research can be generalised to the broader community of African Facebook users.

Online observation procedure

XIX. The profile pages of users were compared against a polling checklist (see Appendix 1 in the supplementary material) that was organised according to different themes. In total, 357 profile pages were accessed based

on the convenience sample drawn from a population of 5701 users who liked the NWU Facebook page. This sample size was calculated using guidelines provided by Krejcie and Morgan[20]. Their guidelines help researchers find appropriately representative samples from target populations. Data collection took approximately 2 months in total and at least 15 minutes per user.

Facebook account cloning attack

XX. To validate the results of the polling checklist, a fake Facebook profile page was created. The aim of this account cloning attack was to evaluate whether users were able to detect a false account trying to gain access to their account. The attack began by sending out friend requests from the fake account. Once the request was accepted, users were informed about the purpose of the attack. The personal information of the users who accepted the request was made available to the researcher for analysis. A total of 237 users were 'friended'.

User surveys

XXI. Two short user surveys were also conducted. The first survey was based on the polling checklist and the second on the account cloning attack. The surveys were done to support and validate the results of the previous methods. The first survey used convenience sampling to access participants from the population. Questionnaires were distributed to the research participants for completion and were collected as soon as the participants were done. A total of 25 individuals participated. The total number of responses was considered to be sufficient as this short survey was designed to validate the online observation results. The second survey was based on 30 third-year and honours students who volunteered to participate in a cyber security awareness training programme.

Results

XXII. The online observation phase of data collection was based on the users who had liked the NWU Facebook page. The sample population consists of 357 users of whom 55% (n=198) are women and 45% (n=159) are men. The most active users were within the 18–25 year age group (n=214); this finding was to be expected considering that the majority of students using Facebook are undergraduate students.

XXIII. It was also found that 67% (n=240) of Facebook users' personal data are partially available, while 33% (n=117) have their full personal details available (Figure 2). Facebook does not put a default block on new users' personal information when they sign up to be a member on the site, which makes it easier for users to view each other's information, and also makes it possible for those with malicious intent to obtain sensitive data. Attackers seek out user names and passwords for Facebook by data mining those credentials. Other people use that information to deceive or market their products to the users through spam email.

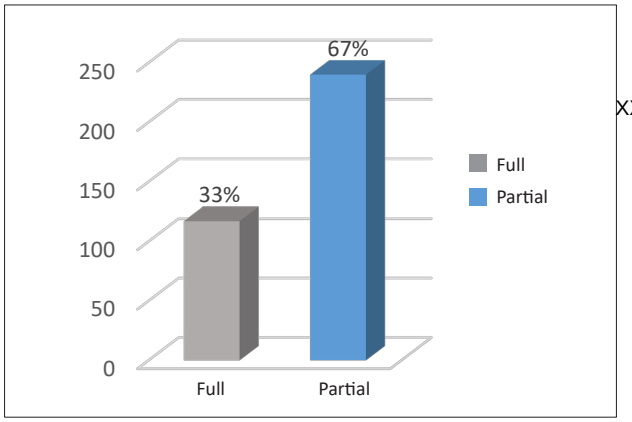

Figure 2: Availability of users' details.

XXIV. Most users' data are partially available on Facebook, possibly because Facebook needs user profiles to be semi-accessible to the public in order for people to connect with users with common interests. The unfortunate side effect of this accessibility is that not everyone wants to be a friend on Facebook.

XXV. Most users (75%; n=269) either often share or sometimes share their geo-location with their friends on Facebook (Figure 3). Most of these users indicated that they share their location when they travel for holidays or when they spend time with friends. Users trust that their data are safe and share their daily activities on Facebook. Criminals can use this information to track users' movements and map their patterns, resulting in a high number of scams on Facebook.

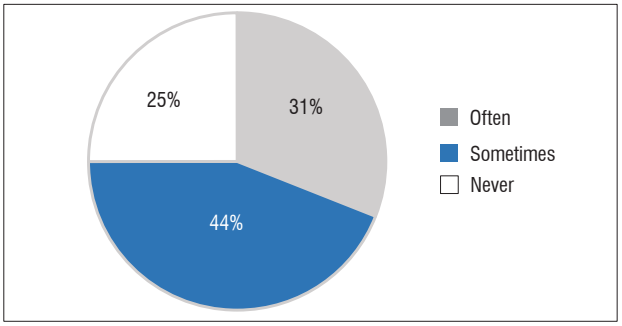

Figure 3: Geo-location sharing by users.

XXVI. Figure 4 shows that 56% (n=202) of users post daily on Facebook, while 38% (n=135) post at least once or twice a week. Figure 4 also reveals that many users access Facebook through their mobile devices as smart devices have global-positioning sensors on them which can share location. Anyone can profile a user's daily routine from the frequency of their updates and location of their postings. Personal data are generated on a daily basis which makes it possible to track and profile such users.

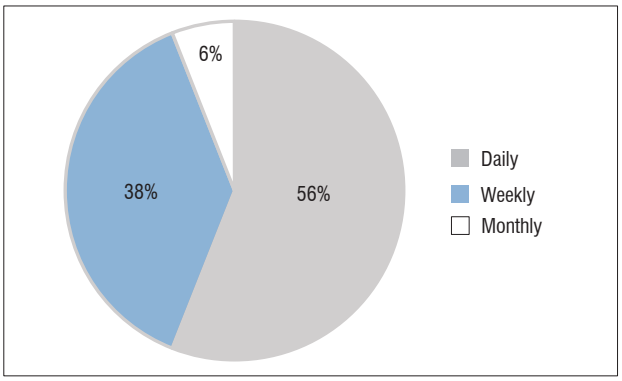

Figure 4: Frequency of user sharing.

XXVII. The most common activity on Facebook is posting status updates (47%), as shown in Table 1; 14% uploaded pictures the most. In some cases, picture or video uploads were personal in nature and displayed a user's car registration number or house number. This practice is not exclusive to Facebook as other sites such as Instagram also have such images.

Table 1: Frequency of user activity

Activity	Frequency
Posting	169 users (47%)
Commenting	70 users (20%)
Liking	68 users (19%)
Uploading	50 users (14%)

XXVIII. Some users also post pictures of friends and Facebook's facial recognition feature tags them automatically without their consent.[13] These pictures can be digitally altered or used for cyber bullying (using the user's image for online jokes or memes) or for propaganda in the case of a public figure.[13] These practices can damage a user's reputation unless the user quickly un-tags themself from the image.

Facebook account cloning attack

XXIX. An account was cloned and used to see if users could be lured by a fake account. Friend requests were sent out and as users responded, they were informed about the objective of this profile. The response rate to this page is shown in Figure 5. A total of 87 out of 237 users had accepted the invitation at the time the results were retrieved. This attack was run over the course of 1 month.

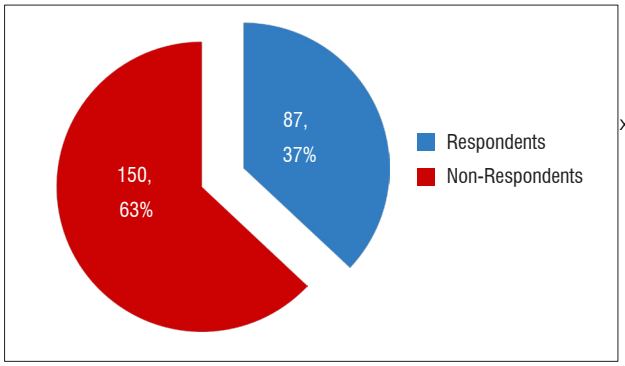

Figure 5: Response rate to a friend request from a fake account.

XXX. The users who responded did not verify the personal details to assess the veracity of the profile page. For example, users did not realise that the profile name and the name of the owner had been modified. It is common practice for Facebook users to either misspell their names purposely or use pseudo-names because they want to hide their identity, but this practice can also lead to users being tricked into accepting account impersonators. The attack indicates that a number of users on Facebook still lack privacy awareness.

User surveys

XXXI. A short user survey was conducted to examine the privacy awareness of Facebook users. The respondents (n=25) confirmed that they had a Facebook profile and were active on it. Of the 25 respondents, 20 agreed that they shared personal data on Facebook. These data consisted of addresses and travel plans which could be exploited by attackers. Most respondents admitted that they frequently uploaded pictures, 13 changed their status regularly, 10 commented and 7 respondents shared their location often – a finding which supports the results of the online observation regarding geo-location sharing. The results of the survey are shown in Figure 6.

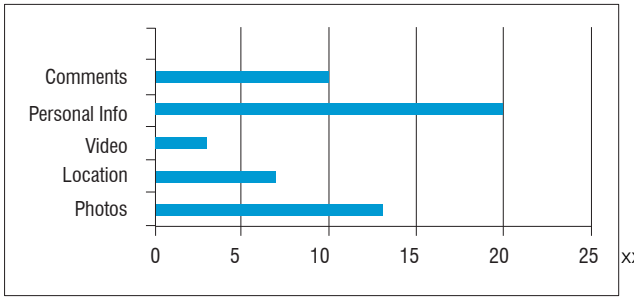

Figure 6: Information shared on users' profiles.

XXXII. Figure 7 shows that 22 (88%) respondents never use Facebook privacy settings to protect their data. This may be because users do not know that these settings exist or may not know how to activate them, which may leave their personal data vulnerable to any potential profiling.

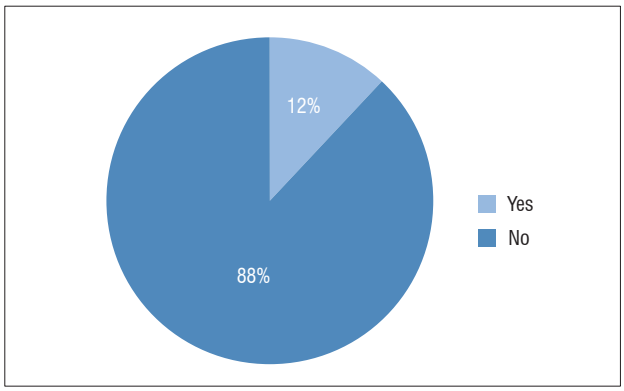

Figure 7: Privacy settings usage.

XXXIII. The second short survey was to investigate whether users were willing to meet someone they connected with on Facebook. A total population of 30 students were asked how they would respond to a request to meet in the real world. The results showed that 41% (combined from 33% and 7%) were willing to meet in person a Facebook friend who they had never met before (Figure 8). This willingness to trust a total stranger may lead to the users being defrauded or scammed by impersonators on Facebook.[5]

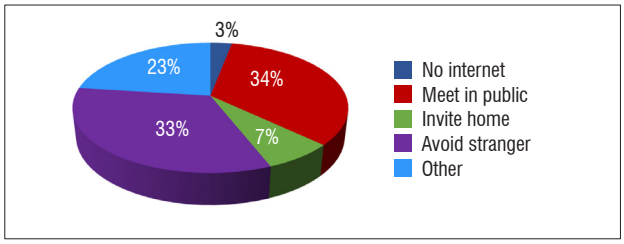

Figure 8: Willingness to meet with a stranger friended on Facebook.

Discussion

XXXIV. Based on the findings of this study, it is necessary for users to be trained on privacy settings on Facebook. Metadata (such as location) accompany posts and uploads that users create online and these 'extra data' can be used for surveillance or profiling purposes. While Facebook uses these metadata to tailor adverts that users see, they may also be misused by third parties. Someone could break into a user's home after obtaining the information on Facebook and studying their movement patterns from geo-location tags.

XXXV. Facebook does have a comprehensive privacy policy in place to deal with some of these challenges. It covers issues such as how data are used, shared, viewed, changed, or removed.[21] Facebook also tries to elicit feedback from users concerning the policy in order to improve it and make it more effective.[21] However, the privacy policy is long and written in technical language which is not easily understood by most users. The policy highlights that privacy is a shared responsibility and users need to be proactive as well. Despite this policy, many users are not aware of this contractual obligation and do not use privacy settings to secure their data.

XXXVI. A conceptual model that reflects privacy and personal information on Facebook has been developed and is shown in Figure 9. It was developed using the findings of the online observation, account cloning attack and user surveys. The aim of this model is to highlight the roles and responsibilities of users, site providers (Facebook in this case) and third parties (i.e. online marketers).

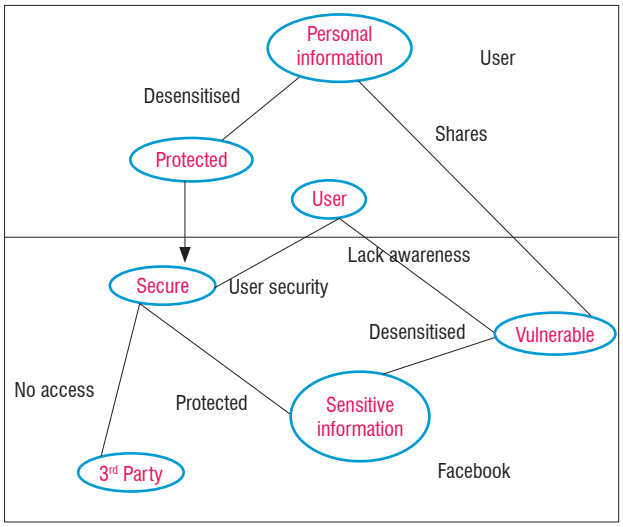

Figure 9: Model of the responsibilities of online actors.

XXXVII. The actors have a shared responsibility to protect and maintain the privacy of data. Users should make use of privacy settings to secure their data whenever they are online. Meanwhile Facebook is responsible for the provision of a secure platform and the enforcement of its privacy policy. Third parties must also ensure that personal data are not stolen or misused. Pro-activeness is necessary for each of these responsibilities to be achieved.

Conclusion

XXXVIII. This study has revealed that users regularly post sensitive data, which can be used to track their movements and activities. Most users are not aware that their posts and updates are in the public domain and can be easily accessed. It is necessary to raise users' privacy awareness to protect them from possible loss of property or surveillance. Privacy settings on Facebook should be simplified for users to understand and given more emphasis so they are used. It is also important for laws that protect users' data to be enforced by regulators. Based on our findings, privacy awareness could be achieved through better user training on how to use privacy settings on Facebook. Users must be taught the different ways in which they can secure their personal information.

Acknowledgement

We thank North-West University for supporting this study.

Authors' contributions

P.N. was responsible for conceptualisation of the study, methodology, data collection, data analysis, sample analysis, validation, data curation, and writing the initial draft. M.V. was responsible for conceptualisation, methodology, student supervision, project leadership, critically reviewing the initial draft and the revisions, and acquiring the funding.

References

1. Titiriga R. Social transparency through recommendation engines and its challenges: Looking beyond privacy. Econ Inform J. 2010;15(4):147–155.
2. Kumar DV, Varma P, Pabboju SS. Security issues in social networking. Int J Comput Sci Netw Security. 2013;13(6):120–124.
3. Malik H, Malik AS. Towards identifying the challenges associated with emerging large scale social networks. Proc Comput Sci. 2011;5:458–465. https://doi.org/10.1016/j.procs.2011.07.059
4. Spinelli CF. Social media: No 'friend' of personal privacy. The Elon Journal of Undergraduate Research in Communications. 2010;1(2):59–69.
5. Blair K. New survey: Burglars use social media to plan crimes [webpage on the Internet]. c2011 [cited 2016 Nov 25]. Available from: http://socialtimes.com/new-survery-burglars-use-social-media-to-plan- crimes_b79475
6. Balduzzi M, Platzer C, Holz T, Kirda E, Balzarotti D, Kruegel C. Abusing social networks for automated user profiling. In: Jha S, Sommer R, Kreibich C, editors. Recent advances in intrusion detection. RAID 2010. Lecture Notes in Computer Science. 2010;6307:422–441. https://doi.org/10.1007/978-3-642-15512-3_22
7. Digital Insights. Social media statistics for 2014 [webpage on the Internet]. c2014 [cited 2016 Apr 14]. Available from: http://www.adweek.com/socialtimes/files/2014/06/social-media-statistics-2014.htm
8. Social Bakers. Africa Facebook users infographic [webpage on the Internet]. c2013 [cited 2016 Nov 20]. Available from: http://www.socialbakers.com/africa-facebook-users-infographic.jpg
9. Pempek TA, Yermolayeva YA, Calvert SL. College students' social networking experiences on Facebook. J Appl Dev Psychol. 2009;30(3):227–238. https://doi.org/10.1016/j.appdev.2008.12.010
10. Johnson B. Privacy no longer a social norm says Facebook founder [webpage on the Internet]. c2010 [cited 2016 Oct 01]. The Guardian. 2010 January 11. Available from: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy
11. Furnell SM. Online identity: Giving it all away? Information Security Technical Report. 2010;15(2):42–46. https://doi.org/10.1016/j.istr.2010.09.002
12. Security and Privacy in Online Social Networks. From social media service to advertising network: A critical analysis of Facebook's revised policies and terms [document on the Internet]. c2015 [cited 2016 Sep 14]. Available from: https://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf
13. Payton T, Claypoole T. Privacy in the age of big data. Lanham: Rowman & Littlefield; 2014.
14. Conger S. Emerging technologies, emerging privacy issues. In: Luppicini R, Adell R, editors. Handbook of research on technoethics. Hershey, PA: IGI Global; 2009. p. 767–793. https://doi.org/10.4018/978-1-60566-022-6.ch050
15. Riesch H. Levels of uncertainty. In: Handbook of risk theory. Amsterdam: Springer; 2012. p. 87–110. https://doi.org/10.1007/978-94-007-1433-5_4
16. Westin A. Privacy and freedom. New York: IG Publishing; 1967. p. 15–20.
17. Wacks R. Privacy: A very short introduction. New York: Oxford Press; 2010. https://doi.org/10.1093/actrade/9780199556533.003.0001
18. Ellison N, Vitak J, Steinfield C, Gray R, Lampe C. Negotiating privacy concerns and social capital needs in a social media environment. In: Trepte S, Reinecke L, editors. Privacy online. Berlin: Springer; 2010. p. 19–32.
19. Hesse-Biber SN. Mixed methods research: Merging theory with practice. New York: Guilford; 2010.
20. Krejcie R.V, Morgan D.W. Determining sample size for research activities. J Educ Psychol Measure. 1970;30(608):56. https://doi.org/10.1177/001316447003000308
21. Facebook. Privacy policy of Facebook [webpage on the Internet]. No date [updated 2014; cited 2016 Apr 14]. Available from: http://www.facebook.com/policies/privacy/basic/?ref_component