Data protection laws and privacy on Facebook

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

Affiliation:
[1]Department of Information Systems, North-West University, South Africa

[2]Department of Computer Science, University of Limpopo, South Africa

Correspondence to:
Mthulisi Velempini

Email:
mvelempini@gmail.com

Postal address:
Private Bag X1106,
Sovenga 0727, South Africa

Dates:
Received: 23 Aug. 2014
Accepted: 15 Apr. 2015
Published: 10 July 2015

How to cite this article:
Nyoni, P. & Velempini, M., 2015, 'Data protection laws and privacy on Facebook', *South African Journal of Information Management* 17(1), Art. #636, 10 pages. http://dx.doi.org/10.4102/sajim.v17i1.636

Background: Social networks have changed the way people communicate. Business processes and social interactions revolve more in the cyber space. However, as these cyber technologies advance, users become more exposed to privacy threats. Regulatory frameworks and legal instruments currently lacking a strong cyber presence are required, for the protection of users.

Objectives: There is need to explore and evaluate the extent to which users are exposed to vulnerabilities and threats in the context of the existing protection laws and policies. Furthermore, to investigate how the existing legal instruments can be enhanced to better protect users.

Method: This article evaluates and analyses these privacy challenges from a legalistic point of view. The study is focused on the South African Facebook users. Poll information gathered from the profile pages of users at North-West University was analysed. A short survey was also conducted to validate the poll results. Descriptive statistics, including measures of central tendency and measures of spread, have been used to present the data. In addition, a combination of tabulated and graphical description data was also summarised in a meaningful way.

Results: The results clearly show that the legal frameworks and laws are still evolving and that they are not adequately drafted to deal with specific cyber violation of privacy.

Conclusion: This highlights the need to review legal instruments on a regular basis with wider consultation with users in an endeavour to develop a robust and an enforceable legal framework. A proactive legal framework would be the ideal approach unfortunately; law is reactive to cyber-crimes.

Introduction

The content of Web 2.0 is largely user generated and site owners and operators are not fully in control of the content rendered by their sites (Mansfield-Devine 2008). Unfortunately, the user generated content may be used in ways for which it was not originally intended. It is important to note that social media generates a lot of personal information on individual profiles. Furthermore, third party applications that facilitate the exchange of information have the ability to access profile information for individuals and associate it with their identities (Gartrell, Han & Beach 2008).

Social networking websites (for example Facebook and Twitter) have gained popularity in recent years. Facebook alone has grown to 1.28 billion users who spend a considerable time on social networks each day (Digital Insights 2014). These sites are part of the larger trend of websites whose content is user generated. Social media users are increasingly concerned about what personal information they may reveal when online and how it can be used. Of concern are third party organisations that derive revenue from personal information collected on websites (Gartrell *et al.* 2008).

Most users are concerned about their privacy, which they feel is under threat more than ever, given the advances in technology. Databases and Internet records containing private data such as financial statements, medical records and mobile calls do exist. Interestingly users have no knowledge of the existence of multiple data stores of their personal information, who is able to access them and how the information is used. They also do not have control over these data stores (Gartrell *et al.* 2008). This lack of awareness of what information is stored about users and how it is used has led many users to question Facebook's approach to privacy.

This research seeks to examine the data protection laws that are designed to help secure the privacy of users in South Africa. Given the risk of disclosing personal information online, users need to be made aware of the policies and legal instruments that have been drafted to protect them. The awareness will give users a safer social network experience. The article also examines possible areas where these laws can be reconfigured and enhanced to better protect users, whilst enabling the owners of these sites to continue providing their services in an optimal and secure manner.

The article is organised into the following sections: a literature review on privacy, social networks and the law and data protection laws applied in different regions in the world. It then discusses the methodology employed to gather data from profile pages of students of North-West University and how this data were analysed. A combination of graphical description as well as tabulated description with statistical analysis is also presented. The article concludes with guidelines and recommendations.

Related work

Privacy, social networks and the law

According to the Information Security Group of Africa (2011) privacy is, 'the appropriateness of the use of personal information and depends on a number of factors such as context, regulatory requirements, the individual's expectations as well as the right of an individual to control how their personal information is used or processed'. Privacy therefore concerns the control individuals have over information relating to them. This control is linked to users' ability to decide on the amount of visibility and online presence.

Privacy can also be viewed as informational self-determination – the right to determine who accesses one's personal data. This interpretation is widespread in Europe (Stahl 2000). Self-determination can be wielded in various ways, for example users can be granted the right (through legal channels) to know when their personal information is collected, the right to decide how their information may be used, for what purposes and by who. The right to decide on information release is the right that many online users lack. Thus, privacy will exist when the usage, release and circulation of personal information can be controlled (Information Security Group of Africa 2011).

A different perspective is that privacy is in fact a form of property. If personal information can be treated as property, then privacy issues can be reduced to more established (intellectual) property laws (Spinello 2000). If it is treated as a form of property, users should be entitled to legal rights to privacy. It is a means of generating value for not only the generators of information, but also those who collect and sell it to other parties. Using this metaphor, it becomes clear that it requires legal protection in the form of comprehensive legislation from the public sector regulators (policymakers and advocates) and the private sector regulators (businesses and consumers) (Spinello 2000).

Various countries have implemented varying degrees of privacy legislation, which has been designed to control how companies access and utilise information about potential customers. America has had a relatively business-friendly, minimal intervention approach encouraging organisations to provide self-regulated privacy protections. By contrast, the European Union has taken a pro-consumer approach with tough regulations banning the use of personal information until consent is received from users (Turner & Dasgupta 2003). Each approach has its benefits and drawbacks. For example, letting the service providers self-regulate will allow for innovation amongst the competing companies with the users rewarding the site operators with best protection privacy laws. Meanwhile, having the government intervening might be necessary given the fact that outside regulators often have better understanding of what constitutes abuse and privacy violation than the companies within the ecosystem. The ultimate aim of either approach is the effective mitigation of privacy issues, which promotes increased user participation, thus improving revenue for online business initiatives and facilitating future growth in the international e-commerce market place.

Some sectors of the online community, however, challenge the involvement of government, arguing that privacy is the sole responsibility of users. The understanding is that users willingly enter into agreements and contracts with companies for the protection of their data (Smith 2004). It is unfortunate that users do not read extensive and comprehensive agreements. This means that individuals would have to possess a greater awareness of and appreciation for personal data. If one considers Smith's (2004) argument, it is evident that he is advocating for users to ensure that their personal information is managed effectively by service providers. Users are therefore expected to lobby individual companies that provide weaker protection mechanisms.

The activities of users can be easily tracked online without the awareness or permission of users, thereby violating the privacy rights of users. Depending on how this information is used, it can later damage or ruin one's reputation, costing one employment or a political office (Warren 2008). Therefore, getting users personally involved in the protection of their privacy is vital in ensuring that violations can be quickly dealt with.

Although there are laws designed to protect the privacy of individuals, many individuals risk their privacy by willingly posting personal and damaging information online (Warren 2008). Research to date has shown that privacy is the responsibility of individuals (Fogel & Nehmad 2009), whilst others are of the view that privacy is the responsibility of companies (Mishra 2008).

Privacy legislation

The Internet is a disruptive technology that has brought about many challenges. One of those challenges has been the protection of privacy, which is generally accepted as one of the main issues of computer and information ethics (Stahl 2000). New technologies raise a number of issues for privacy protection. Whilst participating in online communities (social networks) it is possible for individual users' actions to be tracked without the users' awareness or permission and this presents a threat to the very principles of freedom and openness that the Internet was founded on (Stahl 2000).

Facebook currently operates under its own set of terms and conditions. This means that without sufficient oversight the ecosystem can become very toxic with many dangers for users to watch out for. Facebook attempts to inform its users about changes in its privacy policies, but most users find it difficult and time consuming to read and understand privacy policies. It is even more difficult to figure out how to request that the use of one's personal information be restricted. Privacy concerns are making consumers nervous about going online, but current privacy policies for sites tend to be so long and difficult to understand that consumers rarely read them (Mishra 2008). This is when government legislation becomes necessary: when site operators can no longer effectively ensure user privacy.

The most pervasive individual Web privacy concerns stem from the secondary use of information, defined as personal information collected for one purpose and used, subsequently, for a different purpose (Mishra 2008). According to a report by Mishra (2008):

1. Users are more willing to provide personal information when they are not identified.
2. Some information is more sensitive than others.
3. The most important factor is whether or not the information will be shared with other companies. Users dislike unsolicited communications and any form of automatic data transfer (n.p.).

The privacy challenge has been sensitised by privacy advocates lobbying governments for user protection. They have also established protection laws and regulations in an endeavour to address the privacy challenge. However, the philosophical concepts of privacy, which are not easy to identify yet are fundamental, remain a challenge in drafting privacy-related legal instruments (Stahl 2000). These concepts have been alluded to previously as viewing privacy as property or informational self-determination. However, there are a clear set of common activities that are undoubtedly privacy invasions:

1. The collection and analysis of user data without the user's knowledge, consent or authorisation.
2. Employing of user data in a way other than for which it was intended or authorised.
3. Disclosing, sending or sharing user data without the user's knowledge and permission.

Given all these possible privacy violations, most users want to be informed about what information is being collected, how it will be used and whether the information will be used for the express intent only. Users are less likely to perceive business practices as privacy invasive when they perceive that information is collected in the context of an existing relationship, is relevant to the transaction and will be used to draw reliable and valid inferences and that they have the ability to control its future use (Baker 1991).

Development of data protection legislation in the United States of America

Privacy has been recognised as an important issue affecting business and users and its significance has continued to escalate as the value of information continues to grow. The United States (US) government is encouraged to take responsibility in protecting users from corporate abuse by enforcing appropriate legislative instruments (Mishra 2008).

Privacy legislation in the US had its beginnings in Congressional hearings held in the 1970s, in which privacy advocates sought to ban credit bureaus from using centralised computer databases, leading to the recognition that both organisations and users have responsibilities regarding information collection and use (Mishra 2008). Since 1973, fair information practice principles have served as the basis for establishing and evaluating US privacy laws and practices.

These principles consist of:

1. notice and awareness
2. choice and consent
3. access and participation
4. integrity and security
5. enforcement and redress.

There is general consensus that organisational privacy policies should reflect these principles. Privacy violations that still occur today prove though that this is not always the case. The US has had a relatively business-friendly, minimal intervention approach encouraging organisations to provide self-regulated privacy protections (Turner & Dasgupta 2003). This may explain why most social media sites are not held accountable for violations as they are registered companies in the US. This is changing however as the US government seeks to secure the homeland through the mass surveillance of its citizens and tracking of their online communications (Craig & Ludloff 2011).

Development of data protection legislation in the European Union

During the early 1980s the Organisation for Economic Cooperation and Development (OECD), issued guidelines similar to the ones the United States produced on the protection of privacy and trans-border flows of personal data (Mishra 2008). The OECD guidelines are the current best-practice global standard for privacy protection and are the recommended model for legislation in member countries. Although not legally binding, the guidelines are recognised by all OECD members, especially the European Union (EU) and the US. They are implemented, however, differently by individual members, suggesting that privacy views differ between countries (Turner & Dasgupta 2003).

As the EU developed their privacy legislation in 1995, they produced their own legal document – the Directive on Data Privacy. It places the responsibility only on companies and organisations, which should seek permission before using personal information for any purpose. The EU has taken a pro-user approach with tough regulations banning the use of personal information until consent is received from users (Turner & Dasgupta 2003). EU directives that are based on the OECD guidelines have been noted to be stricter and more comprehensive with respect to privacy than in the US (Mishra 2008).

The EU is restricting the operation of US companies unless they fall in line with the EU guidelines and it is estimated that 90% of US companies have not addressed the EU directive. An example of one of the directives is that companies are required to inform customers when they plan to sell their personal information to other firms (Kruck *et al.* 2002). Hence the occasional lawsuits for antitrust in the EU against search engines like Google. These suits show that it is indeed possible to charge large corporations such as Google or Facebook for any violation their business practices are causing within the country or region they are operating in.

Development of data protection legislation in South Africa

As mentioned before, in Europe, modern privacy legislation has been maturing since 1981, with the establishment of the Convention for the Protection of Individuals. In the US the approach that informed the establishment of privacy legislation followed a more disparate path. The foundation of commerce in the US is based on the laissez-faire principle (a free-flowing private transactional engagement, without state intervention) and, as such, the various states in the US regulate themselves independently (Information Security Group of Africa 2011).

In South Africa, a new *Act* was signed into law on 26th November 2013 and it is officially known as the *Protection of Personal Information Act* (PoPI). This law protects individuals as it prosecutes organisations and third parties that fail to secure private and personal information such as identity and contact details (Ministry of Justice and Constitutional Development 2013).

The PoPI has been created to enable global commerce and cross-jurisdictional information flow. In order to understand and appreciate the boundaries of the right of privacy and to balance privacy with other competing rights in the Constitution of South Africa, it is important to place privacy in the economic and political context in which personal information is used (Ministry of Justice and Constitutional Development 2013).

Protection of Personal Information Act

Background

The PoPI seeks to give effect to the right to privacy as explained in the Constitution by introducing measures to make sure that all organisations working within South Africa process personal information in a fair, responsible and secure manner (Ministry of Justice and Constitutional Development 2013). It requires that personal information be processed in line with the following guidelines:

1. Accountability.
2. Purpose specification.
3. Security safeguards.
4. Data subject participation (KPMG 2009).

The Act seeks to protect privacy by:

1. Protecting personal information processed by public and private bodies.
2. Ensuring the implementation of information protection principles as minimum requirements for the processing of personal information.
3. Providing for the establishment of an information protection regulator.
4. Providing for the issuing of codes of conducts.
5. Providing for the rights of persons regarding unsolicited electronic communications and automated decision-making (Information Security Group of Africa 2011).

The tenets of the *Act* will help to protect user privacy in various ways. For example, the establishment of an information protection regulator is most welcome. This will ensure that service providers will be held accountable for any data privacy violations. The efficacy of the regulator will depend on how swift it can respond to complaints and the compliance measures it will administer (Ministry of Justice and Constitutional Development 2013).

Impact of PoPI

Facebook already operates in territories where data protection laws are established but has since spread to territories where its operations and its privacy implementations are not regulated (KPMG 2009). With the introduction of PoPI, Facebook will be held accountable as much as it is in the US and the United Kingdom. According to the core principles of PoPI, there must be reasonable processing of personal information in a manner that is consistent with the guidelines set out in the *Act*. The *Act* also applies to third parties that store and process information (KPMG 2009).

The effectiveness of PoPI in the social media has not been investigated. It is envisioned that its effectiveness will be subjected to public scrutiny by the research community in the near future. Its introduction has generated a lot of interest in social networks and security. However, the *Act* is still new, having been signed into law on 26 November 2013, and to date there are no cases that have been prosecuted under it.

Framework

This study utilised the mixed-method approach to data collection. This approach was chosen as it allowed for the subject matter to be viewed from a variety of angles. The participants were drawn from the students pursuing their studies at North-West University (NWU) who have liked the official NWU Facebook page. Facebook was chosen as a representative social network site largely because it commands a huge following. It is the largest social media site with 1.2 billion users (as of 2014), a number which is steadily growing (Digital Insights 2014).

Profile page polling

The profile pages of each participant were compared against a set checklist that covers different aspects of the users' activities on the social media platform that are sensitive in nature. These sensitive activities may be violated in the absence of privacy laws. In total, 357 user profiles were targeted for this study based on the convenience sample. Data collection took over two months as each page required on average 15 minutes to analyse and evaluate.

The sample population was selected from the students who have liked the official NWU Mafikeng campus Facebook page, which had 5701 likes from students, lecturers and other stakeholders from the university community when the data was gathered.

Every user on the social networking website Facebook has a profile page containing the user's personal information. The sensitive data were gathered from these profile pages. Each of the 357 user profiles on Facebook was scrolled through by the researcher using a framework that acted as a checklist to assess each user's privacy awareness. This data are in the public domain and in this work the names of users are not used for ethical reasons. Furthermore, this research has an ethical clearance certificate.

It took on average 15 minutes to gather basic user information such as name, address and place of work. The framework was filled in, matching the observed data (which was freely available over the public domain – Facebook). Each profile would have data covering the individual's likes, friends, location information and activities, which were recorded using the framework. This process was repeated for each participating user.

The sample size of 357 users was used based on a number that has been obtained from suggested sample sizes (Krejcie & Morgan 1970). Convenience sampling was used here due to the accessibility and proximity of the target population. All participants were currently enrolled at the university and have their personal data available on Facebook.

Survey

Furthermore, a short survey was developed based on the questions used in the poll to confirm the results of the framework – the checklist instrument. The survey was based on convenience sampling in which students who were willing to participate were targeted for a quick response. The survey had seven questions and was distributed to 70 participants; it was designed to support and confirm the findings of the main research instrument, the checklist.

Data instrument

The checklist framework was utilised to profile users by capturing their details on Facebook. It was designed to cover the privacy and data protection concepts of the research. The survey utilised a short questionnaire with questions that covered data protection and the awareness of users regarding legislation protecting them online.

Results

Demographics

Figure 1 shows the gender composition of the sample population which was chosen for this study.

It was observed that 55% (*n* = 198) of the participants were female whilst 45% (*n* = 159) were male (see Figure 1). The most common age represented was between 18 and 25 (*n* = 214), as depicted in Figure 2. This was expected considering that the majority of students in the sample population were undergraduate students.

As shown in Figure 2, young people are the most vulnerable age group as they are the most active group on Facebook. This

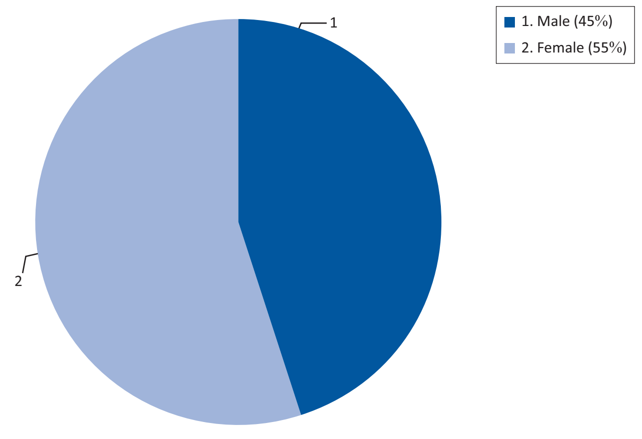

FIGURE 1: User gender.

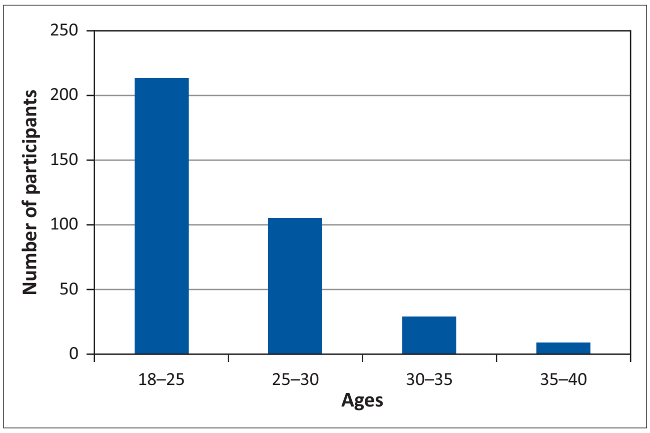

FIGURE 2: Ages of participants.

means that on a more regular basis they are creating personal information about their location, movements, activities and who they spend time with. This sensitive information is publicly available and can be violated by criminal elements and third parties (Gartrell *et al.* 2008).

Users' personal information and self-disclosure

Availability of user details

Figure 3 shows that of the users polled for this study, 67% (*n* = 240) have partially available sensitive information (name, email address or contact numbers) online whilst 33% (*n* = 117) have their full details available (name, email address, contact numbers, address, high school, status, etc.). This is largely because Facebook does not protect personal information of users. The main objective of Facebook is to encourage users to find friends and view other users' profiles.

The fact that most users have their data partially available on Facebook (name and email address or contact numbers) is an indication that Facebook aims to make personal information publicly available (Warren 2008). It is unfortunate that this may result in privacy violations. Furthermore, some users who want to interact only with their friends on Facebook, run the risk of having their posts seen by users who are outside their circle of friends, given the connectedness of Facebook. This violates the privacy of such individuals. On the other hand, some users could use this information for malicious purposes.

Sharing of geo-location

Interestingly, according to the findings of this study, Table 1 illustrates that 31% of Facebook users (*n* = 110) often share their geo-location information with friends on Facebook. The geo-location information ranges from destinations visited, restaurants visited, holiday trips, hotels and accompanying friends. This is based on the level of trust these users have with their friends on the social network. As a result such sensitive information is shared publicly at one's own risk. This can lead to users being targeted by criminals who track their activities via social networks (Blair 2011). The remaining 44% of the sample population (*n* = 157) occasionally share limited geo-location information, such as country or city visited, without sharing the specific location like hotel, with the sole purpose of alerting their friends of their visits. Many users access Facebook on mobile platforms, where location sharing is a by-product of posting anything on Facebook (Clooke 2013). Location information can also be shared without the consent of a user. Only 25% of this sample do not share their location on Facebook. These could be desktop users or users who deactivated the geo-location feature on Facebook.

Method of access

According to the findings demonstrated in Figure 4, 57% (*n* = 205) of users access Facebook using desktop computers and 43% (*n* = 152) use mobile devices (smartphones or tablets) to access Facebook.

This generation of users prefer to log onto Facebook and 'inbox' (send messages) each other in order to communicate, with the added advantage of being able to share multimedia such as photographs, audio and video (Mourer 2014). Unfortunately, some multimedia data contain sensitive information such as physical addresses and vehicle registration numbers.

According to this study 43% of the users access their profiles through their smartphones. This could explain why their geo-location is automatically updated and loaded onto Facebook as metadata. Most smartphone operating systems now incorporate GPS software that allows smartphone owners to share their location with apps like Facebook Messenger. Whilst these apps inform users that this is how they work, most users may not be aware of how this makes them vulnerable. If a user goes online and posts a comment or uploads a picture, their location becomes a part of that post or upload. If the user simply feels like checking in (a term Facebook uses for those who wish to simply state where

TABLE 1: Sharing of geo-location.

Frequency of geo-location sharing	User %
Often	31 (110 users)
Sometimes	44 (157 users)
Never	25 (90 users)

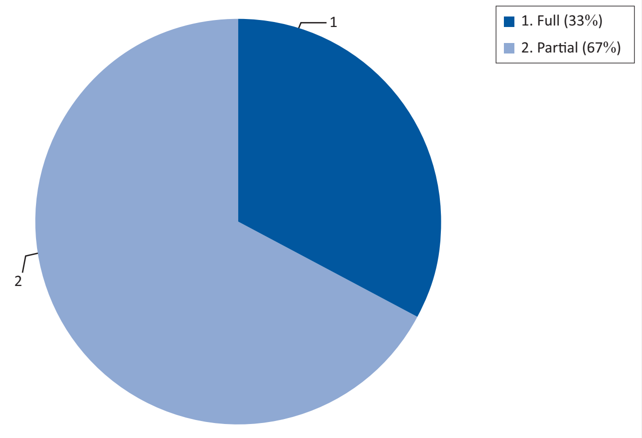

FIGURE 3: Availability of user details.

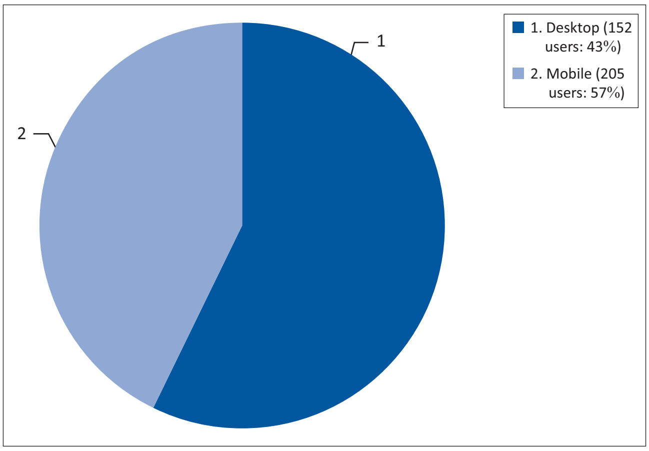

FIGURE 4: Method of access.

they are) then they can do so and the information will be seen by other Facebook users as a post (Clooke 2013).

The availability of geo-location enables third parties to package location-specific commercial advertisement and deliver them to target users (Clooke 2013). However, this can be perceived as annoying and an invasion of one's privacy. Checking in on social media creates a picture based on a user's activities online over a given period of time. These footprints render one traceable (Clooke 2013). As mentioned earlier, criminals can take advantage of the information the social media provide them with (Blair 2011).

Frequency of user tagging

Figure 5, shows the frequency of uploaded photographs that are tagged on Facebook by the study's sample population; 65% (*n* = 233) of the tagging is done by other users whilst 14% (*n* = 49) is done by friends. Tagging a friend avails the information of the tagged user to friends of the tagging user, who are not necessarily friends with the tagged user.

Survey

The survey consisted of questions focusing on the privacy awareness of the users about the PoPI, what violations they have faced on Facebook as well as the features of Facebook they would like to see protected. The study surveyed 70 respondents who participated in an online survey. Figure 6 shows that 57 of users (81%) do not know there was such an *Act* (PoPI) dedicated to personal information protection in South Africa. These users were under the impression that they were simply communicating online with no need to have their privacy protected by the law. Only 19% (13) were aware of the *Act* but were unsure if it was applicable to Facebook and other social media. The *Act* is still new and may not be as well publicised as would be desirable.

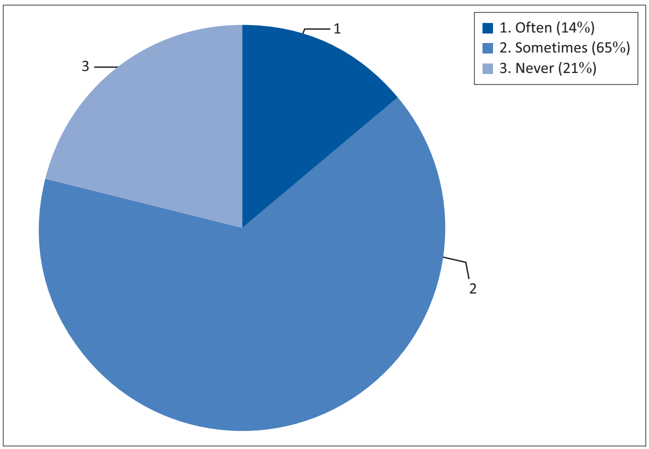

FIGURE 5: Frequency of user tagging.

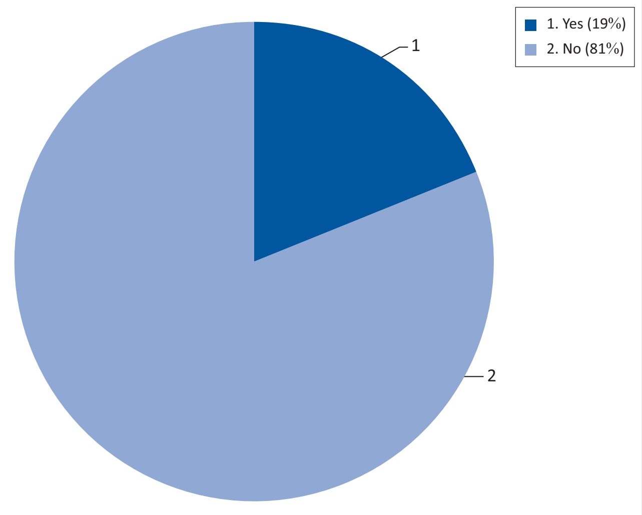

FIGURE 6: User awareness of PoPI.

One of the most frequent violations that the surveyed users experience on Facebook is strangers or other Facebook users who have no relationship with a particular user writing on their wall. In Figure 7, 40 (57%) users stated that this has happened to them, whilst 22 (31%) users said they had been tagged in something they did not approve of or found offensive on their Facebook walls, which could be viewed by anyone. Figure 7 also shows that 20 (28%) users claimed someone had uploaded something they did not approve of without prior consultation. Finally, 10 (14%) users stated that they had never encountered any of these violations.

In Figure 8, not surprisingly, when asked which feature they believed would benefit the most from improvement on Facebook, users stated that they would like to see their news feed improve. According to the survey, 60 (85%) users would like to have control of what they see from other users as well as what

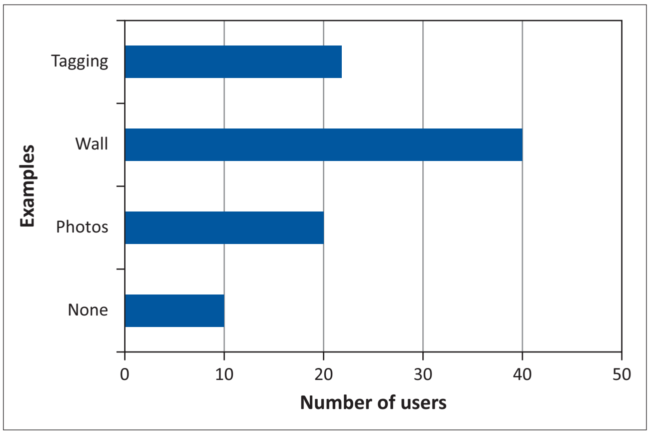

FIGURE 7: Examples of violations of user privacy.

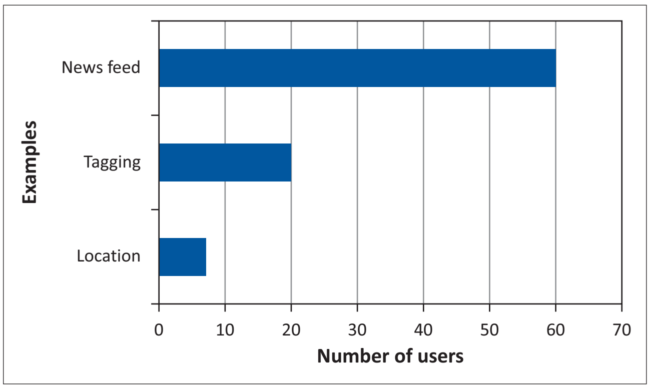

FIGURE 8: Features to be improved upon.

other users see from them via the news feed feature on Facebook. The general account settings of Facebook enable users to control shared information; however, the findings suggest that users require more protection. Furthermore, 20 (28%) respondents would improve the way users can be tagged in unsavoury material on Facebook whilst only 7 (10%) respondents were concerned with location information sharing, which they want changed on Facebook. The poor responses on geo-location information shows that users lack security awareness of how sharing sensitive information and geo-location information impacts negatively on their online presence.

Summary of findings

Privacy

The study reveals that users do not always choose to set their profiles to private when they first register with Facebook. This is because users are not that knowledgeable and also lack awareness. This is consistent with the findings in Figure 8: 86% of respondents (60 news feed respondents including geo-location and tagging respondents) were not aware of the controls that can assist them to regulate their privacy such as picking who can post on their wall, tag them in a photograph or share their location with others without their knowledge. Most user data is partially available on user profiles, a situation that can be exploited by criminal elements. Anyone masquerading as one of the user's friends can access this sensitive data by logging on and searching for this data. Users have less privacy protection on the Internet and this has an influence on the way these sites should be run. Based on these findings, privacy could be achieved through training and awareness on how to fully utilise privacy settings on social media. Users must be taught the different techniques to secure their personal information (Warren 2008).

Users also have experienced different kinds of violations that have infringed on their privacy online. These have ranged from people writing on their walls (reports of unwanted attention, insults or abuse) to being tagged in photographs that are questionable and which may project the user in a negative way (lewd, violent or racist images). Privacy controls (Facebook 2014), if properly taken advantage of, could mitigate some of these violations, but from these findings, it is clear that most users are still unaware of the necessity of the tools to protect themselves (Mourer 2014). This lack of safety consciousness was highlighted in a study by Hoadley *et al.* (2010). The researchers noted that service providers needed to develop privacy enhancing features that are easy to use for the average user. This study has found that most users are not protecting their data, thereby allowing anonymous people on Facebook to access their sensitive data. Users regard the sharing of personal information online to be low risk; therefore, they are not motivated to change their online behaviour (Hoadley *et al.* 2010).

User personal information and self-disclosure

It is easier to view other users' information on Facebook and this makes it possible for those with malicious intent to get hold of sensitive data. The greatest challenge users face is the perception of individuals in a group of friends that they cannot be attacked. However, there is a possibility that they will be attacked. The information that users willingly supply is highly valuable. Attackers are after one's username and password and they do not hesitate to mine Facebook to access such credentials (Fogel & Nehmad 2009).

Attackers have figured out that people hardly change their usernames and passwords, so if they can figure out what their credentials are on Facebook, it is likely they could be the same as the ones used for banking. This is a basic form of social engineering as potential attackers make use of information such as a birthday, pet's name, husband's name, girlfriend's name or high school name, which are the most common types of passwords or security questions used to recover an online account (Fogel & Nehmad 2009).

Geo-location sharing and tagging

To a skilled and seasoned social engineer, location sharing is integral in tracking the movements and establishing patterns of an individual (Blair 2011). This information is quite easy to obtain from the profiles of users. A number of social networks attacks are possible given the high level of trust people place in these sites. In fact, a survey done in 2011 in the United Kingdom revealed that 50 cases of burglary succeeded because the perpetrators relied on social media sites like Facebook in planning their crimes and that location information was useful in their operations (Blair 2011).

The sharing of geo-location makes users vulnerable as they can be tracked. A log of an individual's movements and activities can be created by a potential attacker who can recognise patterns in the user's activities and thereafter plan break-ins when users are not at their place of residence (Blair 2011) with full knowledge when they would be back home. Timing and time management is crucial in any operation.

Most users enjoy sharing their photos with their friends and selected individuals in their news feed or wall posts. The challenge with being tagged is that users can be tagged in some offensive material that might be racist, xenophobic or graphic in nature. These images are then seen by all the friends of their friends as fresh updates on their news feed, thereby bypassing any controls set by the first user. This is an undesirable outcome of tagging. Fortunately Facebook allows users to untag themselves from such images; however, they cannot delete the copies of such images that may have been downloaded on many servers across the globe (Alcorn 2012).

Users often tag each other in photographs on Facebook. Some of the images users are tagged in can leave undesirable impressions on those who view them on their news feed. Facebook has also introduced face-recognition software that can automatically pick up users in images and tag them. Some of these new features from Facebook have met resistance from the user base as they are seen to be clear violations of their privacy. Facebook simply wishes to enable a more efficient service that allows users who know each other to share their experiences with their friends online, but the risk is that users may end up losing their privacy. The need for efficiency may inadvertently create security risks which tend to be unforeseen by the over-eager developers behind these sites. The concept of being tagged in a photograph that you have not consented to is simply a violation of one's privacy. Hopefully this will be considered by service providers when they develop their sites (Alcorn 2012).

Legal issues

Users are not aware of the new legislation, the PoPI, which seeks to defend their rights to privacy. This could be due to a broad disinterest or inability to understand what the *Act* entails. Interestingly, we are migrating more and more to cyberspace and this will necessitate the development of comprehensive and user-friendly privacy legislation to support safety on these websites (Information Security Group of Africa 2011).

South Africa has developed security legislation such as the PoPI as it was necessary to keep up with the pace of technology and e-commerce. There has been a need for separate and more adequate legislation on data protection. The *Act*, however, is not conclusive and does not adequately cover data that is generated on social media sites. There may be a need for tailor-made legislation to help solve any grey areas regarding the application of laws and the description of specific violations (Information Security Group of Africa 2011). There has been a provision within the *Act* for the establishment of an information regulator who has jurisdiction throughout the republic. This board may be able to take up the issues of social media privacy as privacy violations are reported to the regulator. However, it has to be represented and well informed. Unfortunately, the world is lagging behind in cyber security. The design of protection laws is largely reactive instead of being proactive.

There is limited research on the effectiveness of this new PoPI in South Africa. Reports on the application of privacy laws across the world are widely available online. For example, Google was fined 150 000 Euros in France as they violated privacy laws when they failed to inform users regarding the use of personal data (Bodoni 2014). However, this is not the case in South Africa. These cases, however, serve as a benchmark for how PoPI can penalise those who infringe privacy rights. It is possible for the government to hold Facebook accountable as much as the Europeans do and other nations of the world (China, for example, is strict when dealing with Google). This will force the government to be proactive and continue to police the operations of Internet-based companies.

Conclusion

This article has sought to assess how new data protection laws in South Africa affect user behaviour on social media (Facebook in particular). As can be seen in Figure 6, many users (81%) indicated that they were not aware of the new PoPI and how it is supposed to protect their privacy rights online. Highlights from the findings also show that users still post sensitive personal information on their profiles that can be used to track their movements, location and activities by interested parties. The majority of users believe that information posted on their Facebook profiles is not viewable by anyone outside of their social spheres on Facebook. The study has revealed that there is more than enough information available in the public domain about a user, which can be used to profile and track a user's online habits (Warren 2008).

The new *Act* is likely to face a number of challenges since many Internet-based companies operate outside the jurisdiction of South Africa. It is not easy to see an immediate solution to this challenge of policing international digital cyberspace. A central problem is that behaviour on the Web cannot be controlled. This has traditionally been seen as a good thing. Also it is difficult to reach international consensus on Web privacy because the concept of privacy is heavily dependent on widely variable cultural and political issues (Mishra 2008). For example, the self-regulatory approach adopted by the US is in direct contrast with the government-mandated approach adopted by the EU. This has to do with the region-specific attitudes towards state intervention in online activity (Information Security Group of Africa 2011).

Governments in general lag behind in the creation of privacy protection laws. This is caused by lengthy processes which involve the consultation of industry specialists, practitioners, advocates and users in designing appropriate laws for data protection (Mishra 2008). Furthermore, policymakers lack the expertise to enact such laws. As a result, various international countries have implemented varying degrees of privacy legislations (such as the OECD guidelines), which have been designed to control how companies access and utilise information on potential customers (Information Security Group of Africa 2011). Unfortunately, cyber technology is dynamic, fluid and transnational. The laws are largely reactive to abuses and privacy violations.

There is also a need to enforce privacy laws to deter companies from violating the privacy of users. On the other hand, the challenge of getting users to be proactive about their privacy may be the key to gaining success in this area. Future work may explore the crafting of global privacy laws which are in tandem with national laws designed to police the activities of companies whilst protecting users. User security awareness also requires special attention.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Author's contributions

P.N. (North-West University) was responsible for research design, investigation and also wrote the manuscript. M.V. (University of Limpopo) was the project leader and editor of the manuscript.

References

Alcorn, A., 2012, *Facebook really needs more sophisticated privacy controls*, viewed 18 June 2014, from http://www.makeuseof.com/tag/facebook-sophisticated-privacy-controls-opinion/

Baker, J., 1991, 'Personal Information and Privacy', in *Proceedings of the first conference on computers, freedom, and privacy,* pp. 42–45, IEEE Computer Society Press, Los Alamitos. http://dx.doi.org/10.1109/CCFP.1991.664754

Blair, K., 2011, *New survey: Burglars use social media to plan crimes*, viewed 18 June 2014, from http://socialtimes.com/new-survery-burglars-use-social-media-to-plan-crimes_b79475

Bodoni, S., 2014, *Google fined maximum French penalty for privacy violations*, viewed 30 January 2014, from http://www.bloomberg.com/news/2014-01-08/google-fined-maximum-french-penalty-for-privacy-violations.html

Clooke, R., 2013, *Facing the risks of location sharing*, viewed 18 June 2014, from http://www.mobilesecurity.com/articles/526-facing-the-risks-of-location-sharing#sthash.gO0eDEGi.dpuf

Craig, T. & Ludloff, M., 2011, Privacy and big data, O'Reilly Media, Sebastopol.

Digital Insights, 2014, *Social media statistics for 2014*, viewed 23 March 2015, from www.adweek.com/socialtimes/files/2014/06/social-media-statistics-2014.htm

Facebook, 2014, *Privacy policy of Facebook*, viewed 25 March 2015, from www.facebook.com/policies/privacy/basic/?ref_component

Fogel, J. & Nehmad, E., 2009, 'Internet social network communities: Risk taking, trust, and privacy concerns', *Computers in Human Behavior* 25(1), 153–160. http://dx.doi.org/10.1016/j.chb.2008.08.006

Gartrell, M., Han, R. & Beach, A., 2008, *Solutions to security and privacy issues in mobile social networking*, University of Colorado, Boulder.

Hoadley, C., Xu, H., Lee, J. & Rosson, M., 2010, 'Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry', *Journal of Electronic Commerce Research and Applications* 9(1), 50–60. http://dx.doi.org/10.1016/j.elerap.2009.05.001

Information Security Group of Africa, 2011, *Revealing privacy in South Africa: What you need to know*, Information Security Group of Africa, Pretoria, South Africa.

KPMG, 2009, *Information privacy & financial institutions: White paper*, KPMG, Pretoria, South Africa.

Krejcie, R.V. & Morgan, D.W., 1970, 'Determining sample size for research activities', *Journal of Educational and Psychological Measurement* 30, 607–610.

Kruck, S.E., Gottovi, D., Moghadami, F., Broom, R. & Forcht, K.A., 2002, 'Protecting personal privacy on the Internet', *Information Management & Security* 10(2), 77–84. http://dx.doi.org/10.1108/09685220210424140

Mansfield-Devine, S., 2008, 'Anti-social networking: Exploiting the trusting environment of Web 2.0', *Network Security* 11, 4–7. http://dx.doi.org/10.1016/S1353-4858(08)70127-2

Ministry of Justice and Constitutional Development, 2013, *Protection of Personal Information Act, No. 4 of 2013*, Parliament of South Africa, Pretoria, South Africa.

Mishra, A., 2008, *Web privacy: Issues, legislations and technological challenges*, IGI Global, Hershey. http://dx.doi.org/10.4018/978-1-59904-804-8.ch001

Mourer, K., 2014, *Texting to surpass phone calls for business communication*, viewed 18 June 2014, from http://www.icmi.com/Resources/Mobile/2014/03/Texting-to-Surpass-Phone-Calls-for-Business-Communication

Smith, H., 2004, 'Information privacy and its management', *MIS Quarterly Executive* 3(4), 201–213.

Spinello, R., 2000, *Cyber-ethics: Morality and law in cyberspace*, Jones and Bartlett, London.

Stahl, B.C., 2000, *The impact of the UK Human Rights Act 1998 on privacy protection in the workplace*, IGI Global, Hershey.

Turner, E.C. & Dasgupta, S., 2003, 'Privacy on the web: An examination of user concerns, technology, and implications for business organisations and individuals', *Journal of Information System Management* 20(1), 8–18. http://dx.doi.org/10.1201/1078/43203.20.1.20031201/40079.2

Warren, J., 2008, *Self-imposed violations of privacy in virtual communities*, University of Texas, San Antonio.