# CHANGING BEHAVIOUR: WEB 2.0 USAGE AND SECURITY PRACTICES OF ONLINE USERS

Riaan Rudman and Len Steenkamp
Stellenbosch University
South Africa

## Abstract

The proliferation of Web 2.0 technologies and the increasing number of threats have resulted in more emphasis being placed on creating awareness of users on the use of Web 2.0 technologies and related risks. South-African University students are taught about the threats and related security controls. The question arises as to whether they change their behaviour when using Web 2.0 technologies in light of the risks. Against this background, a survey was conducted of South-African university students to determine which online practices they employed when using Web 2.0 technologies. It may appear that educating users on the risks posed is being flogged to death in the popular press, but reality shows that this is taken too lightly.

## Introduction and Problem Statement

Recently, online business-to-business collaboration has been on the increase, where business functionality is supported through virtual applications, often driven by Web 2.0 technologies (referred to as 'Web 2.0' hence forth). This makes it necessary for business users to have greater access to the Internet as part of their normal business day, even in South-Africa with low internet penetration. This trend, which is expected to continue, is driven by the new generation of Internet users entering the workforce from university and bringing with them the familiarity of Web 2.0 (Hampton, Goulet, Marlow & Rainie, 2012). As users are more comfortable with Web 2.0 in their personal lives, they also demand this in their business lives. With the growth and widespread use of Web 2.0, much of the focus has been on ensuring that users gain access to data and resources, with less thought being given to whether users should have access or how they gain access and how that access is controlled. Many organisations are now becoming more worried about the impact of Web 2.0 on security, productivity and privacy. The publicity resulting from the increasing number of Internet incidences has caused more emphasis to be placed on advising users on the use of Web 2.0. The question now arises as to which practices online Web 2.0 users employ when managing their online identity and to what extent do users protect their privacy in light of the increase in publicity around Web 2.0 use, risks and consequences. The primary objective of this research is to assess which practices online users employ when using Web 2.0. University students are used as a proxy for educated users. Their practices were compared to acceptable practices they are taught in class.

It is important to understand how Web 2.0 users manage their identity, as Web 2.0 is a new, poorly understood technology and, with the growing mobility of

users, the potential threat increases (D'Agostino, 2006). The study also considers the popularity of these sites to determine the scale of the potential threat to corporate security, since university students, who are future business IT users, are the most connected Internet users because all of them have access to computer facilities on campus and are the early adopters of technology. In many instances they are the ones responsible for introducing new technologies to businesses. They are also the main users (Clearswift, 2008).

The results of this study will help business determine strategies to aid in the adoption and diffusion of Web 2.0.

## Research Methodology and Target Population

A literature review was undertaken to identify existing research on online users' behaviour. A web-based survey was conducted among students in the Faculty of Economic and Management Sciences at a South African university to assess the practices they employed when using Web 2.0. The questionnaire contained questions to determine how the students' manage their Web 2.0 identity and their usage patterns; as well as to evaluate the users' awareness of the risks relating to Web 2.0 and how they manage these risks. Particular consideration was given to the risks and safeguards the students are taught in class. Before the questionnaire was distributed to the target population, the questionnaire was reviewed by lecturers in both the field of auditing and information systems, a statistician and ten volunteers from the target student population. They considered the questionnaire in terms of logic and intelligibility. Minor amendments were made on the basis of their feedback. Thereafter, the questionnaire was distributed to students enrolled in a number of courses from first year to honours year courses, all in the field of economic and management sciences. These students are taught the risks relating to the Internet, as well as related safeguards, either in their Information Technology or their Auditing and Governance courses. In selecting the students, the researchers were able to identify whether users apply better practices as they become more technology literate and aware of the dangers of Web 2.0, as opposed to other potentially less computer aware users. In total, 2 944 invitations to participate in the study were sent to students. Altogether 660 students completed the questionnaire. The response rate of 22.4% is considered sufficient to arrive at the necessary conclusions. All the responses from the target population were scrutinised to eliminate instances where respondents clearly did not attempt to answer the questions. The answers to the open-ended questions were analysed and summarised in similar categories.

## Literature Review

### Web 2.0

The traditional Internet, hosted mostly static, one-way websites. Users visited these sites passively, mostly to retrieve information. Web 2.0 operates differently. Users are able to actively update websites in real-time, users can collaborate with others in order to contribute content online (referred to as the "*read-write web*"). Although numerous definitions exist for the term 'Web 2.0', it is not well defined (Radcliff, 2007). The debate around defining Web

2.0 falls outside of the scope of this research. On 20 January 2012, Wikipedia (2012) defined Web 2.0 as

> Web applications that facilitate participatory information sharing, interoperability, user-centred design, and collaboration on the World Wide Web. A Web 2.0 site allows users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to websites where users are limited to the passive viewing of content that was created for them.

The definition of Web 2.0 is continuously evolving. Three components or shared values have been identified:

- **Community and social:** This allows users to change and improve content and to simultaneously redistribute it in modified form.
- **Technology and architecture:** These are web-based applications with a rich interface that run in a web browser technology and do not require specific software installation, device or platform.
- **Business and process:** It involves resources on a network made available as independent services that can be accessed without knowledge of their underlying platforms. Software is being delivered as a service rather than an installed product, freeing users from a specific platform.

Web 2.0 constitutes a paradigm shift in the manner in which existing technology is used. It is the evolution of the static browser to a dynamic, asynchronous interface, building on the knowledge and skills of the users. Some examples of Web 2.0 include the following: content generation (e.g., Blogs, Wiki, Really Simple Syndication feeds), building social networks and communicating information (via applications such as Facebook, MySpace, LinkedIn, Twitter), sharing video and audio recordings (e.g., Podcasts and via applications such as YouTube, MySpace), trading products (e.g., eBay), and even living in virtual worlds such as Second Life.

## Historical Review of Prior Research

As the popularity of Web 2.0 services grew, the popular media published various articles on, for example, security risks relating to Web 2.0 services, while others focused mainly on business risks (D'Agostino, 2006; Fanning, 2007; Mitchell, 2007). Popular media publications in almost every industry have published some kind of article outlining how Web 2.0 has impacted that specific industry.

Most research relating to Web 2.0 has been conducted by private organisations such as Gartner, Clearswift, Pew Internet & American Life Project and KPMG, amongst others, with limited academic peer-reviewed research being performed (Shin, 2008). Initially, research focused on understanding the technology, its benefits, uses in a business environment and potential challenges (Clearswift, 2007a; 2007b). Other research studies focused on the areas of privacy (Cavoukian & Tapscott, 2006), collaboration (Lee & Lan, 2007), usage and users' behaviour patterns (Horrigan, 2007; Lenhart & Madden, 2007a & b; Shin, 2008; Smith, 2011).

Various attempts have been made to develop an organisational framework to help businesses to understand and address Web 2.0 risks and to generate business value for enterprises using Web 2.0. The most widely used frameworks were developed by Dawson (2008). Rudman (2010a) developed a framework to identify and manage Web 2.0 risks in a particular company. Before frameworks for risk or value evaluation can be implemented, users' behaviour needs to be understood.

## Prior Research Studies Covering Online Users' Behaviour

Much work has been conducted on users' behaviour, what information users disclose and how users manage their privacy. The Pew Internet & American Life Project has conducted a series of studies on Internet users' behaviour and related topics such as privacy trust online, identity management and protection. These focused on various user groups ranging from teens to established employees. Earlier studies (Fox, Rainie, Horrigan, Lenhart, Spooner & Carter) in 2000 focused on the use of the Internet. These authors concluded that there is a presumption of privacy when users go online and that many users are uneducated about how to manage their identities and the risks they expose themselves too. Early in 2007, when the focus changed to Web 2.0, Lenhart and Madden (2007a) conducted a national survey of young people between the ages of 12 and 17 across the United States. The study focused on which sites were used, the reasons for using these sites and how they were used, as well methods to mitigate any potential threats. During April 2007 another study was conducted that focused specifically on the information teens share, on assessing how teens evaluated the vulnerabilities, and the relationships online. Researchers found that most teens protect themselves by limiting the information they share and to whom, yet rely very little on automated protection (Lenhart & Madden, 2007b).

Guess (2007) reported on a study that investigated how college students were using information technology and its impact on improving the learning experience. Researchers found that students spent significant amount of time on the Internet, mainly accessing it via mobile technology. They also noted a change in the reasons why students were using the Internet, as well as the tools being used. Engineering and business students relied more on spreadsheets and graphics editing tools on the Internet. This confirmed comments by Horrigan (2007).

Other research focused on business users' behaviour in general, as well as industry-specific business users. Clearswift (2007a) investigated the impact of Web 2.0 on security, and while conducting the study also investigated usage patterns and management of identity of employees in the world's two most developed countries. Researchers focused on the type of service most frequently used, the time spent, as well as most prominent risks and related safeguards to mitigate any risks. Another study conducted by Clearswift in 2008, investigated the attitude of human resources (HR) professionals to Web 2.0 and how they had adapted Web 2.0 to their organisations. Authors found that organisations perceived risks in allowing employees uncontrolled access to Web 2.0, and although many sites have security features, many users were

unaware of the features or did not enable these features. Rudman (2010b) wrote a paper on the incremental risks in Web 2.0.

These studies highlight the importance of identity management and risks in an international mature context. In this research there is an implied assumption that the users are informed and aware of the risks and safeguards relating to Web 2.0. However a similar study taking user knowledge explicitly into account has not been conducted.

## Findings

The respondents were questioned about the nature of Internet use before specific consideration was given to Web 2.0 related matters.

### Respondents' Profile and Internet Activity

The 660 respondents comprised 54% male and 46% female students, of whom 71% were white, 24% black (5% preferred not to indicate ethnicity). The demographic profile is not as important as the respondents' connectivity, because all respondents have access to the same resources at University. The majority (52.5%) of the respondents indicated that, other than using their cell phones, they accessed the Internet from their place of residence, while the remainder (43.4%) used the university's computer facilities. The source of access had a direct impact on the frequency at which the respondents accessed the Internet and the time spent on the Internet: 76% of the respondents indicated that they accessed Web 2.0 at least once a week, clearly indicating that this was a favoured activity. The nature of the most frequently visited sites is presented in Table 1. It is interesting to note that the sites with a direct communication component are used more often than content driven services.

Table 1.

*Most Frequently Visited Types of Sites*

| Type of sites | Percentage |
|---|---|
| *Personal communication* | |
| Closed one-on-one communication such as Webmail and Instant Messaging | 40.7% |
| Open communication such as social networking sites | 27.8% |
| *Information source* | |
| Passive interaction information sources | 15.9% |
| Active interaction information sources | 4.2% |
| *Sharing sites* | 8.9% |
| *Online applications, services and worlds* | 2.6% |

### Awareness and Utilisation of Web 2.0 services

Although a wide range of services was used, many of these users were not aware of the nature of the service they used. Those respondents that were able to identify Web 2.0 listed the differentiating characteristics of these sites as interactive, constantly changing, personal information sharing and user-orientated. This is important because the changes in technology, give rise to new risks, which need to be controlled by new safeguards (Rudman, 2010a).

One of the primary characteristics of Web 2.0 is the interactivity of the sites and the multiple features. More than half of the respondents (53.3%) indicated that they mainly view content on the Internet: 15.0% and 8.4% of the respondents indicated that they submitted and amended information online, respectively, while 23.3% used online applications. These results are summarised in Figure 1 and concur with the findings by Guess (2007) and Horrigan (2007).

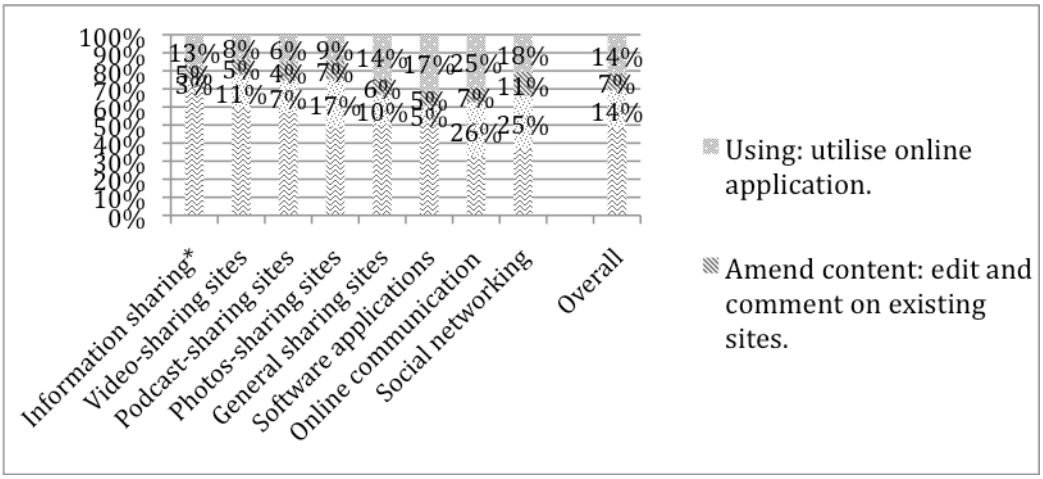


*Figure 1.* Methods of interacting with the types of Web 2.0 services.

** Information sharing refers to websites where information is predominantly shared by way of text.*

## The influence of Web 2.0

Web 2.0 technologies are more resource-intensive and consequently could have a greater negative influence on an organisation, compared to traditional Web 1.0 websites. Therefore a number of questions were asked to gauge the respondents' awareness of the effect of Web 2.0 on them and others. Of the respondents, 30.5% were of the opinion that Web 2.0 usage did not influence university resources. But interestingly, 57.4% were of the opinion that the time spent on Web 2.0 sites influenced other users. This might be because 43.4% of the respondents used the university's computer facilities to access the Internet. Similarly, 46% of the respondents stated that they believed that Web 2.0 use influences students' studies. This, in light of the fact that the respondents mainly used Web 2.0 for non-academic purposes, may indicate that the effect will be predominantly negative. It also potentially takes time away from academic endeavours. Additionally, 48.2% believed that Web 2.0 influenced their social life and the ways in which they interact socially.

## Risks and Consequences

Unproductive time and resources constitute but only one risk. Overall (65.3%) the respondents were not aware of the risks posed specifically by Web 2.0, although the students were taught in class that the same vulnerabilities that affect traditional web applications also impact new technologies such as Web 2.0. New threats have been developed specifically to target Web 2.0, but Web 2.0 did not change the risks, it changed the manner in which the threats are delivered. A detailed list of all risks and safeguards is contained in Rudman (2010b).

The respondents were required to rate seven potential risks, where '1' was the most significant risk and '7' was the least significant risk. Table 2 contains the average ratings for the risks. The most significant risk identified was electronic intrusion. Phishing attacks, a real risk which could be based on socially engineered information, was rated second. Unproductive time and unavailability for services were rated low, confirming earlier findings.

Table 2.

*Average Ranking of Risks by Respondents*

| Risk | Average |
|---|---|
| Electronic intrusion (worms, zombie bots) embedded in downloads | 1.96 |
| Phishing attacks, including spam. | 2.63 |
| Breach of security of the controls on the website | 2.64 |
| Information leakage and brand damage | 2.92 |
| Unproductive time | 3.38 |
| Content errors on websites | 3.40 |
| Denial of service | 3.59 |

## Inappropriate Disclosure of Information

Many of the risks presented in the previous section arise from sharing too much information. Approximately 80% of the respondents believed that sharing too much information could lead to attacks. Two types of personal information could be posted online, either by means of creating a profile or through sharing personal information.

Of the respondents, 80.6% indicated that they created online profiles on Web 2.0 sites, being most likely to share personal information (such as first name [94.5%]; last name [87.5%]), followed by information about where they reside (university name [77.2%]; residence [70.2%]), followed by contact information. They were least likely to share content that is resource intensive to upload or stream video (13.8%) or audio (6.0%) files. They would share personal information regardless of whether it would make them vulnerable to social engineered attacks: 61.7% of respondents acknowledge that a motivated Internet user would be able to identify them from their Internet profiles. In light of the responses above, the respondents were asked which types of information they disclosed on Web 2.0 sites other than when creating their profile (Table 3).

Table 3.

*Nature of Information Shared on Web 2.0*

| Type of Information | Yes | No | Maybe |
|---|---|---|---|
| Biographical information | 53% | 35% | 12% |
| Contact information | 33% | 54% | 13% |
| Personal information | 43% | 43% | 14% |

Respondents would be willing to share biographical and personal information such as their religious affiliation, relationship status, and less likely to share all types of contact information. Most (53%) would also disclose their e-mail addresses. One quarter of the respondents would provide their cell phone numbers and 13% would knowingly provide other information that might allow someone to find them easily, such as address, and home phone number. 12% would provide their passwords online and 10% would share personal identification information such as identity numbers, or medical information.

### Safeguards to Mitigate Risk

In order to limit the risks, safeguards could be implemented, by limiting use, self-protection, or policy implementation. The majority (44.2%) indicated that they would at least limit their activities, if they knew they were being monitored, while 11.6% indicated that they would stop using the Internet. Another 4.3% felt that with the large volume of online activity, it would be impossible for someone to effectively monitor activities and, consequently, they would not act. Of the respondents, 39.9% felt that their activities did not expose them to risks requiring them to change their Internet behaviour, irrespective of the fact that they were taught the risks relating to Web 2.0 in class.

While the respondents may have been unaware of the risks, 60.6% of the respondents did take some steps to protect themselves online ---63.4% made use of the security settings, while 25% were not sure whether they did. Altogether 56.3% made their information only available to their friends. One fifth of the respondents made their profiles visible to anyone, while 10.3% did not know to whom their profiles were visible. Other methods that respondents used to restrict access to their profiles were: giving as little personal information as possible (50.4%), password protection (59.5%) and disclosing information to known friends (37.1%). This confirms findings by Fox et al. (2000) and Lenhart and Madden (2007b).

Many organisations have Internet policies that govern the use of company resources. The majority of the respondents (82.8%) indicated that they would comply with such a policy, if they were aware of it, while 14.2% would probably ignore the policy in their use of the Internet. Alternatively, access could be blocked; however, 68% of the respondents felt that access should not be blocked, even though nearly half (47.2%) stated that Web 2.0 related risks may impact on the security of the organisation. In addition, 37% of the respondents indicated that employees should be entitled to access Web 2.0 content from their work computer for personal reasons, irrespective of the risks. Based on the findings, Table 4 lists the controls the students were taught in class compared to the extent that they would implement the controls.

Table 4.

*Extent to Which Safeguards Are Implemented in Practice*

| Theoretical safeguard | Ignored | Unaware | Effective |
|---|---|---|---|
| Block access to designated websites, file types and utilities | | | X |
| Implement a next generation reputation based filtering | | | X |
| Utilise deep-scanning behavioural anti-malware programs | | | X |
| Monitor, review and investigate resource activity | X | | |
| Ensure that all network and software up-to-date | | X | |
| Utilise browser security and configure browser correctly | | X | |
| Utilise security features and configure correctly | | X | |
| Implement a robust policy | | X | |
| Educate users on Web 2.0 risks and related safeguards | X | | |

## Discussion and Conclusion

Internet security and privacy is a concern for most businesses. With the growing use of Web 2.0, the potential risk related to Web 2.0 will not abate in the future. Against this background, a study was conducted to determine which practices university students employed when using Web 2.0. The respondents indicated that two thirds of them accessed Web 2.0 at least once a week and that social networking sites were accessed frequently. Nearly half of the respondents indicated that they fully engaged with Web 2.0 through amending and submitting content. The respondents were aware of the risks. However this did not influence their online activities. Most respondents indicated that they did take some measures to protect themselves, but they implemented safeguards in a haphazard manner. The results of this study, therefore, indicate that Web 2.0 is used widely and that although students are educated on the risks and controls in class, they do not necessarily implement safeguards to address the risks. Considerations should be given to blocking access to popular Web 2.0 and implementing strict controls that do not rely on user implementation, since potential safeguards would, in all probability, be ignored even by informed users or not used. This also says a lot about the manner in which students study and are able to apply theory to practice. When teaching information security, greater emphasis should be placed on practical examples, identification of risks and the real-life implementation of controls. Moreover, organizations cannot rely only on users to employ proper controls. It may seem as if educating users on the risks posed by the Internet is being flogged to death in the popular press. Yet this study has indicated that this process can never be taken too lightly, especially in protecting businesses' most important resource: information.

## References

Cavoukian, A., & Tapscott, D. (2006). *Privacy and the Enterprise 2.0.* New Paradigm Learning Corporation. Retrieved from http://newparadigm.com/media/Privacy_and_ the_Enterprise_2.0.pdf

Clearswift. (2007a). *Content security 2.0: The impact of Web 2.0 on corporate security*. Retrieved from http://resources.clearswift.com/Externalcontent /Features/Clearswift/9586/200704SurveyReport_US_1063233.pdf

Clearswift. (2007b). *Demystifying Web 2.0*. Retrieved from http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/95 14/ 200707 DemystifyingWeb21].0_US_1062190.pdf

Clearswift. (2008). *Content security 2.0: The role of HR and IT in effectively managing the business benefits and risks of Web 2.0*. Retrieved from http://resources.clearswift.com/main/pages/Clearswift/RSRCCTR/ ContentDisplay.aspx?sid=3230&yid=2711

D'Agostino. D. (Winter 2006). Security in the world of Web 2.0. *CIO Insight*, 12-15.

Dawson, R. (2008). An enterprise 2.0 Governance Framework-looking for input! Retrieved from http://rossdawsonblog.com/weblog/archives/2008/2/an_enterprise_2.html

Fanning, E. (2007). Security for Web 2.0. *Computerworld*, 3 September, 44.

Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C. (2000). *Trust and privacy online: Why Americans want to rewrite the rules.* Pew Internet & American Life Project: Washington, D. C. Retrieved from http://pewinternet.org/Reports/2000/Trust-and-Privacy-Online.aspx

Guess, A. (2007). Students' 'evolving' use of technology. *INSIDE HIGHER ED*. Retrieved from http://www.insidehighered.com/news/2007/09/17/it

Hampton, K., Goulet, L.S., Marlow, C., & Rainie, L. (2012). *Why most Facebook users get more than they give*. Pew Internet & American Life Project: Washington, D.C. Retrieved from http://www.pewinternet.org/Reports/2012/Facebook-users.aspx

Horrigan, J. (2007). *A typology of information and communication users.* Pew Internet & American life Project. Retrieved from http://www.pewInternet.org/pdfs/PIP_ICT_Typology.pdf

Lee, M., & Lan, Y. (2007). From Web 2.0 to conversational knowledge management: Towards collaborative intelligence. *Journal of Entrepreneurship Research*, *2*(2), 47-62.

Lenhart, A., & Madden, M. (2007a). *Social networking websites and teens: An overview.* Pew Internet & American life Project, Retrieved from http://www.pewinternet.org/~/media//Files/ Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf

Lenhart, A., & Madden, M. (2007b). *Teens, privacy, and online social networks.* Pew Internet & American life Project. Retrieved from http://www.pewInternet.org/pdfs/PIPTeensPrivacySNSReport.pdf

Mitchell, R. (2007). Web 2.0 users open a box of security risks. *Computerworld*, 26 March, 32.

Radcliff, D. (2007). Are you watching? *SC Magazine*, September, 40-43.

Rudman, R. (2010a). Framework to identify and manage risks in Web 2.0 applications. *African Journal of Business Management*, *4*(13), 3251-3264.

Rudman, R. (2010b). Incremental risks in Web 2.0 applications. *The Electronic Library*, *28*(2), 210-230.

Shin, D. (2008). Understanding purchasing behaviour in a virtual economy: Consumer behaviour involving currency in Web 2.0 communities. *Interacting with computers*, *20*, 433-446.

Smith, A. (2011). *Why Americans use social media.* Pew Internet & American life Project. Retrieved from http://pewinternet.org/~/media//Files/Reports/2011/WhyAmericansUseSocialMedia.pdf

Wikipedia. (2012). Web 2.0. *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Web_2