Michota, Alexandra

Article

Digital security concerns and threats facing women entrepreneurs

Journal of Innovation and Entrepreneurship

Provided in Cooperation with:
Springer Nature

Suggested Citation: Michota, Alexandra (2013) : Digital security concerns and threats facing women entrepreneurs, Journal of Innovation and Entrepreneurship, ISSN 2192-5372, Springer, Heidelberg, Vol. 2, pp. 1-11, https://doi.org/10.1186/2192-5372-2-7

This Version is available at:
https://hdl.handle.net/10419/146802

Journal of Innovation and Entrepreneurship
a SpringerOpen Journal

RESEARCH Open Access

Digital security concerns and threats facing women entrepreneurs

Alexandra Michota

Correspondence:
alexandra_michota@yahoo.gr
Department of Digital Systems,
University of Piraeus, Piraeus, Greece

Abstract

Women represent the main economic force in most developing countries. As economies become more and more information-driven, the issues of women's access to and the use of information and communication technologies (ICTs) are growing in importance for both developed and developing economies. Some claim that women are rather technophobic and that men are much better users of digital tools while others argue that women enthusiastically embrace digital communication.
The ease with which information and communication technologies can transmit and disseminate information for development is well recognized. However, women's access to ICTs cannot be assumed to occur 'naturally' when gender-blind approaches and technologies are implemented. As a result of profound, gendered applications and implications of ICTs in employment, education, training, and other areas of life, women need encouragement and support to take their rightful place in the information revolution.
Research has demonstrated that security and privacy in use of ICT, especially in the internet, are the most important thematic areas of gender concerns which include freedom of expression, privacy of communication, and secure online spaces where vulnerable groups such as women feel unsafe from harassment. The main concern that discourages women to enter dynamically into e-business market is the disclosure of their personal information compared with men who appear willing to be sacrificing their privacy at the altar of profit of electronic commerce.
The aims of this research are the following: firstly, to present digital threats and risks facing women entrepreneurs daily while interacting with online communities, secondly, to study security gaps that the privacy policies of popular pages contain, and lastly, to give proof that women justifiably worry about their security and privacy when using online communities and virtual worlds, like the social networking sites. It is certain that these pages are insufficient regarding the privacy of their users due to the lack of adequate security measures letting personal data be exposed and available to others.

Keywords: ICT, Women entrepreneurship, e-Business, Digital threats, Security, Privacy

Background

During the 1990s, researchers were quick to observe that women tend to be latecomers to the digital age. As a consequence, the new technology was popularly portrayed as a male domain. Bimber concluded that the gap in ICT usage between women and men is the product of both socioeconomic differences and some combination of underlying gender-specific effects.

As more statistics became available and the Internet and mobile telephony penetration rates began to rise, women started to catch up in many developed countries. In the USA, most new users were women around the year 2000. Gender differences remained but were smaller while years passed and mainly concentrated on marginalized groups, such as ethnic minorities. However, once online, women remained less frequent and less intense users of the Internet (Huyer et al. 2005; United Nations Information and Communication Technologies Task Force 2008).

Nowadays, privacy, security, and internet rights are important thematic areas for women. Women's concerns include having secure online spaces where they can feel safe from harassment and protected from electronic snooping and enjoy freedom of expression and privacy of communication. A corollary of this is the need for campaigns against ICT legislation that can threaten human rights. While many developing countries are grappling with basic access and IT infrastructure issues, some countries in the global North are now defining the basic rights framework for internet use and governance (Acquisti et al. 2007; Dutta and Bilbao-Osorio 2012).

The study is mainly based on the fact that the majority of women are not active in the area of e-business due to the risks posed by digital threats. It is generally accepted that engagement with social networks is obligatory for the success of an e-business activity. It is not a coincidence that the most successful e-entrepreneurs acknowledged that never did they take advantage of the social networking use, they will not have noticed such large percentages of profits. Despite the fact that social networking pages look so user friendly, women once again show reluctance to use them as a tool in their work.

Accordingly, the rest of the paper is structured as follows: the 'Women e-entrepreneurs' concerns' section discusses security and privacy issues concerning their e-business development. The 'Digital threats' section presents the most important digital dangers that limit the female e-business activities. The 'Pornography, trafficking, violence against women, and censorship' section presents a detailed description of the threats that tend to affect and harm the sensitive women 's nature. The 'Social engineering' section analyzes the e-business risks through the social networking use. The 'Absence of women in e-business' section presents the results obtained by statistics that approve the absence of women in e-entrepreneurship. The 'Security requirements' section presents the recommendations from the results and the suggested policies for safer systems with the interaction of fundamental security requirements. Finally, the last section includes the 'Conclusions'.

Women e-entrepreneurs' concerns

Information and communication technologies could give a major boost to the economic, political, and social empowerment of women and the promotion of gender equality. Information technology, applications, and the use of e-services have changed dramatically in the recent past, providing women entrepreneurs and others greater opportunities for personal growth and business success (Gillwald 2001).

Second-generation internet software, referred to as Web 2.0, puts the user in control. Internet search programs now allow users to create, upload, and use their own vertical search engines. Users may search within websites and use feeds, such as from particular newspapers. Local search refers to the ability to recall past search entries. A business

can incorporate such valuable tools as 'click to call', maps, pay per call, pay per click, and coupons in its website. Increasingly, internet searches are conducted with mobile devices, and a business should customize its information accordingly. ICTs allow business persons to manage virtual teams spread around the globe using the e-mail, messenger, telephones, 'live meeting', and 'share point'. A business woman's office becomes where her computer is (Middleton 2011).

Generally, women have less access than men to ICT facilities where they exist. Numerous invisible barriers limit women's and girls' participation in the information society. However, women's access to ICTs is constrained by factors that go beyond issues of technological infrastructure and socio-economic environment. Digital privacy remains a cross-cutting element in shaping (and in this case, limiting) the capacity of women and men to participate on equal terms in the information society.

One of the more pervasive but intractable problems is 'technophobia' or fear of technology due to the lack of e-security. Women, either as entrepreneurs or as customers, hesitate to develop e-business activities. More specifically, the main issues of concern that act as barriers to the increased uptake of information technology and e-commerce including also the social networking are in the following subsections:

Security issues

Ensuring security of payments and privacy of online transactions are keys to the widespread acceptance and adoption of e-commerce. While the appropriate policies are in place to facilitate e-commerce, lack of trust is still a barrier to using the Internet to make online transactions.

Privacy issues

While security is commonly used as the catch-all word for many different reasons why individuals and firms do not engage in extensive e-commerce and use of internet-based technologies, there are other related reasons and unresolved issues, such as tax evasion, privacy and anonymity, fraud adjudication, and legal liability on credit cards (Acquisti et al. 2007).

In many countries, cash is preferred not only for security reasons but also because of a desire for anonymity on the part of those engaged in tax evasion or those who simply do not want others to know where they are spending their money. Others worry that there is lack of legal protection against fraud (i.e., there is no provision for adjudicating fraud, and there may be no legal limit on liability, say, for a lost or stolen credit card). It is necessary to distinguish these concerns from the general security concerns (i.e., transaction privacy, protection, and security) since they may not be addressed by the employment of an effective encryption method (or other security measure).

The 'leaky pipeline' phenomenon means that fewer women enter into the e-business fields, limiting the number of women entrepreneurs in research and development, and at senior positions in the ICT arena (Martinez and Reilly 2002).

Digital threats

The Internet has introduced new risks alongside the promise of enhanced cross-boundary communication. In particular, it has increased the opportunities for

surveillance of interactions between targeted groups and individuals, and for harassment. According to research, there is a 'Top 10' for the most frequent in appearance and most dangerous e-business risks and social networking threats. These are in the following subsections (Bonneau et al. 2009; Jones and Soltren 2005):

Social networking worms

Social networking worms include Koobface, which has become, according to researchers, 'the largest Web 2.0 botnet'. While a multi-faceted threat like Koobface challenges the definition of 'worm', it is specifically designed to propagate across social networks (e.g., Facebook, MySpace, Twitter, hi5, Friendster, and Bebo), enlist more machines into its botnet, and hijack more accounts to send more spam to enlist more machines, all the while making money with the usual botnet business, including scareware and Russian dating services.

Phishing bait

Phishing refers to the effort of posting personal information, usually financial in nature relating to bank accounts and credit cards, using a false pretext as bait. Phishing attempts typically send a spam email.

Trojans

E-business while interacting as a part of the social networks has become a great vector for Trojans. Two characterizing examples are the following:

1. Zeus is a potent and popular banking Trojan that has been given new life by social networks. There have been several recent high-profile thefts blamed on Zeus, notably the Duanesburg Central School district in New York State late in 2009.
2. URL Zone is a similar banking Trojan but even smarter; it can calculate the value of the victim's accounts to help decide the priority for the thief.

Data leaks

Online communities and virtual worlds are all about sharing. Unfortunately, many users share a bit too much about the organization like projects, products, financials, organizational changes, scandals, or other sensitive information. Even spouses sometimes over-share how much their significant other is working late on a top-secret project, and a few too many of the details associated with the said project. The resulting issues include the embarrassing, the damaging, and the legal (Please rob me 2010).

Shortened links

People use URL shortening services (e.g., bit.ly and tinyurl) to fit long URLs into tight spaces. They also do a nice job of obfuscating the link so it is not immediately apparent to victims that they are clicking on a malware installation, not a CNN video. These shortened links are easy to use and ubiquitous. Many of the Twitter clients will automatically shorten any links.

Botnets

Late last year, security researchers uncovered Twitter business accounts being used as a command and control channel for a few botnets. The standard command and control channel is IRC, but some have used other applications - P2P file sharing in the case of the Storm - and now, cleverly, Twitter. Twitter is shutting these accounts down, but given the ease of access of infected machines to Twitter, this will continue.

Advanced persistent threats

One of the key elements of advanced persistent threats (APT) is the variety of intelligence gathering techniques to access sensitive information of very important people (e.g., executives, officers, high-net-worth individuals), for whom online communities and virtual worlds are used as occupational tools. Information disclosed by APTs can be a treasure trove of data. Perpetrators of APTs use this information to further their threats - placing more intelligence gathering (e.g., malware, Trojans) and then gaining access to sensitive systems. So, while not directly related to APTs, online communities, even the social networks are a data source. Less exotic, but no less important to individuals is the fact that information on your whereabouts and activities can give more run-of-the-mill criminals an opportunity.

Cross-site request forgery

While it is not a specific kind of threat, cross-site request forgery (CSRF) attacks exploit the trust of any online networking application has in a logged-in user's browser. So, as long as the network application is not checking the referrer header, it is easy for an attack to 'share' an image in a user's event stream that other users might click on to catch/spread the attack.

Impersonation

E-business and social network accounts of several prominent individuals have been hacked (most recently, a handful of British politicians). Furthermore, several impersonators have gathered hundreds and thousands of followers on Twitter - and then embarrassed the folks they impersonate (e.g., CNN, Jonathan Ive, Steve Wozniak, and the Dalai Lama) or worse. Twitter will now shut down impersonators attempting to smear their victims but at Twitter's discretion. Admittedly, most of the impersonators are not distributing malware, but some of the hacked accounts certainly have (e.g., Guy Kawasaki).

Trust

The common thread across almost all of these threats is the tremendous amount of trust users have in online communities' applications. Like an e-mail, when it hit the mainstream, or instant messaging, when it became ubiquitous, people trust links, pictures, videos, and executables when they come from 'friends' until they get burned a few times.

The *European Network and Information Security Agency (ENISA)* issued a statement reiterating the main points that users of online communities have to keep in mind and proposed policies to be followed by the competent institutions to tackle them. The

most important are listed below (European Network and Information Security Agency 2009; Please rob me 2010):

Digital folders of personal data: Online profiles in any online community can be saved by others and to be part of digital dossiers of personal data. Indeed, some personal information may be collected via a simple search, unless users change the default security settings in their profile.

Secondary data: In addition to the information which users voluntarily post, members of such Web pages automatically reveal sub-items, which relate to the way they use the offered services, for example, the length of a communication, the visits to other users' profiles, and the messages that are sent over the network. The privacy settings of these pages do not sufficiently specify who may have access to the data, and it is not clearly defined what constitutes personal data and what not. Secondary data may be used for financial benefits from the resale to third parties.

Face Recognition: The photos used in virtual profiles are a digital identity of the user. Through advanced technologies such as (face recognition) these photos can be linked with information from other websites and services, where the same user has posted other elements, eventually leading to the collection of much more data for the user than he had in mind to reveal through the e-business.

Detection into the natural real world: Through new technological developments, there is a great possibility to identify a user in the real world by inspecting photos he has published in an online community (for example, a photo in front of his home). Users often do not realize how important it is to not publish photographs where the site is intuitive to users.

Metadata: Many social networking platforms allow users to mark their photos with metadata. These can be links referring an e-mail or a social profile account. This presents a risk for unwanted photo interface with personal data. Even if users keep security measures in respect of their personal photos, others have rights to interfere with them and retrieve sensitive personal details such as age of birth, home location, family members, etc. In addition, several photos contain data, such as the serial number of the camera, which could pose a threat to the user's privacy (Bonneau et al. 2009).

Pornography, trafficking, violence against women, and censorship

Another justification for the interception of internet communications often presented to the general public is that it is needed to combat the sexual exploitation of women and children and to prove that e-entrepreneurship is not a masculine issue. It is commonly known that there is no gender divide in e-business, and phenomena like the following that aim to harm women physically, psychologically, and mentally should stop appearing (Bianchi et al. 2008; Hafkin and Huyer 2006).

The picture that emerges from most analyses of new information and communication content is of a masculine rhetoric, and a set of representations which are frequently sexualized and often sexist. Pornography, e-mail harassment, 'flaming' (abusive or obscene language), and cyber-stalking are well documented. It is estimated that 10% of sales via the Internet are of sexual nature, whether in the form of books, video clips, photographs, online interviews, or other items. New technical innovations facilitate the sexual exploitation of women and children because they enable people easily to buy,

sell, and exchange millions of images and videos of sexual exploitation of women and children. These technologies enable sexual predators to harm or exploit women and children efficiently and anonymously. As a result of the huge market on the web for pornography and the competition among sites, pornographic images have become rougher, more violent, and degrading. Affordable access to global communication technologies allows users to carry out these activities in the privacy of their homes.

What is even more disturbing is the use of the Internet as a tool in the prostitution and trafficking of women. In 1995, an estimated 1.8 million women and girls were victims of illegal trafficking, and the numbers are growing. The Internet is used in multiple ways to promote and engage in the sexual exploitation and trafficking of women. Pimps use the Internet to advertise prostitution tours to men from industrialized countries. These men then travel to poorer countries to meet and buy girls and women in prostitution. Traffickers recruiting women from the Baltic States use the Web to post advertisements for unlikely jobs in Western Europe (such as waitress or nanny). Information on where and how to find girls and women in prostitution in cities all over the world is posted on commercial Web sites and non-commercial newsgroups. In 2001, the Council of Europe established a working group to study the impact of new information technologies on trafficking of human beings for the purpose of sexual exploitation.

There are numerous organizations working on the issues of women's trafficking and have done much to raise concern over the use of the Internet for trafficking women and children, and the explosion of pornography on the Internet. While recognizing that traffickers and pornographers have moved their businesses to the Internet, women's organizations have also been aware of the dilemma of calling for government measures to curb this.

One of the fiercest debates in the area of internet rights regards the issue of freedom of expression and censorship. Some organizations have used the presence of pornography on the Internet to call for stricter policies for monitoring and censoring content on the Internet, including the development of software devices that would track down the creators and consumers of pornographic materials. Other women's organizations have been at the forefront of pointing out the danger of inviting censorship measures that could very easily be extended to other content areas, and limit freedom of expression far beyond the realms of pornography and trafficking. Legislation can be interpreted widely, leaving it open for states to decide what they would consider 'illegal' or 'harmful practices'.

Above all else, women should be informed, made aware, included in the discussions and debates taking place around these trends, and consulted in the development of any policies and practices that are advocated by state agencies and other bodies.

Social engineering

What is mentioned before is the immediate relationship that connects the e-entrepreneurship with social networking. It is generally approved that every successful e-entrepreneur should be a well-informed social networking user. Once again, it is observed that women using social networking sites as a tool for their e-business promotion are willing to disclose and share much less information than men do because of their digital privacy concerns.

The term social engineering is referred to as a specific method of electronic attack, which is characterized as the biggest threat for the network security. The official definition says that social engineering is the action of oral guidance of individuals with aim to the detachment of information. Even if it is similar to the subterfuge or the simple fraud, the term is mainly connected with the deceit of individuals aiming at the detachment of confidential information that is essential for the access in some calculating system. Usually, the one that applies does not come face to face with the individual that deceits or induces (Gross and Acquisti 2005; Yang and Yang 2007; Eidlin and Appelbaum 1983).

The steps that an intruder follows in order to achieve intrusion in a network of computers with the methods of social engineering, are the following:

- He approaches in some way an individual who has permitted access in the network.
- He presents himself as a confident individual.
- He tries to extract information from the individual who approached, that places the safety of network at risk.

Absence of women in e-business

The gender distribution of ICT access is also skewed. ICT access by women tends to lag that of men, but the gaps are generally declining. However, the gaps remain large in older age groups and in areas of newer technologies (ICT Market 2012; International Telecommunication Union 2010; Montagnier and van Welsum 2006; Dutta and Bilbao-Osorio 2012).

The following figure looks at the presence of women in occupations that use ICTs. In most countries, women account for between 30% and 50% of employment in ICT-skilled employment according to the broad, ICT-using definition (Figure 1).

Figure 2 presents the number of e-entrepreneurs as a percentage of the total employed population by gender.

System security requirements

The fundamental safety requirements to a system are the confidentiality and the integrity of data, as well as the availability of the system. Figure 3 presents the interaction of fundamental security requirements in a system (Raykova et al. 2012).

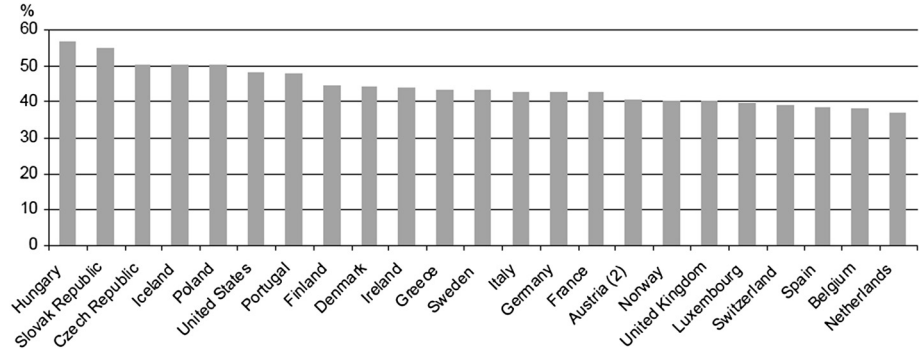

Figure 1 Share of women in ICT-using occupation (selected countries).

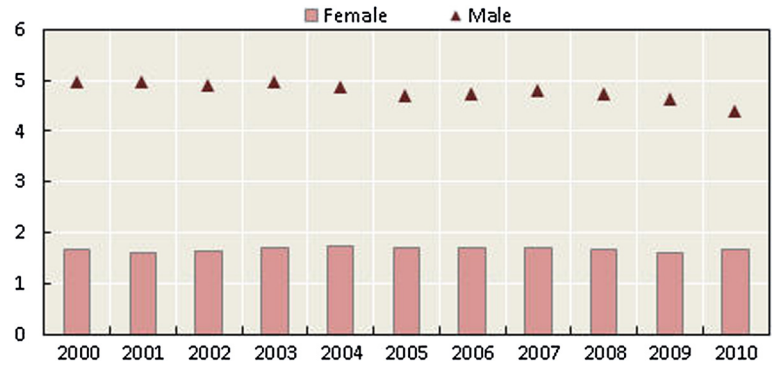

Figure 2 E-Entrepreneurship.

Confidentiality means prevention of unauthorized disclosure of information. Therefore, the data used for the delivery of services should be disclosed only to authorized persons. Integrity is the requirement of the unauthorized modification and deletion of data, as well as creating new data, i.e. to ensure the validity, accuracy, and completeness of the data during the import phase, treatment, and outcome of treatment. Finally, the availability is the property of a system to offer services that are accessible and without undue delay. This parameter is very important since majority of these are real-time systems and services are changing and improving while the number of users are continuously increasing.

Results and discussion

This section analyzes the results of the measured data. The data shown in Figure 1 clearly reveals a linear trend with women not preferring ICT-using occupations. The standard deviation result indicates that a typical point is about 40% in selected countries. It would be noticeable that the selected countries are mostly developed and the IT occupations are highly popular in the e-market. Moreover, it can be easily understood from the graph in Figure 2 that the relationship of e-entrepreneurship present a

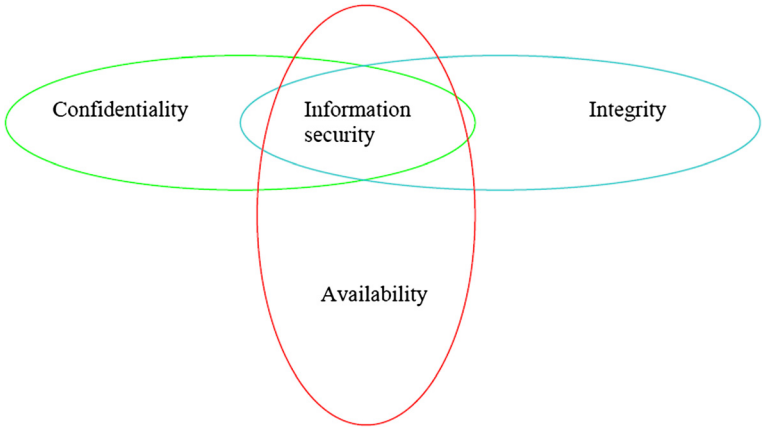

Figure 3 Interaction of fundamental security requirements in a system.

gender divide. The insecure online communities and the arising appearance of digital threats seem to discourage the female gender in interfering with e-entrepreneurship.

A comparison between the graphs in Figures 1 and 2 clearly underlines the absence of women from the e-commerce world due to the inadequate security and privacy policies in the online platforms.

A multi-faceted approach is needed to develop an integrated approach to e-commerce security. Each component of the e-commerce system should be robust and have its own independent security controls put in place.

Raising security awareness by contributing industry-wise initiatives and liaison with governmental and law enforcement agencies will help women e-entrepreneurs understand the threats and trends. Ensuring secured development methodologies which are used to undertake programming and security-best practices are being applied through the organization will build a solid platform from which to deter electronic crime. Using staff and website user security awareness training, data classification and protection and staff controls and checks will assist in reducing the vulnerabilities. Applying a strategy of 'defense in depth' to protect e-commerce systems will help mitigate the effect of botnet attacks, and a supported and maintained plan for incident detection, prevention, and management will need to be in place. As a result, the empowerment of women e-entrepreneurship is more than certain.

Conclusion

Never before has there been a greater need for e-entrepreneurs to protect their privacy and anonymity. With the rapid development of the ICTs, the computer systems contain more and more sensitive user data, and security requirements are growing explosively. For this reason, it is necessary to develop techniques to safeguard privacy, particularly for space-time data. Many questions arise about the way they manage their systems to orbit the data, the methods and the architectures of the systems that should be implemented to protect them, and how to combine all these methods in order to improve the applications and offer better services. Summing up, this article argues for a re-thinking about women and ICT usage with the prerequisite course on the improvement of telecommunications-information systems providing greater security and ensuring privacy that truly allow girls and women to become equal members of an information and digital network society.

Methods

This study applied quantitative method in order to analyze data and get important information such as demographic information of the respondents. This study employed a random sample technique for its respondents on the condition that the gender of the respondents was exclusively female. The graphs describe the presence of women in occupations that use ICTs in selected countries, as well as present the number of e-entrepreneurs as a percentage of the total employed population by gender.

Abbreviations

APT: Advanced persistent threats; CSRF: Cross-site request forgery; ENISA: European network and information security agency; ICTs: Information and communication technologies.

Competing interests

The author declares that he has no competing interests.

Authors' information
AKM is a Ph.D. researcher at the University of Piraeus. Her interest field is Network Security and Privacy. She is occupied as an IT-instructor as well as a network security consultant.

Acknowledgements
This article was prepared under the European Conference "More technologies? More Women Entrepreneurs".

Received: 20 November 2012 Accepted: 7 May 2013
Published: 25 May 2013

References

Acquisti, A, Gritzalis, S, Lambrinoudakis, C, & de Capitani Di Vimercati, S (2007). *Digital Privacy*. NY: AUERBACH Publications, Taylor and Francis Group.

Bianchi, G, Boschi, E, Gaudino, F, Koutsoloukas, EA, Lioudakis, GV, Rao, S, Ricciato, F, Schmoll, C, & Stohmeier, F (2008). *Privacy-preserving network monitoring: challenges and solutions*. Stockholm, Sweden: ICT Mobile & Wireless Communications.

Bonneau, J, Anderson, J, & Danezis, G (2009). Prying data out of a social network. In *the first international conference on advances in social networks analysis and mining* (pp. 249–254). Piscataway: IEEE Xplore.

Dutta, S, & Bilbao-Osorio, B (Eds.) (2012). *Global information technology report 2012: living in a hyperconnected world*. Geneva: World Economic Forum and INSEAD.

Eidlin, F, & Appelbaum, R (1983). *Social Science, Social Engineering, and Public Policy*. Chicago: American Political Science Association Proceedings.

European Network and Information Security Agency. (2009). In G. Hogben (Ed.), *Security Issues and Recommendations for Online Social Network*. ENISA: ENISA Position Paper No1. Crete.

Gillwald, A (2001). Telecommunication Policy and Regulation for Women and Development. *The Southern African Journal of Information and Communication, 1*(1).

Market, ICT (2012). *Trends, Analysis & Statistics*. http://www.reportlinker.com/report/best/keywords/ict?utm_source=adwords2&utm_medium=cpc&utm_campaign=High_tech_and_Media_ROW&utm_adgroup=Ict_ROW&gclid=CKPSqLPovrcCFczC3godh2QAKg. Accessed 10 Sept 2012.

International Telecommunication Union. (2010). *Measuring the Information Society*. Geneva: International Telecommunication Union.

Gross, R, & Acquisti, A (2005). *Information revelation and privacy in online social networks (The Facebook case), Pre-proceedings version*. Alexandria: ACM Workshop on Privacy in the Electronic Society (WPES).

Hafkin, N, & Huyer, S (2006). *Cinderella or Cyberella? Empowering Women in the Knowledge Society*. Bloomfield, CT: Kumarian Press.

Huyer, S, Hafkin, N, Ertl, H, & Dryburgh, H (2005). Women in the information society. In G. Sciadas (Ed.), *From the digital divide to digital opportunities: measuring infostates for development* (6th ed.). Montréal: UNESCO and Orbicom.

Jones, H, & Soltren, JH (2005). *Facebook: threats to privacy*. Cambridge, MA: Massachusetts Institute of Technology http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf. Accessed 10 Sept 2012.

Martinez, J, & Reilly, K (2002). *Looking Behind the Internet to Enable Citizen Information Systems: Empowering Women for Public Policy Advocacy*. Santo Domingo: The United Nations International Research and Training Institute for the Advancement of Women (UN-INSTRAW).

Middleton, J (2011). *Broadband Boost Linked to Economic Growth*. Available at http://www.telecoms.com/33619/broadband-boost-linked-to-economicgrowth/

Montagnier, P, & van Welsum, D (2006). *ICTs and gender-evidence from OECD and non-OECD countries*. http://unctad.org/sections/wcmu/docs/c3em29p025_en.pdf. Accessed 15 Sept 2012.

United Nations Information and Communication Technologies Task Force. (2008). *Measuring ICT: the global status of ICT indicators (Partnership on measuring ICT for development)*. New York: United Nations Information and Communication Technologies Task Force.

Please rob me. (2010). *Raising awareness about over-sharing*. http://pleaserobme.com/why Accessed 29 Jan 2012.

Raykova, M, Cui, A, Vo, B, Liu, B, Malkin, T, Bellovin, S, & Stolfo, SJ (2012). Usable, secure, private search. *Piscataway: IEEE Security & Privacy, 10*(5), 53–60.

Yang, L, & Yang, SH (2007). A framework of security and safety checking for internet-based control systems. *International Journal of Information and Computer Security, 1*(1/2), 185–200.

doi:10.1186/2192-5372-2-7
Cite this article as: Michota: **Digital security concerns and threats facing women entrepreneurs.** *Journal of Innovation and Entrepreneurship* 2013 **2**:7.