International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.org & www.ijocit.ir
ISSN = 2345-3877

The Complex Case of Online Privacy for Iranian Users of Social Networks

Arash Shaghaghi[1], Bahram Sadeghi Bigham[2]

Department of Computer Science and Information Technology, Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran

ashagagi@iasbs.ac.ir[1], b_sadeghi_b@iasbs.ac.ir[2]

Abstract: While social networks such as Facebook and Twitter are censored within the Iranian network, the number of Iranian users that use such services is facing an outsized growth. As a result, an increasing number of Iranian users have taken the habit of using some type of anti-censorship tool to access blocked content, which is an act against the Iranian ICT laws by itself. At the same time, each year numerous cases of identity theft, robberies, harassment and alike are reported in countries such as United States that happen due to both technical glitches/misconfigurations by the service provider and the inconsiderate behavior of users when using those services. As a matter of fact, countries such as UK and US are making efforts to increase peoples' awareness about required security and privacy precautions and enact laws that support user's right of having online security and privacy. However, relevant literature review indicates that the Iranian authorities are mainly focusing on preventing and discouraging the use of social network tools and are unwilling to accept the increasing usage yet. In this paper we present our survey results among 511 Facebook users residing in Iran, which shows that Iranian users have a very limited knowledge about potential privacy and security risks of using anti-censorship tools and online social networks such as Facebook. We conduct a risk analysis based on surveyed facts and suggest recommendations on how to improve this condition.

Keywords: Privacy, Social Networks, Internet Filtering, Anti-censorship tool.

1. Introduction

The penetration of Internet in the Middle East is faster than the world's average and Iran has by far the highest number of users in the region [1]. Iran is known to be using tight Internet censorship both to protect its network from sophisticated foreign cyber-attacks and prevent access to "immoral" and certain political

websites [2]. Currently, social networking websites such as Facebook and Twitter are in the government blacklist and Iranian users are not expected to use these online services. At the same time, due to the current sanctions against Iran, many high profile online services ban requests originating from Iran [3].

Similar to citizens of countries with such restrictions or users in certain organizations, Iranian users could use some type of anti-censorship technologies to access blocked content. The estimates of the number of Iranian users on censored services such as Facebook indicate that the use of these tools is actually very high [4]. On the other hand, while being a member of online social network tools is not considered a cybercrime itself, the government has recently enacted laws that prohibit providing or re-distributing circumvention tools [5]. Therefore, the government does not educate or inform users on how to protect their data and security while using the restricted online services or using the circumvention tools. In other words, as the users leave the safe borders they are highly vulnerable to online threats.

The situation worsens considering that today social networking and cloud-based services are increasingly important due to the recent surge in online interaction and sharing of personal information online has become the rule for users around the world [6]. Although countries such as United States or United Kingdom advise their users to be cautious when sharing information on social network websites and provide multiple sources of information on how to do this, studies have shown that users are far away from making well-informed decisions regarding the amount of private information they reveal online [7]. The numerous incidents of identity theft, embarrassment [8], robberies and loss of employment [9] reported each year highlight an important negligence among users.

In this paper we start by presenting some required background information in Section 2. Thereafter, in Section 3, we describe our survey structure and format regarding Iranian users' habits when using international social network tools and their knowledge about potential security and privacy threats. Referring to the survey results available in Section 4, we include a security and privacy risk analysis relevant to Iranian users. We conclude by proposing future research directions.

Last but not least, the authors would like to emphasize that the paper is only conducting a study from an information security and privacy expert point of view and no part of this work should be considered out of this sole scope.

2. Background

In this section some background information is provided so that the reader has a better understanding about the purpose of this work and the current situation of key topics discussed.

2.1 Privacy

In this paper, we employ the definition of privacy by Westin, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated" [10]. United Nations Declarations of Human Right and many other international treaties recognize privacy as fundamental human right [11]. Moreover, respecting personal privacy of people is widely recognized and advised in Iranian-Islamic culture [12].

2.2. Privacy in Social Network Tools

On average, each Facebook user creates 90 pieces of content including photos and life event updates per month [13]. There are now more than one billion Facebook users and this is equal to the population of the whole world in 1804 [14]. Therefore, social networks are ideal for data mining and information gathering for both malicious and benevolent purposes. In fact, marketing companies, governments, thieves and hackers could all benefit from such information and this is the reason for such high monetary values assigned to major providers such as Facebook and Twitter [15].

Recently, several governments have enacted laws to enforce privacy preserving regulations and standards [16]. Nevertheless, the Internet has no governing or regulating body and businesses can still provide their product or services worldwide from countries with less control. At the same time, there are extended studies on privacy issues in social network tools and cloud-based services in the literature. These mainly aim to improve the privacy of online systems platform by improving the relevant technical details and/or improving the usability of systems.

On the other side, giant service providers such as Google do not seem to be interested in improving users' privacy. For example, Google has been clear that Gmail users have no expectation of privacy when using their service [17]. Similarly, Facebook has been charged by the watchdog organization Privacy International for severe privacy flaws and the concerns about data matching, data mining and transfer to other companies [18].

Studies have shown that even users with well computer literacy and educated about online privacy are still not cautious regarding their social network profile privacy settings and the private information they reveal on such systems

[18]. In fact, researchers associate most of the privacy and security incidents to improper and uninformed decision making of users [7].

2.3 Social Networks in Iran

Currently, the government blocks Iranian users' access to popular social networks such as Facebook and Twitter [19]. As mentioned previously, although being a member of these services is not considered a crime by itself, bypassing Internet filtering is against Iranian laws.

In order to allow users enjoy the benefits of such type of services, national social network websites such as Cloob.com have been designed and introduced but they have a very limited audience compared to international services [4]. In fact, officials have indicated that there are more than one million residents of Tehran on Facebook and international surveys estimate that Facebook has more than six million Iranian users – not counting Iranians who live outside of the country [1]. Moreover, the newly elected president of Iran and its colleagues in the government have recently started using Facebook to be in direct contact with the Iranian nation and their pages have attracted large number of audiences [20]. In fact, President Rouhani has been clear that he perceives important strategic potentials in social network platforms [21].

2.4 Internet filtering in Iran

Nowadays, Internet filtering is facing an upward trend and is applied in both western and developing countries [22]. In this manuscript, we are not interested to discuss the reasons of Internet filtering nor the ethical issues related to it.

Typically, Internet filtering is conducted at one or more of the following levels: national government, national or local ISP, operator of local network and software-based filters on individual devices [23]. In Iran, The Ministry of Communication and Information Technology of Iran applies Internet filtering to protect the national security and community-accepted standards of decency. The Working Group for Determining Criminal Content is identified as the main responsible authority for defining blocked or unacceptable content [24]. While Iran is believed to have one of the worlds most sophisticated filtering and monitoring systems [23], there is no official record indicating what filtering mechanisms are being used. Previous research has indicated that other than well-known filtering solutions such as IP filtering, Content-Based Filtering and Port Blocking, software level technologies such as SmartFilter™ and Hardware level technologies such as Deep Packet Inspection (DPI) devices are being used [23, 24, 25].

2.5. Circumvention tools

By definition, a filtering or censorship circumvention tool should allow censored users connect to uncensored Internet securely and anonymously. However, studies have shown that only few of available tools ensure security and privacy of their users [2]. To be effective, such tools should make censorship too costly or lead the technology evolution [25]. Circumvention methods could be simple techniques, protected communications or complex computer programs. Essentially, all these methods redirect users' requests to an intermediary computer, known as proxy, which is located in a different network and is accessible to the censored user [26].

The number of commercial anti-filter or anti-censorship applications has been steadily increasing between 1993 and 2010 and governments with less Internet censorship such as United States have had a key role in their development [25]. There are five main methods used in commercial anti-filtering applications namely, HTTP Proxy, CGI Proxy, IP Tunneling, Re-routing and Distributed Hosting. Recently, the number of IP Tunneling and Re-routing based tools has increased but still HTTP Proxy tools such as UltraSurf are the most used solutions [23, 27]. In another categorization, circumvention technologies have either centralized or Point-To-Point (P2P) architecture [28]. In the former, all the censored users' data are transmitted to one intermediary while in the latter, data are sent to multiple peers. In other words, in a centralized system users' trust is dependent on the main provider and in a distributed system trust is distributed among multiple peers. Therefore, a distributed architecture, such as the one used by TOR, could lead to an improved privacy, anonymity and a better performance. Nevertheless, in a distributed architecture the provider costs are much higher with a large user base and therefore centralized architectures such as those used in HTTP proxy tools are preferred [24, 28].

3. Research Methodology

3.1 Sampling and Research Setting

An online survey was conducted in summer 2013 to evaluate the knowledge and familiarity of Iranian Facebook users, residing in the country, about using commercial anti-filtering tools and the potential privacy and security threats that could affect them when using social network tools. Generally, online surveys rely on self-section mechanisms and make randomized sampling difficult [18]. Our online survey had 511 participants and, according to Morgan Sample Size for Research Activities, for the estimated six million Iranian users on Facebook with 97.5% confidence level this sample size has 5% margin of error. This is assumed to be a relatively good sample as this is the first survey

of its kind in the region and there are certain limitations on sending public invitations.

The online survey was advertised on popular Iranian Facebook pages and other websites that could have had Iranian visitors with a profile on Facebook. Five participants were selected in random and received 500,000 Rials, the currency used in Iran, as appreciation for their contribution – all participants were informed about this potential reward before starting the survey. The questionnaire was designed using SurveyMonkey and all of the data was collected anonymously. There was no time limitation for answering the questions and no question could have been left unanswered. The purpose of the study was described in the first page and a short video was made available to participants to teach them about how their data will be used and stored. All the participants of the survey indicated that they have a Facebook profile and, in fact, those without this were asked to leave the survey at the beginning. Also, the questions were available both in Persian and English and the grammar and structuring of questions were analysed by three other academics. Moreover, as this was a long questionnaire (15-20 minutes) and Internet connections are unstable outside of main cities of Iran, a participant had the choice of answering questions in multiple tries and with the help of a randomly generated code they could resume from where they left of – no registration was required.

3.2 Survey Measures and Data Collection

The online questionnaire consisted of 34 multiple-choice questions. The questions surveyed participants' knowledge and usage of anti-censorship tools, privacy and security threats relevant to the use of anti-censorship tools, general knowledge and familiarity about potential privacy and security threats when using Internet and social networks, basic information regarding Facebook habits, familiarity with privacy matters of Facebook and participants' demographic information. The survey started by asking whether Internet filtering affects participant's everyday tasks – excluding using social networks - and how often s/he uses anti-censorship tools. Thereafter, in order to understand users' knowledge about anti-censorship tools, they were asked 1) how do they decide which tool to use, 2) how they learn the usage of the tool, 3) if they know that using and re-distributing anti-censorship tools are illegal and 4) if they are aware of threats to information privacy when using commercial anti-censorship tools. Thereafter, in order to have a better idea about the participants' IT and information security awareness a series of questions asked how much participants use Internet, the main reason that participants use Internet for, if they

believe they have sensitive information stored in social network websites or cloud-based services, if they have heard about Stuxnet and other serious IT security risks targeting Iran, how did they learn to use social network tools such as Facebook, and if they are familiar with security and privacy risks affecting users of social network websites. Moreover, they were asked if they use Iranian social networks such as Cloob.com and if they know where they should refer to in case of a social network related privacy violation incident such as identity theft. The penultimate page of the questionnaire had a series of questions to help us understand about participants' general habits when using Facebook. We asked them about the time they spend on Facebook each day, how often they visit Facebook per day, how long each visit lasts, what type of personal information they share on Facebook and if they used their real name for their profile. Additionally, they were asked if they are familiar with Facebook privacy settings, if they have restricted their profile to Friend or Public, and how many Friends they have and how much they know these Friends in the real world. This section was finished by asking the participant if they knew about the government members' pages on Facebook and wondering in case Facebook and Twitter were not filtered, would they still use anti-censorship or anonymity tools to access Facebook or Twitter. Finally, some demographic information such as age range, level of computer literacy, gender and the latest academic degree were asked.

3.3 Survey Findings

218 of participants were Female and 293 were Male. Among participants, 58% had at least a bachelor degree or were an undergraduate student, 20% had no academic education and the rest had a postgraduate qualification. The majority of respondents (63%) were between the ages of 18 and 35, 25% were between 35 and 55, and 12% were above 55 or less than 18 years old. 48% of attendees classified themselves as being average computer users, 28% believed they are amateurs and 24% claimed they have computer skills above average. 52% of respondents indicated that are affected by Internet filtering in their everyday online tasks and all the participants indicated that they use anti-censorship tools at least once the other day and not just for social networks. In fact, half of the respondents keep them open even after visiting a censored content. 65% of respondents find out about an anti-censorship tool from a friend or relative and 29% mentioned that the same person taught them how to use the tool. Furthermore, 40% stated that they found out about the tool from search engines or forums. Almost half reported that they knew about the illegality of

anti-censorship tools and only 17% of respondents believed such tools may endanger their information privacy. 70% of respondents considered using social networks one of the main reasons of using Internet and 66% believed they have sensitive information stored on social networks or cloud-based services. Most respondents knew about the multiple foreign cyber-attacks against Iranian network but only 23% knew about privacy and security threats in social networks and they thought such warnings are mainly rumors to discourage the use of these services. Furthermore, 30% knew the difference between secure and non-secure connections such as HTTPS and HTTP and only 6% of attendees knew about using MD5 to verify a file download from Internet. The majority of respondents learned about Facebook intuitively or with a help of a friend who is already a member. 22% indicated that they use Iranian social networks actively; and only 34% knew that the Iranian Cyber Police would assist them if they face privacy and security incidents on social networks. Half of the participants had their Facebook account for more than a year, 56% checked this account daily, more than half of attendees spend between 15 and 45 minutes on each visit. On the other hand, 12% of respondents indicated that their Facebook is always open on their mobile device. 60% of attendees indicated that they provide real personal information such as relationship status, date of birth and work or education details and 56% of respondents used their real names for their profiles. 63% knew about Facebook privacy setting and yet only 25% have applied some form of privacy preserving restriction to their profile. 85% of respondents indicated that they have not always known a Facebook Friend before accepting his/her request. Most participants knew about the new presence of the government on Facebook and Twitter and found it ambiguous as such services are blocked for the people. Finally, only 20% of attendees would still use anonymity services such as TOR for accessing social network tools if they were not censored anymore.

4. Discussion

We now analyze the results of our survey from an information security expert viewpoint. We have identified four main categories of risks. Each category is analyzed in two levels namely, Users and National Security.

4.1 Risks Relevant to Limited Knowledge and Improper Use of Filtering Circumvention Tools

The number of Iranians on Facebook is an immediate indication of the high usage of anti-filtering tools and the ineffectiveness of current censorship. As the results indicate, only very few users have information about potential threats of using these tools and the majority have learned about circumvention tools from unreliable

sources. More importantly, users do not just use anti-filter tools for social network websites and many have indicated that they use them during their everyday browsing such as checking email.

The current situation could help an attacker to gain users trust and distribute a working but malicious circumvention tool. For example, a Trojan like application that allows browsing censored content but monitors and stores all transmitted communication. The attacker could use the transmitted data to learn authentication information and sensitive information such as email contents and banking details. Moreover, a sophisticated attacker could modify the transmitted information coming from or going to the user. Now, if the user has sensitive information that is strictly confidential that if revealed could endanger the government or the whole country, then this case should be dealt with at national security level.

The current condition could result in several other attack scenarios such as delivering malware through the data that the program transmits in the background or send a malicious file along with the original file to the victim machine.

4.2 Risks Relevant to Limited Knowledge and Improper Usage of Social Network Tools

The findings of our study confirm that Iranian users are following the international trend and are becoming more and more accustomed to share information online and interact through social networks. Improved connections and the availability of Third-Generation (3G) mobile networks are facilitating this shift of interaction. In fact, our survey indicates that an interesting majority has no problem with starting relationships on social networks. However, the users seem to have a very limited knowledge about the potential threats to information privacy and security when using these tools. This situation is very similar to the time social networks started to become popular in western countries. As a matter of fact, criminals exploited this vulnerability and committed crimes such as robberies and identity theft. For example, several robbery incidents happened when a user Checked-In to a location far away from his hometown and a fake or malicious friend used this information to plan the best time to enter into the victim's house [34]. Moreover, several cases have been reported that Facebook users have lost their jobs due to uploading offending posts against the company or the manager they work for [35].

Referring to the recent reports about United States National Security Agency (NSA) surveillance on the Internet we note that social networks are one of the main platforms that foreign secret agencies use to gather information

about humans all around the world [30]. As discussed in Facebook Iceberg Model [18], Facebook's visible part is innocent looking and is all about social networking and entertainment. The invisible part of the iceberg is where huge invasion of privacy, data aggregation and exploitation by third parties occur. In fact, Facebook or Twitter privacy settings are only applicable to the visible part and have no effect on the hidden mining of information [18]. When we consider international social networks from this viewpoint then it becomes a national security concern.

While multiple cases have been reported that Facebook has enabled the local police to find criminals by circulating their details, the same approach could be used to disseminate false information. For example, recent fake profiles related to the Iranian government members that distribute false information to intimidate individuals or the government.

4.3 Risks Relevant to Limited Education and Awareness in Information Security Topics

The survey results indicate a relatively limited knowledge about information security and privacy topics among attendees. Although the majority knew about recent cyber-attacks against Iran, they mainly considered them to be against the government not the people. However, reports indicate that the Middle-East region has the highest level of cyber-attacks against users and communications networks have very low security compared to countries such as the UK. On the other hand, it is noted that the majority of Iranians draw a line between real and virtual life and they do not consider online risks seriously. The increasing numbers of Iranians using Internet with such limited privacy and security awareness could impose serious risks both to themselves and the government. The risks involved with use of anti-censorship tools and social network, as discussed previously, are good examples for this claim.

Countries such as United Kingdom and United States are investing to increase the number of information security [32] and privacy experts and consider the presence of an Information security expert an essential requirement for any business. Moreover, these countries are making huge investments to improve users' awareness about online threats [31]. For example, the Australian government holds a national online privacy campaign and promotes online privacy preserving strategies [33]. As discussed in subsection 2.2, governments are also enforcing laws that obligate service providers to give a higher priority to users' privacy.

4.4 Risks Relevant to Low Level of Trust to Government Precautions

Although bypassing Internet filtering is against the Iranian laws, it is still reasonable to expect that the government should support and assist those who pass the safe borders. Currently, there are no laws to protect users when using censored materials and especially social network tools. The Iranian Cyber Police have recently announced that will they consider cases of privacy violation in social networks such as Facebook. However, as there are no supporting laws this seems to be a political gesture rather than a real solution. Furthermore, it is not clear that in such cases the victim will be fined for bypassing filtering or not. Furthermore, topics such as "Halal Internet" [29] have lowered people's trust in the government precautions. In fact, it seems that the government is trying hard to dissolve the problem rather than find practical solutions to solve it. Another solution to the rise of social networks such as Facebook was the implementation of Iranian equivalents such as Cloob.com. Although the idea was inspired from popular social networks in China, yet due to the limited provided features they are not popular.

The low level of trust between people and the government in this sector could lead users trust foreign entities and this could affect the national security.

5. Conclusion and Future Work

As the survey results confirm, the current government strategies towards information privacy and security seem inappropriate. Our study also confirms that current restrictions have not been successful in restricting user's access to blocked content and ensuring national security considerations. Furthermore, although the majority of our participants knew about the illegality of using anti-filtering tools, they still used them. Findings suggest that the level of information security and privacy awareness in Iran is very low compared to the developed countries. At the same time, the usage of social network tools and anti-censorship is increasing day by day and this could lead to serious threats to people and government. Recently, there have been news about removing filtering for Facebook and Twitter and we believe without proper strategies this could result in catastrophic results. In fact, as the president of Iran stated new strategies need to be defined to cope with the current situation.

At this stage, with the consideration of risks discussed in Section 5 we present some recommendations. Information security and privacy is a moving target that requires constant update in technical, regulatory and social areas. The very first step is to create research groups and educate academics in each of the aforementioned areas and benefit from experts'

opinion. In fact, such experts should be employed within small and large organizations and be involved within the organization daily process and decision makings. In general, a less Police-like approach towards Internet and filtering will help attract users' trust. There is an evident requirement of enacting supporting laws for assisting users when using social network tools such as Facebook. Moreover, holding privacy and security awareness campaigns throughout the country are immediate strict requirement if social network tools are going to be removed from the list of banned services. Otherwise, the nation will face the same problems that western countries have experienced with the increasing usage of social networks, if not worse. Furthermore, the Iranian Cyber Police should arrange for transparent negotiations with Facebook and other social networks and ask them to improve their usability for Iranian users. For example, they could ask these websites to make their Terms of Service (TOS) available in Persian language. Also, the government should plan to educate users about the threats involved when using anti-censorship and circumvention tools and if the current situation is not changed it should help them find the most secure and reliable tools.

The area of research proposed in this paper is still at the early stages in Iran. We suggest future researchers to identify practical solutions on how to approach the discussed risks and threats within the current constraints and conduct surveys at government level to evaluate their applicability. Also, further studies are required to have a clearer image about the current ICT situation in Iran.

Acknowledgment

We express our gratitude to reviewers and their helpful suggestions. The authors would also like to thank all the anonymous participants of our online survey.

References

[1] A. T. Chatfield and R. Akbari and N. Mirzayi and H. J. Scholl, "Interactive Effects of Networked Publics and Social Media on Transforming the Public Sphere: A Survey of Iran's Leaderless 'Social Media Revolution'", IEEE Computer Society, (2012) 2552--2562.

[2] F. Shirazi, "Free and Open Source Software versus Internet content filtering and censorship: A case study", Journal of Systems and Software, vol. 85(4), (2012) 920--931.

[3] D. McCullagh, "How U.S. sanctions hurt Iranian Internet activists", Retrieved 04.09.2013, Available online at: http://news.cnet.com/8301-31921_3-57402034-281/how-u.s-sanctions-hurt-iranian-internet-activists.

[4] J. Knowles, "58% of Iranians use Facebook despite blocks and censorship: study finds", Retrieved 22.08.2013, Available online at: http://thenextweb.com/me/2012/11/08/iranian-online-research-panel-releases-its-latest-study-into-attitudes-and-behaviours-online-inside-iran.

[5] A. Dehshiri, "Legality of Bypassing Internet Filtering in Iran", Retrieved 31.07.2012, Available online at: http://cgcsblog.asc.upenn.edu/2013/06/10/legality-of-bypassing-internet-filtering-in-iran/.

[6] B. Kцnings and D. Piendl and F. Schaub and M. Weber, "PrivacyJudge: Effective Privacy Controls for online Published Information", SocialCom/PASSAT, IEEE, (2011) 935--941.

[7] J. Fogel and E. Nehmad, "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns", Computers in Human Behavior, Computers in Human Behavior, vol. 25, 153--160.

[8] D. Barret and M.H. Saul, "Weiner Now Says He Sent Photos", Retrieved 20.08.2013, The Wall Street Journal.

[9] T. Monkovic, "Eagles employee fired for Facebook post", Retrieved 20.08.2013, The New York Times.

[10] A.F. Westin, "Privacy and Freedom", 1970, Bodley Head.

[11] A. Acquisti and S. Gritzalis and C. Lambrinoudakis and S. di Vimercati, "Digital Privacy: Theory, Technologies, and Practices", 2007, Auerbach Publications.

[12] A. Rasooli, "Personal and Public Privacy under the Eight Terms of Imam Khomeini Command", Retrieved 20.09.2013, Available online at: http://rasekhoon.net/article/show/187051.

[13] Facebook Statistics, Available online at: http://www.facebook.com/press/info.php?statistics.

[14] R.J. Rosen, "Facebook's population is now as big as the entire world's was in 1804", Retrieved 19.09.2013, Available online at: http://www.theatlantic.com/technology/archive/2012/10/facebooks-population-is- now-as-big-as- he-entire-worlds-was-in-1804/263250.

[15] J. Kiss, "Facebook's value climbs above $100bn for first time", Retrieved 18.08.2013, The Guardian.

[16] N. Singer, "An American quilt of privacy laws, incomplete", Retrieved 02.08.2013, The New York Times.

[17] "Google says email users have 'no legitimate expectation' of privacy", Retrieved 17.08.2013, Euronews, Available online at: http://www.euronews.com/2013/08/15/google-says-email-users-have-no-legitimate-expectation-of-privacy.

[18] B. Debatin and J. P. Lovejoy and A. Horn and B. N. Hughes, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences". Journal of Computer-Mediated Communication, vol. 15(1), 83--108.

[19] N. Karimi, "Iran restores blocks on Facebook, Twitter", Retrieved 05.10.2013, USA TODAY, from http://www.usatoday.com/story/news/world/2013/09/17/iran-restores-blocks-on-facebook-twitter/2824479/.

[20] "Iran foreign minister Zarif tweets happy Jewish New Year", Retrieved 11.09.2013, The British Broadcasting Corporation (BBC), from http://www.bbc.co.uk/news/world-middle-east-23990717.

[21] "Iran Rethinks Facebook under Rouhani", Retrieved 01.10.2013, Al-Monitor, Available online at: http://www.al-monitor.com/pulse/originals/2013/09/iran-reconsiders-facebook.html.

[22] "Internet censorship listed: how does each country compare?", Retrieved 05.09.2013, The

Guardian, Available online at: http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list.

[23] S. N. Hamade, "Internet Filtering and Censorship, Information Technology: New Generations", IEEE Computer Society, (2008) 1081--1086.

[24] Reporters without Borders, "Iran", Retrieved 20.09.2013, Available online at: http://surveillance.rsf.org/en/iran/.

[25] C. S. Leberknight, M. Chiang, H. V. Poor, and F. Wong, "A taxonomy of Internet censorship and anti-censorship", Available online at: http://www.princeton.edu/~chiangm/anticensorship.pdf.

[26] S. Burnett and N. Feamster and S. Vempala, "Chipping away at censorship firewalls with user-generated content", Proceedings of the 19th USENIX conference on Security, (2010) pp. 29.

[27] H. Roberts, "Circumvention Landscape Report: Methods, Uses, and Tools", The Berkman Center for Internet and Society at Harvard University, 2007.

[28] "How to Bypass Internet Censorship", Circumvention Tools, Retrieved 20.08.2013, Available online at: www.howtobypassinternetcensorship.org/files/bypassing-censorship.pdf

[29] D. Carrington, "Iran tightens grip on cyberspace with 'halal internet'", Retrieved 12.07.2013, The Cable News Network (CNN).

[30] J. Ball and J. Borger and G. Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", Retrieved 12.11.2013, The Guardian, Available online at: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[31] I. Barker, "UK government launches cyber security awareness campaign", Retrieved 11.10.2013, BetaNews, Available online at: http://betanews.com/2013/06/24/uk-government-launches-cyber-security-awareness-campaign/.

[32] "£7.5m university fund to train cyber security experts", Retrieved 11.10.2013, The Guardian, Available online at: http://www.theguardian.com/media-network/partner-zone-infosecurity/university-train-cyber-security-experts.

[33] "Privacy Awareness Week", Retrieved 15.07.2013, Available online at: http://www.privacyawarenessweek.org/2012/oaic/index.html.

[34] N. Bilton, "Burglars Said to Have Picked Houses Based on Facebook Updates", Retrieved 19.07.2013, The New York Times, Available online at: http://bits.blogs.nytimes.com/2010/09/12/burglars-picked-houses-based-on-facebook-updates.

[35] D. Kerr, "Facebook updates could cost young people jobs: study finds", Retrieved 25.08.2013, CBS News, Available online at: http://www.cbsnews.com/8301-205_162-57586908/facebook-updates-could-cost-young-people-jobs-study-finds.

Authors profile.

Mr. Arash Shaghaghi

Arash Shaghaghi is currently a PhD candidate and researcher in Research School of Computer Science at the Australian National University (ANU). He holds an MSc Information Security from University College London (UCL), BSc Information Technology from Heriot-Watt University and BSc Information Technology Engineering from Institute for Advanced Studies in Basic Sciences (IASBS). His current area of research and expertise is Information Privacy and Computer Security.

This paper was written and submitted while Arash was an Honorary Research Assistant at UCL and a Research Assistant at IASBS.

Dr. Bahram Sadeghi Bigham

Dr. Bahram Sadeghi Bigham is an Assistant Professor in Computer Sciences and dean of the Department of Computer and Information Sciences at the Institute for Advanced Studies in Basic Sciences (IASBS), where he is recognized as the founder and director of the RoboScience lab. Dr. Sadeghi is the founder and the general chairman of the International Conference on Contemporary Issues in Computer and Information Sciences (WWW.CICIS.IR). His research interests are in the areas of Algorithms, Computational Geometry, Data Mining, Artificial Intelligent and E-learning. He is interested in applications of CG in robotics problems (robot motion planning, robot vision and ...) Prior to arriving at IASBS, Dr. Sadeghi worked as a Postdoctoral Fellow at the University of Cardiff in the School of Computer Science. In June 2008, He completed his Ph.D. at Amirkabir University of Technology (Tehran Polytechnic), where he also completed a M.Sc. in 2000. His B.Sc. is from University of Birjand.

