Telematics and Informatics 33 (2016) 109–128

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

User awareness and tolerance of privacy abuse on mobile Internet: An exploratory study

Cormac Callanan [a], Borka Jerman-Blažič [b,*], Andrej Jerman Blažič [c]

[a] International Postgraduate School Jožef Stefan and Aconite, Ireland
[b] Institute Jožef Stefan and University of Ljubljana, Faculty of Economics, Slovenia
[c] International Postgraduate School Jožef Stefan, Jamova 39, Ljubljana, Slovenia

ARTICLE INFO

Article history:
Received 24 October 2014
Accepted 10 April 2015
Available online 21 May 2015

Keywords:
Mobile services affordability
Conceptual model
Security technology
User privacy and security
Circumvention tools
Network market development

ABSTRACT

The paper presents the results of an exploratory study about the level of privacy abuse and the awareness level of users when communicating and using mobile Internet. The study looks into the relationships and associations between the telecommunications market developmental level, the wealth of a country, users' skills, the affordability of mobile technologies, the level of user tolerance of state-mandated content censorship, and related privacy threats. The results and findings are drawn from a collection of data gathered from ten countries which have a low reputation for respecting human rights. These countries are primarily Asian or African states. Differences within the user community tolerance levels are discussed from the perspective of the key parameters which define the level of development of the information society and also the user skill levels. For a better understanding of the issue, a brief introduction explains the capacity of smartphones to ensure user privacy, and availability of the circumvention tools for smartphones.

1. Introduction

The International Telecommunication Union (ITU) is a specialized UN agency that is responsible for the ICT-related issues, and the primary official source for global ICT statistics concerning the spread of information and communication technologies used to measure the level of the information society development all over the world. The ITU records show that the cellular mobile communications growth curve has flattened out over the last few years, reaching 96% penetration by the end of 2013 while mobile broadband access continues its steep rise with an average annual growth rate of 40%. The fixed-broadband market is still growing, however, compared to the mobile its growth is slower but steady across both developing and developed regions. As a consequence of the strong growth in the mobile-market uptake, the household Internet access growth has also accelerated over the last years, mainly in the emerging economies, and reached a global penetration rate of over 40% by the end of 2013 (ITU, 2013). According to the Internet Society Report for 2013 (ISOC 2013), the number of mobile broadband Internet subscribers worldwide is close to two billions, which is three times the number of fixed broadband Internet subscribers. Many developing countries with limited fixed network infrastructure opted for the wireless broadband services to foster their economic growth. These are now offered in over 100 countries all over the world. In these countries, the wireless Internet access – usually through a mobile broadband network via a fixed wireless network or a satellite – is often the only alternative to a fixed network infrastructure. Studies (Broadband Commission for Digital development

* Corresponding author. Tel.: +386 1 4773408.
E-mail address: borka@e5.ijs.si (B. Jerman-Blažič).

http://dx.doi.org/10.1016/j.tele.2015.04.009
0736-5853/

and Cisco, 2013) claim that the use of mobile Internet networks and devices will continue to grow, driven by an ever-increasing supply of mobile applications and services, and will contribute to countries' economic development. The strong link between the mobile market uptake and service affordability, measured as a percentage of GNI (Gross National Income), will continue to shape the mobile market with the launch of new applications and new challenges. Applications for sensors, cameras, GPS and other in-built components introduce many new services; however, they also give birth to new challenges such as user privacy violations and data protection vulnerabilities. In general, users expect the base framework of a mobile device to be secure or sufficiently attentive to inform the user about the potential risks of malware intrusion or an interception tool that is part of a downloaded mobile phone application or introduced unnoticed by the network operators. The same applies to the users' expectations regarding their trust in the neutrality of service or network operators (Zhen et al., 2013).

Mobile devices are persistently connected to a radio data network all day, every day. The radio data network is managed and controlled by a network operator. This operator can manage the network and handsets remotely, with little or no knowledge or consent of the end user (Cisco, 2014). In addition, as a by-product of the mobile network design, the operator can easily access large volumes of personal data (e.g., individual user's movements, locations, communication exchange, visited websites, and downloaded content) on every handset connected to the operator's network (Liang and Yeh, 2011). In short, such handsets are sophisticated devices that include all the elements of an excellent covert monitoring tool.

Since mobile technologies are in use around the globe, there are numerous manufacturers designing, developing and selling equipment that can monitor and intercept mobile communications. This enables the data content to be passed to mobile operators, states agencies, companies, and sometimes end users (Enck et al., 2009; Jamaluddin et al., 2004). Tools and applications that are designed to prevent the monitoring or Internet-content blocking, known as the circumvention technology tools, as well as other security systems, were mainly created by the developed countries in the past, but were also used elsewhere. In some countries, vendors or operators are legally bound to offer a "backdoor" device entry to the government intelligence agencies. With the arrival of the user communication and movement monitoring tools, the use of the circumvention tools started to grew among the general public, especially when open source solutions became publicly available, such as Tor (Tor, 2012). These tools are widespread across the developed world, in the countries with high levels of democracy and human-rights protection (Maitland et al., 2012). Nevertheless, the studies have shown that even there, most users do not have sufficient technical knowledge or skills to download and use the privacy protection tools (Felt et al., 2012). On the other hand, the development of security and safety strategies for the mobile network users in the less developed countries with lower levels of human-rights protection proved to be complicated. Traffic monitoring and Internet-content blocking are frequently applied, but not sufficiently studied due to the difficulties in surveying the user communities. The applied restrictive measures are mainly justified by a state adopted strategy (Wustrow et al., 2011) that acts to restrict the information flows. These measures include limitations to the on-line information access, message filtering, and the prevention of dissemination of independent information. Furthermore, users are not familiar with the possibilities offered by the tools for communication security provision, privacy protection, and censorship circumvention.

Given these conflicting elements, the current study is one of the first attempts to investigate the influence of the information society development level on public awareness about security threats and user attitudes towards the state imposed Internet-content censorship in the developing or emerging economies with a lower level of human rights protection. In particular, we have examined several user communities in an attempt to answer the following research questions:

1. Is there a strong correlation between the level of information society development and the level of user awareness of traffic monitoring and content blocking?
2. Are user skills enhancing users' capacity to recognize content blocking and monitoring?
3. How is affordability and accessibility of technology related to the user capability to use smartphone applications for better privacy protection?
4. Which entity is recognised by users as an entity responsible for Internet censorship, and how is this related to the level of information society development?
5. Which telecommunications market stakeholders and players are trusted by users to protect their privacy?
6. Is the user tolerance of the state applied Internet content censorship, introduced as a protective measure against harmful content, related to the level of information society development, and wealth of a country?

In addition, we compared the differences in a users' understanding of security and privacy among emerging and developing economies. The answers to research questions were derived from the collection of data gathered through an exploratory study implemented in Africa (Tunis, Egypt), the Middle East (Saudi Arabia, Syria, Iran, and Oman), Asia (Vietnam, China, Azerbaijan, and Uzbekistan), and Europe (Belarus). These eleven ten countries were selected on the basis of the human rights related criteria developed by Freedom House, an independent non-governmental organization dedicated to the protection of human rights around the world, and the Broadcasting Board of Governors (BBG). They were also involved in the data collection and management for the purposes of this study (Callanan and Dries-Ziekenheiner, 2012).

The goal of this research was to provide a conceptual model that can serve as a comprehensive research approach for further investigation of the user trust in the on-line services, and the correlation between the level of trust enjoyed by one of the telecommunications market stakeholders, countries' welfare, and the level of information society development.