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.

Our aim was to gain a better understanding of the situation, which is usually a precursor to new advanced and affordable IC technologies in the developing world. This direction is usually taken in order to build trust and confidence in the existing communication networks (Bury et al., 2010). We were aware of the challenges of obtaining information about emerging and developing countries users perception of security and their fears since it is not an easy task and depends on many factors. The same is true for the mapping of these perceptions into an actual policy for the promotion of "off-the-shelf" protection tools, such as the circumvention tools. However, we believe that it is necessary to investigate these complex relations in different parts of the world. Our findings should contribute to the provision of fair, secure and neutral network services, which are considered a prerequisite for further development of the information society around the globe.

The paper is organized in several sections. The introduction outlines the research initiative and the motivation. Section 2 provides information about the technical background and related studies with some technical insight. Section 3 presents a brief assessment of mobile devices that are most frequently used in the studied countries, and their limitations in terms of security and privacy. The fourth section presents the survey sampling, methodology and findings and the paper concludes with a section that discusses the results, and brief conclusions as well as recommendations.

2. Related works and brief technical background

Running applications and using a handset as a communications and working tool connected to a mobile network are by far the activities most exposed to threats (Fleizach et al., 2007). Not only are users exposed to various potential attacks with malicious code, the main privacy threat on the mobile networks is the collection of real-time data, which is generated from the use of mobile devices (Bellens et al., 2013). This does not apply to the text and voice data only since location data and other forms of online communications are among the key targets for the Internet-traffic monitoring and/or blocking operations. Physical access to a mobile phone is, conceivably, the most intrusive of all threats (Mylonas et al., 2013b). By gaining physical access, an attacker exposes the mobile device's storage media, leading to the possibility of extracting and disclosing the stored data and credentials. Close-proximity access (such as the near-field communications, tethered connections, and Bluetooth) can yield similar results. Privacy in a ubiquitous computing environment was studied a long time ago by Bellotti and Sellen (Bellotti and Sellen, 1993). They discussed various threats and classified them into the two categories of *technological threats* and *network-design threats*. In this paper we address both types of threats, and follow the understanding of the privacy provision as recommended by Price et al. (Price et al., 2005). According to them, the key enabler of privacy provision are fair information practices and technologies for supporting practices, such as user anonymity and the protection of data during service use, as well as subsequent data storage. Similar aspects of privacy were identified by Adams and Sasse (Adams and Sasse, 1999), and Bellotti and Sellens, who classified the areas where users can control the disclosure of data and, consequently, privacy. Joinson and coworkers (Joinson et al., 2010) confirmed that privacy and trust have a symbiotic relationship, and that users have fewer privacy concerns when they are faced with a trusted requestor. Although, literature defines different aspects of trust (Ažderska and Jerman-Blažič, 2013), the most general definition describes trust as a subjective probability that an entity will perform in an expected and beneficial manner, and refrain from causing unexpected harm (Ažderska and Jerman-Blažic, 2012a,b). This is similar to the institutional trust as defined by Grefen et al. (Grefen et al., 2003): "Trust is an implicit set of beliefs that the other party will behave in a dependent manner and will not take advantage of the situation." However, there are no guarantees in the current mobile networking setting that the data collected without users' consent and without any formal legal request would be used for non-harmful aims.

First, we wanted to determine, if the most popular mobile devices in a given country market with a given legal environment, including on-line content censorship, enable circumvention technology, and if the availability of technology influences the use of the circumvention tools. Fig. 1 illustrates the mobile device model, and the shared responsibility for the provision of security between the mobile device manufacturers and operators. The model clearly identifies, who is responsible for the implementation of a particular mobile device security feature (e.g., operation system (OS) or device developer), and which applications can be used to upgrade the current security levels (application store and user). Operational functionality of these features depends on the network capability and functionality which falls within the operators' domain.

Current developments in Internet technologies offer many simple circumvention tools for privacy provision, and content blocking evasion. They are designed to find paths to bypass Internet restrictions, and can be used for multiple purposes. They are considered the information systems security technologies (Straub and Nance, 1988; Straub and Welke, 1998; Dhillon and Torkzadeh, 2006; Dinev and Hu, 2007; Zafar and Clark, 2009). They bear similarities to the security technologies used in commercial settings. For example, the technologies and strategies used to mitigate the website blocking may be similar to those for the prevention of a denial of service attack on the network itself, since both attacks seek to restrict information dissemination. Security technologies are also denoted as "protective" tools when compared to the, negative "(harmful) or, positive" (productivity enhancing) tools. Protective tools are designed to neutralize or disable the negative technologies which differ from the positive technologies in that they provide less direct or only subtle benefits in terms of user security (Dinev and Hu, 2007). It is important to note that the research on security technologies is influenced by the trade-off between the enhanced security features and other factors, such as interoperability and standardization (Maitland et al., 2012). From the user device perspective, there are two main elements of the security tool design – it must be simple to use, and a device's technology design has to be compatible with the security technology complexity, which is influenced by the functionality of the communications network (Global Privacy Report, 2013).

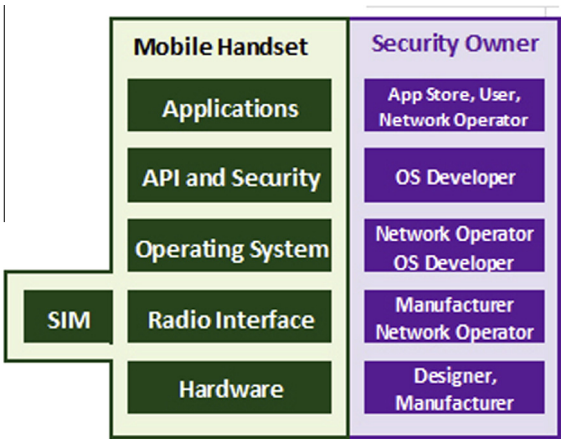

Fig. 1. Responsibility of security provision in mobile communications. SIM – Subscriber Identity Module, OS – Operating System, API – Application Interface.

Circumvention technologies which are currently in use have various technical requirements and mixed levels of effectiveness, depending on their intended use. The usability of circumvention tools may be hindered both by their added latency (Fabian et al., 2010) and the source, e.g., when developed by the non-profit and academic research organizations that typically lack resources for usability testing. Practical guides written by the organizations working in the field of human rights and technology provide comparative analyses and specific guidance for the appropriate use (Maitland et al., 2012) of the available tools. They classified the circumvention tools in two categories based on their functionality: the text or voice encryption only tools, and the "general circumvention tools". The general circumvention tools reroute the entire Internet traffic in the event of blocking or monitoring. They use the following security technologies:

- Virtual Private Network (VPN) application relays the communicated data to a location not visible to the monitoring entity. The application relays any content through the VPN tunnel set up between two Internet servers. Although encryption is commonly used as a part of this technique, this functionality is not always enabled by default. This circumvention application is also known as the tunneling. A tunnel is recognized by the operating system as a separate Internet connection, thus it can be used without any specific handset application settings. A critical problem occurs when the VPN fails since access to the remote public Internet website continues on the standard unprotected Internet connection without an alert to the user. .
- Proxy technology enables the evasion of the filtered or blocked access. Users ask the proxy server to access the blocked content on their behalf. As long as that proxy is not being blocked itself, the user gains access to the content bypassing the local filtering. Traffic to the proxy must be encrypted. The proxy servers are accessible through the web-based interfaces, which use either common or unique Internet based URLs (Universal Resource Locator). They provide access to the required information, and enable user anonymity. Examples of this technology include applications such as Proxify, Psiphon, Global Pass, SSH tunnels (Dusi et al., 2008), Corporate VPNs, Freegate, Ultrasurf, and Guardster (Freegate, 2012; Guardster., 2012; Evigator, 2012). Since the proxy computers (Proxy, 2012) are easily discovered and blocked, some proxy services manage to cycle their computers through a range of Internet protocol (IP) addresses to avoid any proxy server blacklists. The effectiveness of this evasion technique depends on the number of available Internet addresses (IP), and their distribution across the IP-address space. At a high level, this mechanism is used by popular services, such as Tor (Dingledine et al., 2004), Global Pass, and other tools enabling user device anonymisation. Servers providing user anonymity in e-mail communication through anonymous remailers or blog computers are also considered as a type of proxy server.
- Decoy technology enables clients to connect to any unblocked Internet hosting service provider. Decoy routing could be used to connect the user to a blocked destination without the cooperation of the user host (Karlin et al., 2013). For the operation of the later, two layers of the network connectivity are required: one Internet connection that is capable of reaching a third-party service, and another, with an overlay connection that is capable of carrying the actual data traffic that is being transported.

Circumvention tools that provide only encryption to covertly hide the covert traffic inside the communication channels are used for other types of communication data (e.g., images and video files) via techniques known as steganography. Steganography is a method used to encrypt a message in a transferred image. These are particularly useful when the encrypted traffic is considered suspicious or is simply blocked. Some examples of the covert channels include TCP-over-DNS (Burnett et al., 2005), and CovertFS (Baliga et al., 2007).

3. Popular handsets and their security technology

Currently, many different circumvention technologies are in use, and this is one of the reasons why the security of users using a mobile devices to connect to the Internet is still the main user protection management concern. Kingpin and Mudge (Kingping and Mudge, 2001) were among the first to discuss the lack of security in the Operating Systems (OS) of the early handheld mobile devices. A number of other authors have since investigated a variety of vulnerable mobile devices, but their research was focused on the malware imported through downloaded applications (Mylonas et al., 2013a; Grace et al., 2012; Zhou et al., 2012). They did not focus on the privacy provision in the context of the Internet content blocking and data protection. For that reason, we first examined the properties of the most frequently used smart phones in our target countries in order to find out, if this technology is available and can be used by the interested users.

Examination of the public source documentation on the popularity of different mobile handsets in the target countries (Statcount, 2012) yield the following selection of handsets: Nokia (32%), Samsung (20%), and Apple (19%). These three manufacturers cover about 72% of the mobile-handset market but it is important to note that the mobile handset markets change rapidly, as demonstrated by the data collected from the user-communities survey. The technical properties of OS Apple iPhone 4 (released in October 2011), Nokia N8, HTC Sensation (released in May 2011), and Blackberry Curve 9360 (released in August 2011) were examined in accordance with following criteria: the ease of use, resilience, and circumvention capabilities. In addition, we studied certain properties of these devices; e.g. the availability of applications for a particular OS in the case of a non-native OS security application; OS interoperability, such as hardware limitations to the non-native OS applications; the possibilities to configure Internet routing (no special device security settings are required); user anonymity (anonymisation of personal identifiers, and the application of the circumvention tools supported by the OS); availability of a cryptographic tool for user data protection; resilience capacity to traffic blocking by the network operator; possibilities for carrier changes; the ease of installation; availability of a friendly graphical user interface, and the choice of natural languages supported. A brief overview of the identified technical capabilities for the privacy abuse prevention is presented in Table 1. Table 1 clearly shows that most of the studied security capabilities for data protection and privacy provision can be implemented and used in combination with the most popular mobile device OS platforms, either by implementing additions to the native OS, or through specific applications that extend the OS platform security. Table 1 also shows that the most popular handsets were equipped with security technology, and the additions to the basic OS functionality (to upgrade general security) could be uploaded and used.

4. Research model design

The conceptual model was designed to investigate the correlations between the level of information society development, and users' trust in the on-line mobile services. The model was derived from the relevant parameters and data collected during the survey. The role of the stakeholders in the telecommunications market was deemed critical for user privacy protection, because monitoring and content blocking is implemented through the networks the stakeholders manage. Additional parameters were used to measure the level of information society development based on the telecommunications market profiles of the studied countries. Other relevant information shed light on the affordability and accessibility of technology, as well as the wealth of a country measured by GNI. Information we could not obtain from public sources was collected directly from the users in the selected countries.

Table 1
Evaluated tools present or uploaded on the smart phones and the results regarding their properties for provision of security, resilience and usability.

Function	Tool	Android			IOS			Symbian			Blackberry		
		S	R	U	S	R	U	S	R	U	S	R	U
Voice – encryption facility	Skype	3	3	4	3	3	4	3	3	4	3	3	4
	Viber	2	3	4	2	3	4	–	–	–			
	Acrobits	3	2	4	3	3	4	–	–	–			
	Internal SIP							3	2	2	3	2	2
Text – encryption facility	Skype	3	4	4	3	3	4	3	3	4	3	3	4
	Viber	2	3	4	2	3	4	–	–	–	2	3	4
	Whatsapp	1	1	4	1	1	4	1	1	4	2	3	4
	TextSecure	4	3	3	4	3	3	–	–	–	–	–	–
Circumvention	OpenVPN client Feat VPN	3	3	3	3	3	3	–	–	–	–	–	–
	PPTP native	2	2	3	2	2	3	–	–	–	–	–	–
	L2TP/IPSEC native	3	2	3	3	3	3	3	2	1	–	–	–
	Orbot	4	4	4	4	4	4	–	–	–	–	–	–
	ExpressVPN	2	2	4	2	2	4	–	–	–	–	–	–
	Puffin Browser	3	2	4	3	2	4	–	–	–	–	–	–
	Opera mini	3	2	4	3	2	4	3	2	4	3	2	4

Scoring: 1 = low, 5 = high. S = Security; R = Resilience; U = Usability.

4.1. Stakeholders and players on the telecommunications market

Most countries have a government department for information and communications technologies (ICT) responsible for setting and implementing the government telecommunications market policy, facilitating the delivery of broadband Internet and administering the electromagnetic spectrum for communication and broadcasting. A robust, modern and efficient telecoms infrastructure is considered to be vital for the national economy. As a consequence, most of the governments tend to view the ICT sector as a source of sustained national economic growth and competitiveness. This is achieved by the promotion of investments into the modern infrastructure, as well as the provision of a supportive legislative and regulatory environment. The telecommunications market is usually regulated by a body known as the Telecommunications Regulator, which is supposed to be an independent body and not directly controlled by the state. However, this is very often not the case. This body is normally responsible for the regulation of the TV and radio, as well as the telecommunications sectors, including the fixed line and mobile network infrastructure, as well as the radio spectrum used by the wireless networks. Network services are offered by the telecommunications operators, who play in the state regulated market environments. Telecommunications operators are often requested by the state entities to implement the Internet traffic blocking and monitoring. However, if such implementation is not supported by an official legal request, it significantly interferes with fundamental human rights (UN, 2011). In recent years, some well-known democratic states have also promoted the use of Internet blocking technologies in relation to a variety of narrowly specified types of content. The subject matters vary from the availability of Nazi memorabilia via online marketplaces to the gambling websites hosted in the countries with liberal gambling regulations (Maitland et al., 2012). States with significantly less open information regimes and little regard for human rights have adopted wide scale Internet blocking as a technical resource for extending their practice of information control into the online world.

When selecting the countries for this study, we looked for developing and emerging economies with more or less severe Internet content censorship. Developing economies have low GNI and poor telecommunications infrastructure. Emerging economies exhibit robust and continual economic expansion coupled with the fast growth of new products and services to satisfy their consumer demands. However, it should be noted here that the mobile communications services and customers belong to an area with the fast changing statistics. For example, in China, over 30 million additional subscribers were added to the mobile networks in the first quarter of 2012 alone (Callanan and Dries-Ziekenheiner, 2012). Therefore, we carefully considered the situation in all selected countries, and categorized them as developing or emerging economies. Categorization was done on the basis of GNI, and the level of development of the telecommunications market that reflects the growth of new customers, new services, availability of the ICT, and the overwhelming success of the mobile communications.

In that context, the information about the main market players, especially regarding their ownership, was considered to be relevant for the conceptual model design. The mobile markets in these countries are dominated by five mobile operators with the highest number of consumers. They generate revenues of over USD 300 billion, have 1.7 billion subscribers, 500 million of subscribers are actively using the mobile data services. In total over 44 mobile operators are present, 9 of them are 100% state- owned operators (the overall subscriber base for these operators is over 1.1 billion), and 35 have a mixed ownership structure. The survey data confirmed that the main focus of the mobile Internet users in these countries is on news and other content mainly described as entertainment relying on video content from sources such as YouTube and its national variants.

4.2. Questionnaire design and data collection

A comparative evaluation of the current human rights protection policies in the context defined by the UN Internet Report (UN, 2011), countries telecommunications market regulations, as well the customer and workforce characteristics lead to the final selection of ten countries: Azerbaijan, Belarus, China, Iran, Oman, Saudi Arabia, Syria, Tunisia, Uzbekistan, and Vietnam. Egypt and Libya were also targeted but due to the serious political upheavals in 2012, the data collected was not sufficient for data processing. In Syria, the data was collected just before the outburst of political upheavals.

The selected countries were classified as developing or emerging economies on the basis of the GNI data obtained from the World Bank Statistics (2012). The lowest GNI was found in Vietnam (USD 3 620) and Uzbekistan (USD 3 670); the highest GNI was found in Oman (USD 25 320) and Saudi Arabia (USD 30,160). The GNI of other targeted countries fits between these two extremes, e.g., USD 14 950 in Belarus and USD 9 040 in China. Affordability of the mobile services (pre-paid and post-paid broadband mobile network service measured as a percentage of GNI) ranged from 1.6 for Oman to 8.3 for Syria, and 10.2 for Vietnam (ITU, 2013).

The Kingdom of Saudi Arabia with the GNI of USD 30 160, the Sultanate of Oman with the GNI of USD 25 320, Belarus with the GNI of USD 14 950, Iran with the GNI of USD 12 895, Libya with the GNI of USD 11 936, Azerbaijan with the GNI of USD 10 365, Tunisia with the GNI of USD 9 650, and China with the GNI of USD 9 040 were categorized as the countries with high or moderate GNI and developed mobile markets. The level of mobile market development was determined on the basis of the mobile services penetration index, and affordability of the mobile broadband prices. The penetration index in these countries ranges from 99% in Azerbaijan to 198% in Saudi Arabia. Affordability of the mobile services (pre-paid and postpaid broadband mobile services) ranges from 1.6 in Oman to 3.6 in China. Egypt with USD 6 047, Syria with the estimated USD 5 100 (2011), Uzbekistan with USD 3 670, and Vietnam with USD 3 620 formed the second group of countries. In this group, the mobile

service penetration index ranged from 58% in Syria to 83% in Uzbekistan. Affordability of the mobile services ranged from 8.3 in Syria to 10.2 in Vietnam.

Questions were formulated with the intention of collecting the answers and data that will help us build a conceptual model (Callanan et al., 2013). In addition, Freedom House worked with the local partners to identify key lead researchers in the targeted countries, who could perform the collection of data. The questionnaire consisted of 23 questions (see Annex 1). The first five questions were designed to collect information about the basic characteristics of a mobile phone user, such as the type of service used, the type of technology used for Internet access, the type of customer relationship (pre-paid or post-paid service), the entity paying for the service (to understand user independence and control). The next two questions were about the types of mobile phones. These two questions were included, because the technical study showed that there are differences between the most frequently used mobile phones OS in their capacity to protect user privacy. Other questions dealt with user skillfulness, capabilities, and frequency of the mobile phone upgrade application downloads. This information is an indication of the user capability to download applications for the protection of privacy and security. This group of questions also addressed the issue of jailbroken phones (phones modified to enable users to install applications from non-regulated marketplaces). The last group of questions directly addressed the issues dealing with the type of information relevant for user privacy, as well as the issues of monitoring and content blocking. The last question addressed the issue of trust. Twelve telecommunications market stakeholders were listed, and users had to choose a number between 1 and 12 on a Licker scale to describe how much they trust individual stakeholders. The questionnaire was translated into national language(s), the survey was promoted, and questionnaires distributed by an appointed in-country survey leader. Translation and localization of the instrument were carried out by the Freedom House language experts. In most of the countries, the survey was administered through online survey sites; however, in some countries the answers were collected on paper, and then submitted online. When respondents had no Internet access or their connection was not secure, the lead researchers personally administered the instrument, and entered responses into the survey tool.

Once the online responses were collected, they were translated back into English. In each surveyed country, the survey leader was asked to identify a sample of key stakeholders, and a higher portion of arbitrary users with selected demographics properties, such as sex, age and education level. The total user survey sample was $N = 1\,644$. Egypt data were not considered in the analysis due to the low number of received answers as turmoil were present in the country during the time of data collection.

We acknowledge that this survey was very limited. The data collected was not weighted to represent the general population, since the main objective of this study was to investigate correlations between content blocking and monitoring, and mobile phone users' trust and attitudes towards the state-sponsored blocking and monitoring activities. All anticipated physical, psychological, social or legal risks were minimized. All in-country survey leads were discrete when recruiting the study participants, and operationalising the survey instrument.

Respondents' identities were kept confidential. Survey participants were not misinformed about the true nature of the project; namely, all country survey leads received an introductory document outlining the research objectives, and the involvement of Freedom House. In most of the studied user communities, survey leads managed the demographics of the sample, trying to strike a good balance in terms of respondents' sex and age. To ensure reliability of the sample, the experts tested sample data against the Cronbach alpha. The test results returned positive. Respondents were aged 15–48; 21% were female, 34% were young users (min = 15 and max = 22 years). The same applies to the level of education of the surveyed users (Callanan and Dries-Ziekenheiner, 2012).

It is necessary to underline that it is very complicated to collect data through direct interviews with respondents in the targeted countries. Sometimes our local survey leads needed protection. In such cases, we prioritized data obtained from other sources; i.e., we did not insist on obtaining complete and more detailed feedback about day-to-day user experiences. This is one of the circumstantial limitations we had to accept, because it is out of researchers' control; e.g., in Vietnam it is illegal to conduct surveys without a state license.

81% of the surveyed mobile users had mobile phone access to the Internet. Almost 33% of users accessed the Internet with a mobile handset using a Wi-Fi connection, while others use mobile network Internet access. Some 32% of users had limited Internet access; e.g., pay-as-you-go service (17%), which was the most popular service of this kind. In addition, the collected data showed the following:

- Over 57% of users answered that they, Rarely " or, Never" share content using Bluetooth. Over 38% indicated that they share content, Often" or, Sometimes" - in this way they confirmed that they know how to share content. Sharing content using the personal area networks (short distance) is more secure and difficult to detect and intercept by investigators, unless the Bluetooth network ID (unique to each handset) is pre-stored by the handset retailer.
- Over 70% of users paid for their own phone services, while in 22% of the cases the bill was paid by the user's family. This explains who could easily access the billing information and usage data.
- Over 68% of all respondents indicated that they have their own smartphone, leaving a significant minority of 23% who did not have a smartphone, and a small group of 7% who did not know what a smartphone was.

The charts of the descriptive statistics are presented in Fig. 2.

In general, we can conclude that there is a growing supply of handsets and an increased number of new mobile packages offered on the target markets. This was considered an indicator of the greater availability of the mobile technology. These

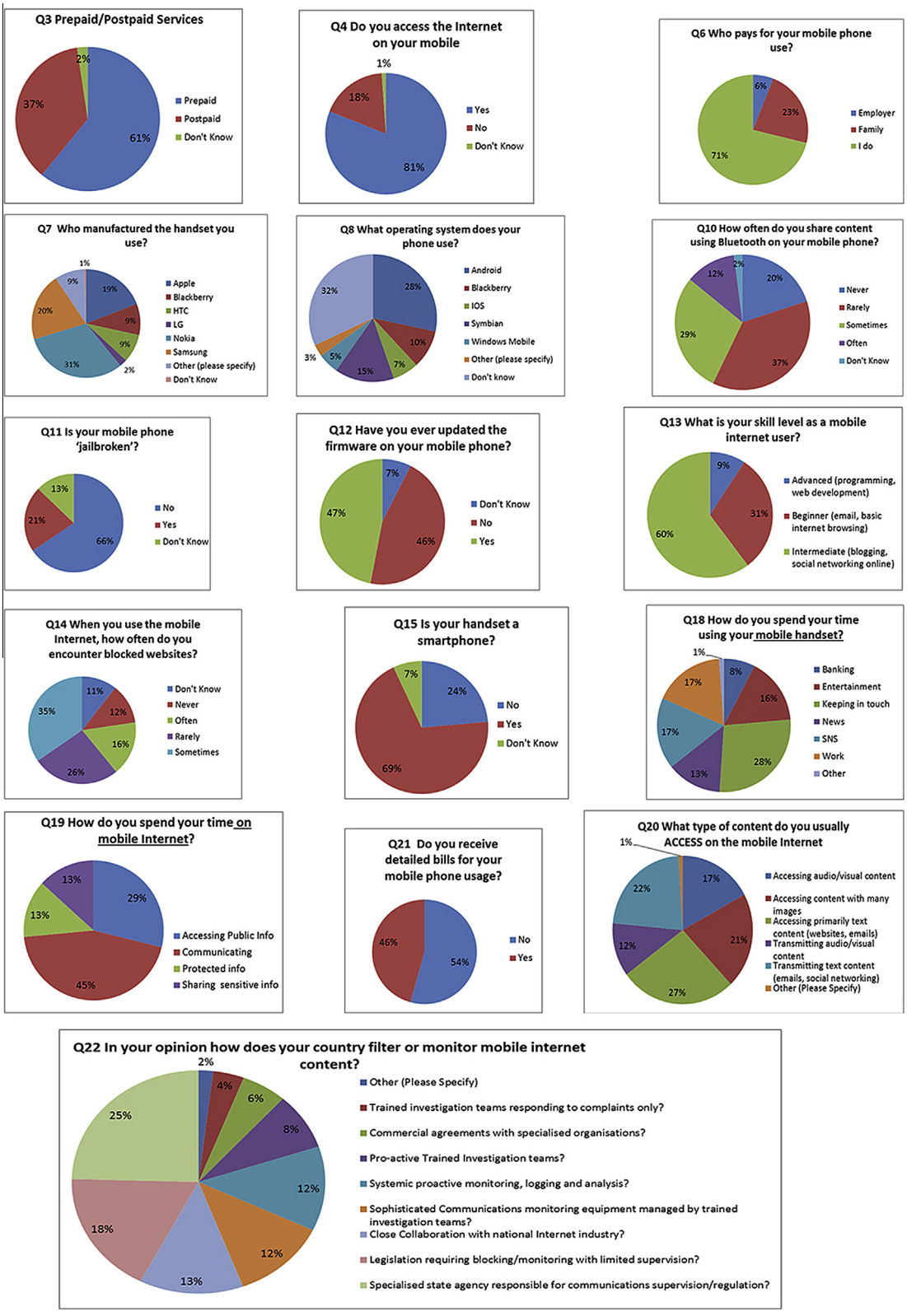

Fig. 2. Descriptive statistics.

findings suggest vibrant, competitive, and profitable markets with a strong demand for future mobile services. A wide variety of handsets presents significant technical challenges for the state security agencies and operators, who prefer to target their monitoring activities specifically designed for a complex range of market-available handsets enabling Internet access.

5. Data analysis

The research questions identified in the introductory part of the paper where reformulated into hypotheses, which were to be confirmed or rejected by the data analysis.

An important aim of the study was to determine if there are any differences between targeted communities in terms of their attitude towards the state Internet-content restrictions, communication blocking, and monitoring. It should be noted that much of the content blocked in the studied countries, such as child pornography, gambling and hate speech, is considered illegal also in other countries across the world, where the respect for human rights is not in question, such as France and Italy. Freedom House (Freedom House on the Net, 2013) published a report on Internet freedom, which covers developments in 60 countries around the globe. On the "Limits on Content" scoreboard, Iceland ranked first with the lowest score (1/35), which indicates maximum freedom. Iran ranked last with the highest score (32/35). Most of the countries with 20 or more points are from the Asian-Pacific and African regions. However, blocking access to information such as religious content, foreign news, or selected national news sources, as well the politically sensitive content is a problem that directly challenges our freedom of speech. In addition, the interpretation of what constitutes hate speech or terrorist content differs from one country to another. The following hypotheses were formulated based on the research questions presented in the introduction:

H1. Greater user awareness of the Internet content restrictions is associated with higher level of information society development.

H2. The level of user skilfulness positively correlates with the user capability to recognize traffic monitoring and content blocking.

H3. A higher level of information society development contributes to the greater user awareness that content blocking and monitoring is initiated by state owned agencies.

H4. Users with advanced skills and those who often download content via mobile Internet trust the state-owned telecommunications market players less than other market players.

H5. Skilled users with jailbroken phones know better how to improve their privacy protection.

H6. User tolerance of content blocking and the user trust to state- owned agencies as entities that care about their privacy is correlated with the high level of information society development, the availability of technology, and the wealth of a country.

The conceptual model that was designed after the survey data evaluation was used to confirm or reject the six hypotheses. The methodology used to design the model is described in the next section.

5.1. Methodology

Three regression models were built with the variables obtained from both sources of information: the feedback from the survey respondents and the country statistics obtained from public sources. A factor analysis was performed using target country data in order to obtain a limited number of factors from several state variables, such as GNI, mobile market penetration, affordability and availability of technology measured on the basis of the pre-paid and post-paid mobile broadband package prices (expressed as a percentage of GNI), and the mobile Internet usage.

It was found that high, positive and significant correlations exist between the GNI and mobile market penetration ($r = 0.79$; $p = 0.007$). The factor analysis using the Principal Axes Factoring method (PAF) gave a single-factor solution as the GNI variability and mobile market penetration were explained with one factor of 86%. A moderately high and positive correlation was also found between the price of pre-paid and post-paid mobile services as a percentage of GNI ($r = 0.64$; $p = 0.04$) and the mobile Internet use. The PAF factor analysis resulted in a single factor explaining 82% of the variability of the mobile broadband price variables (pre-paid and post-paid) measured as a percentage of GNI. The factor scores were saved as new variables, one describing the level of the information society development, and the other describing the affordability and accessibility of technology. User skilfulness was used as the third independent variable. These new variables were used as the country-level variables for the subsequent analyses. To test the hypotheses deriving from them, we used a multilevel, multivariate, logistic regression. This analysis was performed simultaneously on two levels: first, all respondents were included in the sample, and second, all countries were included in the sample. Since the second level sample size

was rather low, only (computationally less demanding) random intercept model was investigated. At the same time, several predictors were included in the regression models in order to obtain more valid results regarding the explanatory power of the included predictor. The hypotheses were tested with $\alpha = 0.05$ and $p < 0.05$, which were treated as statistically significant.

Four regression models were built to answer the research questions and to check the validity of our hypotheses. The first regression model included market-development variables used for measuring the level of information society development (mobile market penetration data, GNI), while the second regression model used affordability of the broadband technology (expressed as a factor score obtained as a result of the factor analysis of the pre-paid and post-paid mobile service prices measured as a percentage of GNI). The independent user-level variables are: the level of user skills (based on self assessment – beginner, intermediate, or advanced), the frequency of application downloads (at most sometimes or often), smartphone Internet access (yes or no), the pre-paid and post-paid mobile services and the mobile manufacturers (e.g., Nokia, Apple, Samsung, Blackberry, or other). The dependent variables are: the frequency of encountering blocked web sites (rarely, sometimes, or never), phone firmware updates (yes or no), users' opinion about who is responsible for monitoring and Internet content blocking (state or non-state), who is perceived as a trustworthy provider of mobile privacy protection (answers were grouped into three categories: state and state-owned agencies, non- state agencies, and private sources), and the use of a jailbroken phone, which enables the installation of applications from other manufacturers.

The results of the logistic regression are the odds ratios (OR) that show the correlation between each predictor and a dependent variable. The odds of occurrence of a given (non-referent) event vs. an alternative event (the reference category can be found between parentheses in the tables) are calculated for each outcome of a dependent variable, and compared to each other. When the odds ratio equals one, the non-referent event has the same odds to take place for each outcome (non-referent and referent outcome) of a dependent variable. When the odds ratio is bigger than one, the non-referent event of a predictor variable is more "likely" to happen for the non-referent category of a dependent variable. When the odds ratio is lower than one, the non-referent event of a predictor variable is less "likely" to happen for the non-referent category of a dependent variable. Interpretation of the correlation between a numeric predictor (e.g., the level of information society development) and a dependent variable is such that for each predictor variable unit increase the odds of a non-referent event of a dependent variable increase ($OR > 1$) or decrease ($OR < 1$) by a given number. In the multivariate logistic regression, a given predictor variable is true when the values of all other variables included in the model remain constant.

The statistical significance of the odds ratio is expressed with p-values. Correlations with p-values lower than or equal to 0.05 are treated as statistically significant and are presented as bold numbers in the Tables 3–6.

The sample characteristics are presented in Table 2.

5.2. Results and findings

Descriptive statistics produced from the collected survey data are presented in the charts in Fig. 2. The phones most frequently used by the respondents were: Nokia (32.8%), followed by Samsung (20.8%), and Apple (18.8%). The mobile Internet is used by the majority of respondents (81.9%), and the prepaid mobile services are used by 63% of all respondents. The highest percentage (58.1%) of respondents describes themselves as intermediate mobile Internet users. 63% of respondents often downloads some of the content via mobile Internet. 25% of respondents stated that they had a jailbroken phone, and 50% had a phone with updated firmware. The content blocking is noticed by 58% of all mobile Internet users, who encounter blocked websites at least sometimes. The majority (68%) believes that blocking is done by the state agents. 21% of respondents trust the state to protect their privacy when accessing Internet through their mobile phones. A bit higher share of respondents (34%) trusts no one, 19% trust the non-state agents, and 26% trust the private contacts.

Table 2
Sample characteristics.

Accessibility of technology		Skilfulness		Protection		Monitor & trust	
	f (%)		f (%)		f (%)		f (%)
Used handset		*Apps download*		*Jailbroken phone*		*Trusted agents*	
Apple	297 (18.8)	At most sometimes	577 (36.6)	Yes	327 (25)	No one	520 (34)
Blackberry	149 (9.4)	Often	999 (63.4)	No	979 (75)	State	320 (20.9)
HTC	134 (8.5)	*Skill level*		*Updated phone*		Non-state	292 (19.1)
LG	30 (1.9)	Beginner	474 (30.9)	Yes	720 (49.9)	Private	399 (26.1)
Nokia	519 (32.8)	Intermediate	917 (59.8)	No	723 (50.1)	*Monitor*	
Samsung	322 (20.3)	Advanced	143 (9.3)			State	748 (70.2)
Other	133 (8.4)					Non-state	318 (29.8)
Mobile internet						*Blocked websites*	
Yes	1274 (81.9)					Never	565 (41.5)
No	281 (18.1)					Sometimes	509 (37.3)
Mobile service						Often	289 (21.2)
Post-paid	573 (37)						
Pre-paid	975 (63)						

f – frequency.

Table 3
Factors associated with frequency of encountering blocked websites (results of multilevel multinomial logistic regression; reference category = often).

Predictors (reference category)	Never	Sometimes		
	OR (95 % CI)	*P*	OR (95 % CI)	*p*
Post-paid (pre-paid)	1.06 (0.73; 1.52)	0.77	1.05 (0.74; 1.49)	0.77
Mobile internet yes (no)	1.34 (0.75; 2.39)	0.32	1.36 (0.77; 2.43)	0.29
Apple (other)	0.53 (0.24; 1.2)	0.13	0.66 (0.3; 1.47)	0.31
Blackberry (other)	0.37 (0.15; 0.92)	**0.03**	0.34 (0.14; 0.85)	**0.02**
HTC (other)	0.29 (0.12; 0.7)	**0.01**	0.44 (0.19; 1.03)	0.06
LG (other)	1.44 (0.25; 8.28)	0.68	1.07 (0.18; 6.53)	0.94
Nokia (other)	0.68 (0.32; 1.45)	0.32	0.66 (0.31; 1.4)	0.28
Samsung (other)	0.48 (0.22; 1.05)	0.07	0.46 (0.21; 1.02)	0.06
Download at most sometimes (often)	2.31 (1.54; 3.46)	**<0.001**	1.76 (1.19; 2.61)	**0.01**
Skill level beginner (advanced)	2.6 (1.37; 4.92)	**<0.001**	1.92 (1.04; 3.55)	**0.04**
Skill level intermediate (advanced)	1.62 (0.94; 2.79)	0.08	1.63 (0.97; 2.76)	0.07
Religion: Islam	0.44 (0.09; 2.18)	0.32	0.38 (0.09; 1.54)	0.17
Broadband affordability	2.17 (0.69; 6.78)	0.18	0.7 (0.25; 1.95)	0.49
Market development	1.54 (0.51; 4.64)	0.45	2.92 (1.08; 7.93)	**0.04**

OR = odds ratio; *p* = *p*-value; CI = confidence interval.

The first regression model was used to test the H1 and H2 claims, which identify the factors associated with the user awareness of monitoring and blocking. The awareness of monitoring and blocking was measured by two different variables; the first was the frequency of occurrence of the blocked content events when using mobile Internet, and the second was the user opinion about the entity that monitors and blocks the mobile Internet usage In this section, we shall analyse the first aspect, i.e. the frequency of occurrence of the blocked content events. Results of the multivariable regression analysis are presented in Table 3.

As is evident from Table 3, the mobile Internet skills correlate with the frequency of occurrence of the blocked websites. Compared to the advanced users, beginners have higher odds of never encountering a blocked website (OR[1]: 2.6 [1.4; 4.9], $p < 0.001$); they also have higher odds to encounter blocked websites sometimes, rather than to often (OR[1]: 1.9 [1.04; 3.5]; $p = 0.04$). The information society level of development measured as the mobile market development and wealth of the wealth (GNI) are also associated with the frequency of encountering blocked websites. Users from the more developed markets report more blocked website events ($p = 0.04$). Skilful users and users from developed and wealthy markets are more aware of blocking than the less skilful users and users from the less developed and less wealthy markets. This confirms the first and the second hypothesis (H1 and H2).

However, if we measure affordability of technology on the basis of market diversity, we notice that the users of some smartphone brands are more likely to come across a blocked site than others (e.g., the Blackberry users have higher odds of encountering blocked websites than users of smartphones from other (non-listed) phone manufacturers. It is not easy to explain such facts; because they could be related to the restrictions imposed by the manufacturer's network or they could be related to different device functionalities (some could have more functionalities than others).

The dependent variable for the second model was user awareness of the content blocking and traffic monitoring implemented by the state owned market players (state owned vs. non-state owned entities). The analysis has shown that of all predictors, only the level of information society measured as a market level of development correlates with the user awareness of the state imposed filtering of the Internet content. The more developed is the markets, the higher are the odds that users are aware of the state-imposed content filtering. The results further support the hypothesis derived from the research question considering the correlation between the market development and wealth of a country, as well as the concern for the state-imposed content blocking. Users from more developed and wealthier markets are more aware of the state-imposed monitoring compared to those from the less developed markets.

Data from Table 4 (OR = 2.14 (CI = (1.73; 2.64)) and $p = 0.001$) led to the conclusion that the more developed the market, the greater the chances of an increased awareness of the state-initiated filtering and monitoring. This confirms the third hypothesis (H3).

The next regression model was intended to provide information about the predictors associated with the users' trust in different telecommunications market players (state-owned teleoperators (ISPs), non-state owned, private, or none) to protect their privacy when using their mobile communication services. Several predictors were included in the regression model to obtain more realistic results about factors that could be associated with the mobile Internet users' trust.

The mobile phone users who download content via mobile Internet sometimes at most, trust the state-owned operators more than anyone else on list. Compared to the beginners and intermediate users, the advanced mobile Internet users trust more the non-state than the state-owned operators. Therefore, the trust issue correlates with the user skilfulness levels. This confirms the fourth hypothesis (H4). We could observe some differences between different smartphone brand users; e.g., the Blackberry, Samsung, and Nokia users trust the state-owned agencies more than other entities on the list. This regression

[1] The odds ratio when holding other predictors in the model constant.

Table 4
Factors associated with opinion on who is responsible for filtering the Internet content (results of the multilevel binary logistic regression; reference category = non-state).

Predictors (reference category)	OR (95 % CI)	*p*
Post-paid (pre-paid)	1.2 (0.86; 1.66)	0.285
Mobile internet yes (no)	0.7 (0.44; 1.14)	0.153
Apple (other)	0.91 (0.46; 1.8)	0.776
Blackberry (other)	0.96 (0.42; 2.19)	0.921
HTC (other)	0.63 (0.3; 1.3)	0.207
LG (other)	0.68 (0.21; 2.21)	0.525
Nokia (other)	1.11 (0.59; 2.08)	0.744
Samsung (other)	1.23 (0.64; 2.4)	0.535
Download at most sometimes (often)	1.22 (0.88; 1.7)	0.23
Skill level beginner (advanced)	0.76 (0.43; 1.37)	0.368
Skill level intermediate (advanced)	0.86 (0.5; 1.47)	0.572
Religion: Islam	0.97 (0.57; 1.64)	0.899
Broadband affordability	0.83 (0.56; 1.22)	0.34
Market development	2.13 (1.38; 3.27)	**0.001**

OR = odds ratio; *p* = *p*-value; CI = confidence interval.

Table 5
Factors associated with opinion to whom user trust (results of multilevel multinomial logistic regression; reference category = state).

Predictors (reference category)	No one OR (95 % CI)	*P*	Non-state OR (95 % CI)	*P*	Private OR (95 % CI)	*p*
Post-paid (pre-paid)	1.23 (0.85; 1.76)	0.27	1.12 (0.75; 1.67)	0.58	1.41 (0.96; 2.07)	0.08
Mobile internet yes (no)	0.66 (0.41; 1.06)	0.09	1.04 (0.59; 1.83)	0.89	0.91 (0.53; 1.56)	0.73
Apple (other)	0.57 (0.25; 1.32)	0.19	0.62 (0.25; 1.57)	0.32	0.43 (0.18; 1.01)	0.052
Blackberry (other)	0.37 (0.15; 0.92)	**0.03**	0.45 (0.16; 1.27)	0.13	0.31 (0.12; 0.8)	**0.02**
HTC (other)	0.97 (0.37; 2.59)	0.96	1.35 (0.48; 3.8)	0.57	0.85 (0.31; 2.36)	0.76
LG (other)	0.41 (0.08; 2.08)	0.28	1.15 (0.23; 5.71)	0.87	0.93 (0.2; 4.24)	0.92
Nokia (other)	0.53 (0.24; 1.17)	0.12	0.39 (0.16; 0.94)	**0.04**	0.36 (0.16; 0.79)	**0.01**
Samsung (other)	0.42 (0.19; 0.93)	**0.03**	0.53 (0.22; 1.28)	0.16	0.37 (0.17; 0.84)	**0.02**
Download at most sometimes (often)	1.58 (1.1; 2.27)	**0.01**	1.1 (0.73; 1.64)	0.65	0.97 (0.65; 1.45)	0.89
Skill level beginner (advanced)	0.54 (0.26; 1.11)	0.09	0.79 (0.35; 1.78)	0.57	0.46 (0.21; 0.98)	**0.04**
Skill level intermediate (advanced)	0.52 (0.28; 1)	**0.05**	0.66 (0.31; 1.38)	0.27	0.45 (0.22; 0.89)	**0.02**
Religion: Islam	3.05 (0.44; 20.86)	0.26	1.66 (0.4; 6.87)	0.49	2.33 (0.26; 20.61)	0.45
Broadband affordability	1.03 (0.26; 4.08)	0.97	0.95 (0.34; 2.64)	0.92	0.64 (0.13; 3.04)	0.57
Market development	1.19 (0.32; 4.46)	0.80	0.49 (0.18; 1.34)	0.17	0.97 (0.21; 4.39)	0.97

model included a variable of the state-supported religion. The correlation between the state religion (measured by the share of Muslim population) and user trust did not yield statistically significant results. However, we should mentioned that the odds ratios for the Muslim religion, although not significant, are above value one in all three non-referent dependent variable categories. A higher share of Muslim population seems to lower the odds for the state (referent category) which contributes to the higher trust of the protective role of the state entities. If we were to include more predominantly Muslim countries, the explanatory power of the results regarding the role of the religion could yield results in favour of this presumption. This analysis confirms the fourth hypothesis (H4).

The next regression model was designed to investigate the correlation between user skilfulness and their capability to protect their privacy by uploading necessary additions to the OS. Users with the jailbroken phones and users who frequently download firmware upgrade applications were expected to have the necessary skills for the installation of security applications, and were expected to care more for protection of their privacy. Table 6 clearly shows that the skilfulness of the smartphone users positively correlates to their ability to protect themselves against monitoring and blocking. The less skilful users are less likely to have a jailbroken phone and are less likely to update their phone firmware as they less frequently download applications. Therefore, there is a correlation between users' skilfulness and their ability to download additional tools to improve their security. This confirms the fifth hypothesis (H5).

We decided to further explore the user tolerance of the state-implemented Internet content blocking and monitoring. The insight in the data has shown that the tolerance and acceptance levels of the state censorship differ from one country to another. For this reason, we performed a more detailed analysis of the collected answers to question No. 23 for each country. Question No. 23 listed twelve entities and respondents were asked to rank them on a trustworthiness scale from 1 to 12. The top of the scale position (position No. 1) was reserved for the most trustworthy entity, while the least trustworthy was to be ranked twelfth. Based on user answers, we were able to identify two groups of countries. The rankings of the listed entities in the question No. 12 are presented in Tables 7–9. The overall ranking (all countries together) is presented in Table 7; here the dominant role was played by users coming from seven countries forming the first group, who do not trust the state-owned

Table 6
Factors associated with having "jailbroken" phone and with updating phone firmware (results of multilevel binomial logistic regression; reference category = yes).

	Not "jailbroken" phone		Not updated phone firmware	
Predictors (reference category)	OR (95 % CI)	*p*	OR (95 % CI)	*p*
Download at least sometimes (often)	2.55 (1.88; 3.47)	**<0.001**	2.83 (2.37; 3.37)	**<0.001**
Skill level beginner (advanced)	2.41 (1.65; 3.54)	**<0.001**	3.54 (1.96; 6.39)	**<0.001**
Skill level intermediate (advanced)	1.84 (1.41; 2.4)	**<0.001**	1.71 (1.001; 2.93)	**0.049**

OR = odds ratio; *p* = *p*-value; CI = confidence interval.

Table 7
The ranking of the entities to whom user trust in the group consisting from three countries.

Trusted entity/User ranking in the country	China	Oman	Saudi Arabia
Government	**3**	2	3
State Agency	9	3	2
ISP inside country	7	1	**5**
ISP from outside	**2**	6	6
NGO inside	4	8	8
NGO outside	6	**10**	**11**
CSP inside	1	9	9
CPS outside	4	**11**	**10**
Personal contact inside	**10**	4	1
Personal contact outside	**11**	7	7
Software engineers	8	5	4
Other	12	12	12

Table 8
The ranking of the entities to whom user trust in the group of seven countries.

Trusted entity/User rRanking in the country	Azerbaijan	Iran	Syria	Uzbekistan	Belarus	Vietnam	Tunisia
Government	5	**12**	**11**	**10**	**12**	**12**	**11**
State Agency	**9**	**11**	**10**	**7**	**11**	2	
ISP inside country	**11**	**10**	**9**	**11**	7	3	1
ISP from outside	4	9	1	2	6	1	6
NGO inside	**10**	**8**	**8**	**9**	8	4	4
NGO outside	6	4	6	4	9	7	7
CSP inside	3	6	7	6	4	11	8
CPS outside	8	5	4	8	5	8	9
Personal contact inside	**2**	**1**	5	5	**1**	10	**2**
Personal contact outside	12	**2**	**3**	**3**	**2**	5	**5**
Software engineers	7	7	**2**	**1**	**3**	9	3
Other	1	3	12	4	10	6	12

Table 9
The ranking of the entities to whom user trust all countries.

Trusted entity/User ranking in the country	All
Government	**12**
State Agency	**10**
ISP inside country	9
ISP from outside	**1**
NGO inside	8
NGO outside	6
CSP inside	7
CPS outside	**5**
Personal contact inside	**3**
Personal contact outside	**4**
Software engineers	**2**
Other	11

entities at all. Their ranking is presented on Table 8. The second group consisting from three countries is presented on Table 9. It was surprising for the later to find out that although users in China, Oman, and Saudi Arabia were well aware (close to 60%) of the specialised state agencies, and Internet blocking and monitoring imposed by the national legislation

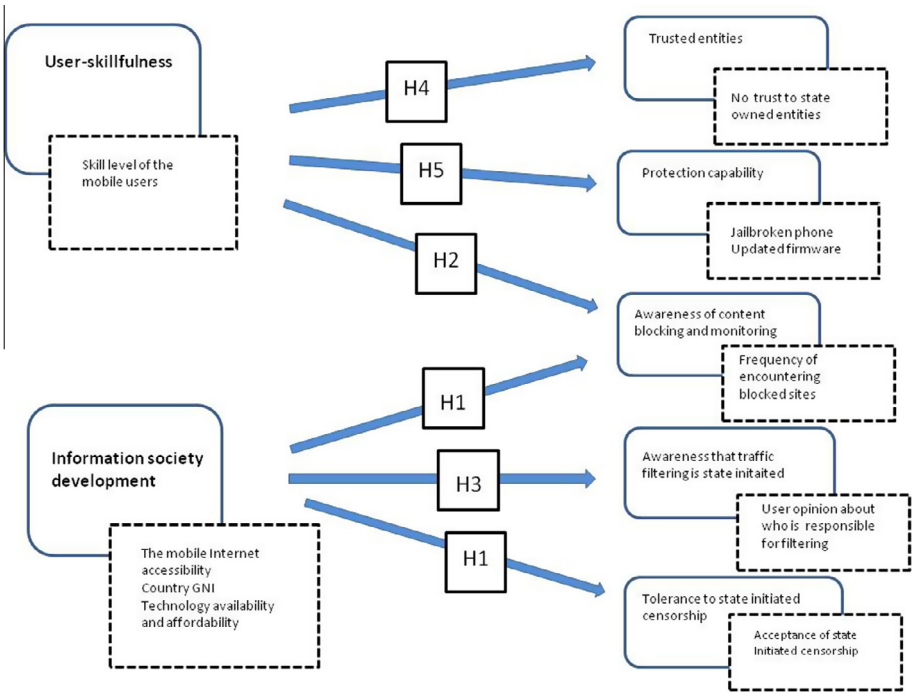

Fig. 3. The conceptual model.

and the state entities, their user communities trust their governments and believe the state-owned agencies protect their privacy and protect them from harmful content. This ranking is presented in bold. Oman and Saudi Arabia have a very high level of information society development, mobile technology is highly available and both of them are very wealthy countries. China has a much lower GNI copared to these two countries, however, its market is highly developed, users are skilled and a lot of technology on the market is produced at home (China has its own mobile technology manufacturers and network providers). Situation in the remaining seven countries is different. GNI in some countries (e.g., Belarus) is twice the GNI of the poorest states (e.g., Vietnam). These seven user communities recognised their governments and state-owned agencies to be the least trustworthy privacy protection entities, and placed them in the 11th or 12th position which is presented with bold numbers. These findings confirm the sixth hypothesis (H6).

Findings from the regression analysis presented above were used to design the conceptual model presented in Fig. 3.

6. Discussion

6.1. General findings

The general findings underline the fact that users of the ten studied countries are aware that a wide variety of Internet content is blocked. Some types of blocked content, such as child pornography and hate speech, are considered illegal in many other countries around the world. However, blocking religious content, foreign news, or national news sources, as well politically-sensitive content is problematic. In addition, the interpretation of what is considered hate speech or terrorist content is much broader or differently classified in different countries. The experts participating in the survey reported that the type of content filtered is not the same in all countries. Phishing and gambling are less prohibited (filtered only in three countries according to the Freedom House Report, 2013) than the leading political, religious and adult-only content, which is filtered in all of the concerned countries. Foreign news content is filtered in seven of the studied countries. State involvement is **usually justified with the need to support and encourage extensive investments** that contribute to the growth and development of the sector. The second, equally important excuse for the exhaustive censorship is to ensure suitable levels of state control over the mobile operators and the community.

For the majority of targeted user communities from the countries with low freedom score according to the Freedom House scale but with high level of information society development, the state control seems acceptable. Some of the theories about the trust relations in the electronic world point to the evident mitigation of the expected risks by the users. Ibbott and O'Keefe (2004), who based their theory on the Gallivan and Depledge (2003) work claim that trust in the context of electronic relationships mitigates relational risks, i.e., the trust between communicating parties reduces the perceived risk of undesired outcomes, and the relaying party between the communicating entities become a part of the mitigated risk.

They also note that when trust is defined in terms of the relational risk, it can be seen as an alternative to the control mechanisms, i.e., partners trust the actions of each other as an alternative to specifying detailed protocols for each other's behavior. The studies carried in communities from the developed part of world, e.g., in California and Greece (Ackerman et al., 1999; Buchanan et al., 2007; Mylonas et al., 2011), with high country scores for freedom show that user feelings about privacy are very complicated, and sometimes contradictory. When asked directly about their privacy preferences, users present themselves as very protective regarding their personal data, which is often in contradiction to the everyday actions they practice on the telecommunications networks. This does not correspond to the user professional preferences found in the studies of social networks (Ažderska and Jerman-Blažic, 2012a,b). Explanations presented in these studies most probably point out to the users' negligence and their lack of knowledge or understanding of the privacy threats, as well as the above mentioned trust between the communication parties, including the relaying party. Another explanation of the user actions that violate their preferences lays in the evidenced user trust in our study. Users trust the regulatory agencies and state-owned teleoperators. By inspecting the survey results of the two different groups of countries, we found out that the more developed markets offer more affordable technology, the countries are wealthier and the trust in the state-related entities on the mobile networking market is higher. However, it should be noted here that the recently revealed activities of the PRISM project had a great influence on the users from the developed regions, and has shaken their trust in the on-line services. The Global Report on Privacy (Global report 2013) revealed that almost 80% of respondents were concerned about their privacy online. The ESET Survey (Forbes, 2013) revealed that 83% of those polled changed their social media account privacy settings over the last 6 months. Furthermore, the Trust Privacy Index for 2013 (Bachman, 2013) also pointed out that 74% of Internet users were voicing concerns about their privacy, and 76% were saying that they were more likely to check the websites and applications for privacy certification or seals.

6.2. Differences between user communities in target countries

Based on the study results we can conclude that the user communities in the countries with vibrant, competitive, profitable, and very developed mobile markets with strong demand for services do not demonstrate or care much about strong governmental regulation. This is the case with the Chinese user community, as well as the user communities in Saudi Arabia and the Sultanate of Oman. These countries have high (Oman, Saudi Arabia) or moderate (China) GNI, and the majority of their users have high skill levels. The collected data confirmed that 89% of respondents from China, 90% of respondents from the Saudi Arabia, and 92% of respondents from the Sultanate of Oman believe they are highly skilled users. They are also very active in downloading content and firmware updates (between 61% and 71%). China has one of the leading emerging markets for the mobile technology, with the largest number of subscribers and national valued manufacturers. In China, the pre-paid offers for mobile services (measured as a percentage of GNI) are very affordable. The same applies to the Saudi Arabia and the Sultanate of Oman, where users trust their governments, state agencies and country's own ISPs. In China, the government and state agencies ranked high on the trustworthiness scale, at least when excluding the ''Don't know'' responses; when the ''Don't know'' responses were included, the ranking somehow changed and commercial organizations inside and outside China were somehow preferred to the governmental ones. The situation with the user level of trust is different in other studied countries. In Vietnam, Syria, and Uzbekistan the users only trust foreign ISPs. The government and governmental agencies are not trusted at all. It follows from that, countries, where the mobile technology market is developed and technology freely offered to the citizens, some restrictions and regulations by the government, if they are aligned with the development strategy of the country or the prevalent religion (e.g., Muslim religion in Oman and Saudi Arabia), are not perceived as a great evil by the users, and sometimes completely unnoticed. The Kingdom of Saudi Arabia, the Sultanate of Oman and the People's Republic of China are the examples of countries where users perceive content blocking as an attempt of the state to protect its people from adversary religious content or other content not aligned with their culture and the state regime. This is also what makes them different from the users in the developed part of the world. In contrast to that, users from the less developed countries with strongly controlled markets and more oppressive regimes are less likely to tolerate this kind of state involvement and lack trust in the state-owned entities. The government policy is not well perceived and distrust in the state-owned operators is high.

7. Concluding remarks

In conclusion, we can say that the level of the telecommunications markets development, and consequently also the level of the information society development is one of the most influential indicators regarding the user acceptance or rejection of the state initiated Internet content blocking and monitoring. However, the presented study has revealed that the current situation regarding the awareness of the privacy abuse and the use of appropriate security technology tools for better privacy protection should be studied and explained by considering many influential mobile market factors and players with different interests. Their presence and strategy is relevant when planning the future development of a safe and secure, trustable and ubiquitous communications environment, which is an important element of the economic development of a country. We can also claim that a single player acting in isolation on these market cannot change the current situation, since both platform-security development at the OS level, as well as the circumvention application development stakeholders have, so far, left some user communities outside of the mainstream development goals. The collected data have shown also that the mobile OS developed by the leading global manufacturers focus largely on the security features and platform security

models that rely on the amount of trust placed by the users to the network operators, which is the case in the most developed economies or wealthy countries with vibrant and developed markets. This is not a safe assumption for the user communities with low skill levels and restricted availability of technology, which is reflected also in the low level of economical and mobile market development. The mobile communications market in these countries is dominated by many US and European manufacturers that deliver enhanced mobile coverage and connectivity to the concerned citizens without much care for the users' needs for self-protection. It is also obvious that the complex environments in which the mobile operators operate create challenges for the government, industry and mobile users in order to strike the appropriate balance between the current trends in sharing significant amounts of data online and protecting that data from abuse with further investments in the mobile technology. It also became clear that in a tightly regulated market, such as the ubiquitous mobile market, with a limited number of operators and a highly regulated telecommunications infrastructure, privacy protection that requires user skillfulness is difficult to achieve. Smartphones and other modern mobile devices are complex computers with a vast range of sensors and functionalities. As a consequence users clearly need more knowledge and information to enhance their skills for an efficient use and self protection. In that context, an information campaign focusing on the risk assessment and risk mitigation is welcomed by any acting player in the field. Users' attention must be gained in order for them to understand their high-risk environments and activities to be performed, especially when the risks and the resulting consequences cannot be eliminated.

Appendix 1. The Questionnaire

1. What country do you live in?
2. Which mobile service do you use?
3. Do you use a pre-paid or post-paid mobile service?

[a] Pre-paid	[b] Post-paid	[c] Don't know

4. Do you have access to the Internet using mobile Internet services?

[a] Yes	[b] No	[c] Don't know

5. How do you access the Internet on your mobile phone?

a. Wi-Fi
b. A limited bundle with my subscription
c. An unlimited data bundle with my subscription
d. I pay per MB/Kb of data usage
e. I have no access
f. Other [please specify]
b. A limited bundle with my subscription

6. Who pays for your mobile phone use?

a. I do
b. Another member of my family
c. My employer

7. Who manufactured the handset you use?

[a] Nokia	[b] HTC	[c] Apple	[d] Samsung	[e] Blackberry
[f] Other [please specify]				

8. What operating system does your phone use?

[a] Android	[b] IOS	[c] Symbian	[d] Blackberry	[e] Windows Mobile
[f] Don't know	[g] Other [please specify]			

9. Where do you download apps for your mobile phone?

[Often, Not Very Often, Sometimes, Rarely, Never, Don't know How]
a. Apple App store
b. Android Market
c. Blackberry App World
d. Windows Mobile Marketplace
e. Nokia OVI [Symbian]
f. Other [please specify]

10. How often do you share content using Bluetooth on your mobile phone?

[a] Often	[b] Not Very Often	[c] Sometimes	[d] Rarely	[e] Never

11. Is your mobile phone jailbroken?

[a] Yes	[b] No	[c] Don't know

12. Have you ever updated the firmware on your mobile phone?

[a] Yes	[b] No	[c] Don't know

13. What is your skill level as a mobile Internet user?

a. Beginner [email, basic Internet browsing]
b. Intermediate [blogging, social networking online]
c. Advanced [programming, web development]

14. When you use the mobile Internet, how often do you encounter blocked websites?

[a] Often	[b] Sometimes	[c] Rarely	[d] Never	[e] Don't Know

15. Is your handset a smartphone?

[a] Yes	[b] No	[c] Don't know

16. What do you download to your mobile handset?

[Often, Sometimes, Rarely, Never, Don't know how]			
[a] Free Apps	[b] Paid Apps	[c] Free Content	[d] Paid Content

17. What type of apps/content do you download, and how often?

[Often, Sometimes, Rarely, Never, Don't know]				
[a] Music	[b] Videos	[c] Games	[d] News and Affairs	[e] Other [Please specify]

18. How do you spend your time using your mobile handset?

[Categorize in percentages]
a. Work use
b. Keeping in touch with family and friends
c. Entertainment [music, videos, games]
d. Banking
e. Other [please specify]

19. How do you spend your time using your mobile Internet?

[Categorize in percentages]
a. Accessing public information
f. Communicating with colleagues and friends
g. Accessing protected information
h. Sharing potentially sensitive information regarding my country

20. What type of content do you usually access on the Internet [Categorize your use in percentages]

a. Accessing primarily text content [websites, emails]
b. Accessing content with many images
c. Accessing audio/visual content
d. Transmitting text content [emails, social networking]
e. Transmitting audio/visual content
a. Accessing primarily text content [websites, emails]

21. Do you receive detailed bills for your mobile phone usage?

[a] Yes	[b] No

22. In your opinion, how does your country filter or monitor mobile Internet content?

a. Legislation requiring blocking/monitoring with limited supervision?
b. Specialized state agency responsible for communications supervision/regulation?
c. Trained investigation teams responding to complaints only?
d. Pro-active trained investigation teams?
e. Sophisticated communications monitoring equipment managed by trained investigation teams?
f. Close collaboration with the national Internet industry?
g. Commercial agreements with specialized organizations?
h. Systemic pro-active monitoring, logging and analysis?
i. Other [please specify]

23. Who do you trust to protect the privacy of your mobile Internet communications?

[Never, Most of the Time, Sometimes, Rarely, Never, Don't know]
a. Government
b. State agencies
c. Communications service providers located inside your country? [ISP, Mobile, Telecommunications company]
d. Communications services providers located outside your country? [ISP, Mobile, Telecommunications company]
e. Non-governmental organizations located inside your country?
f. Non-governmental organizations located outside your country?
g. Commercial organizations located inside your country?
h. Commercial organizations located outside your country?
i. Personal friends/contacts located in your country?
j. Personal friends/contacts located outside your country?
k. Software and application developers
l. Other

References

Adams, A., Sasse, M.A., 1999. Taming the wolf in sheep's clothing: privacy in multimedia communication. Proc. ACM Multimedia, 316–321.

Ackerman, M., Cranor, L., Reagle, J., 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. Proc. ACM Conf. Electron. Commerce, 89–97.

Ažderska, T., Jerman-Blažič, B., 2013. A holistic approach for designing human-centric trust systems. Syst. Prac. Action Res. 26 (5), 417–450.

Ažderska, T., Jerman-Blažič, B., (2012) Developing trust and reputation taxonomy for a dynamic network environment. V: The Seventh International Conference on Systems, February 29 – March 5, 2012,In: Saint Gilles, Reunion Island. KAINDL, Hermann (Eds.). ICONS 2012. [S. l.]: IARIA, 2012, pp. 109–114.

Ažderska, T., Jerman-Blažič, B., (2012), Trust as an organismic trait of e-commerce systems. V: IFIP, International Cross Domain Conference and Workshop on Availability, Reliability, and Security, 2012, Prague, Czech Republic. Quirchnmayer, G. (eds.). Multidisciplinary research and practice for informations systems: proceedings, (Lecture notes in computer science, Springer, 2012, vol. 7465, pp. 161–175.

Bachman, K., (2013) A Report on consumer privacy from the U.S Government Accountability Office, control over personal data By Katy Bachman. URL:http://www.adweek.com/news/technology/government-report-calls-comprehensive-privacy-law-153996 (accessed July 5th, 2014).

Baliga, A., Killian, J., and Iftode, L., 2007. A web based covert file system. Proceedings of the 11th USENIX workshop on Hot topics in operating systems HOTOS, 2007, pp. 14–21.

Bellens, R., Vlassenroot, S, Verstrataeten, D., Guatama, S., (2013) Collecting and Processing of Crowd Behaviour Data URK: https://biblio.ugent.be/publication/2049934/file/2049935.pdf (accessed January 31st, 2013).

Bellotti, V., Sellen, A., 1993. Design for privacy in ubiquitous computing environment. Proc. ECSCW 1993, 77–92.

Broadband Commission for Digital development and Cisco (2013), Planning for progress, July 2013, URL: http://www.broadbandcommission.org/ (accessed February 25th, 2014).

Buchanan, T., Paine, C., Joinson, A.N., Reips, U.D., 2007. Developing measures of on-line privacy concern and protection for use on the Internet. J. Am. Soc. Inform. Soc. Technol. 2007, 20–34.

Burnett, S., Feamster, N., and Vempala, S. (2005), Chipping away at censorship with user-generated content, in USENIX Security Network Traffic. IEEE International Conference on Communications, 5, Proceedings, pp. 2041–2045.

Bury, S., Ishmael, J., Race, J.P.N., Smith, P., 2010. Designing for social interaction with mundane technologies: issues of security and trust. J. Pers. Ubiquit. Comput. 14, 227–236.

Callanan, C., Jerman-Blažič, B., Dries-Ziekenheiner, H., (2013) Empirical assessment of data protection and circumvention tools availability in mobile networks. V: The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic, CyberSec, 2013, Kuala Lumpur. Proceedings, 2013, pp. 206–220.

Callanan, C. and Dries-Ziekenheiner, H., (2012) Safety on Line, December, 2012, URL:http://www.freedomhouse.org/sites/default/ (accessed January 31st, 2013).

Cisco 2014 Lawful Interception for 3GPP: Cisco Service Independent Intercept in the GGSN, accessed 4.7.2014, http://www.cisco.com/web/about/security/intelligence/LI-3GPP.html and The Annual Security Report – Insights across four key areas: Trust... goals will hinge on effective privacy policies and robust technology, URL:http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (accessed 7th July 2014).

Dhillon, G., Torkzadeh, G., 2006. Value-focused assessment of information system security in organizations. Inform. Syst. J. 16 (1), 293–314.

Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inform. Syst. 8 (7), 386–408.

Dingledine, R., Mathewson, N., and Syverson, P. Tor (2004): The second-generation onion router. 13th USENIX Security Symposium (2004), pp. 312–318.

Dusi, M. Gringoli, F., Salgarelli, L., (2008) A Preliminary Look at the Privacy of SSH Tunnels, Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on, pp. 3–7, 2008.

Enck, W., Ongtang, M., McDaniel, P., (2009), On lightweight mobile phone application cerification, In Proceedings of the 16th ACM Conference on computer and communication security ACM, pp. 235–245.

Evigator, (2012) http://www.evigator.com/iphorensic/ (accessed June 7th 2012).

Fabian, B., Goertz, F., Kunz, S., Muller, S. and Nitzsche, M. (2010). - A usability analysis of the tor anonymity network, in Proceedings of the 16th Americas Conference on Information Systems (AMCIS) (Lima, Peru, 12–15 August 2010), in Sustainable Business management, Nelson, L., Shaw, M.J., Strader, J.t, eds, pp. 63–76.

Felt, P.A., Egelmen, S. and Wagner, D. (2012), I'got 99 problems, but vibration ain'nt one: A survey of smartphone users' concerns, SPSM 12, ACM, 2012, Raleigh, North Carolina, USA, Proceedings, pp. 37–46.

Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G.M., Méhes, A., (2007) Can You Infect Me Now? Malware Propagation in Mobile Phone Networks, The 5th ACM Workshop on Recurring Malcode (WORM'07), Alexandria, VA, November 2007), pp.87–96.

Forbes, 2013. The Promise of Privacy. URL: <http://www.forbes.com/insights/promise_of_privacy/index.html> (accessed June 14th, 2014).

Freedom house report (2013), Freedom on the Net Report, URL:http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.VDUBSmPlHig (accessed, 30th June).

Freegate. (2012) http://www.dit-inc.us/freegate/ (accessed May 5th, 2012).
Gallivan, M.J., Depledge, G., 2003. Trust, control and the role of interorganizational systems in electronic partnerships. Inform.Syst. J. 13 (2), 159–190.
GLOBAL PRIVACY REPORT 2013 Consumer attitudes towards privacy in mobile apps., URL:http://mediacenter.avg.com/content/dam/mediacenter/MEF_GlobalPrivacyReport_ExecutiveSu mmary_FINAL.PDF (accessed June 27th, 2014).
Grace, M., Zhou, Y., Zhang, Q., Zou S.,Jiang, X., (2012). Riskranker: Scalable and Accurate Zero-day Android, Malware detection, MobiSys 12, Proceedings, ACM, pp. 334–345.
Grefen, D., Karahanna, E., Straub, D.W., 2003. Trust and TAM in online shopping: an integrated model. MIS Q. 27 (1), 51–90.
Guardster. (2012) http://www.guardster.com (accessed May 6th, 2012).
Ibbott, C.J., O'Keefe, R.J., 2004. Trust, planning and benefits in a global interorganizational system. Inform. Syst. J. 14, 131–152.
ITU, Measuring the Information Society Report for (2013), http://www.itu.int/ (accessed, February 28th, 2014).
Jamaluddin, J., Zotou, N., Coulton, P., (2004), Mobile phone vulnerabilities: a new generation of malware, IEEE International Symposium on consumer electronics, Proceedings, pp. 199–202.
Joinson, Adam N., Ulf-Dietrich, R., Buchanan, Tom, Paine Schofield, Carina B., 2010. Privacy, trust and self-disclosure on-line. Hum. Comput. Interact. 24, 1–24 (2010).
Karlin, J., l Ellard, D., Jackson, W. A., Jones, E., C., Decoy Routing (2013): Toward Unblockable Internet Communication, www.usenix.org/event/foci11/tech/final./Karlin.pdf (accessed, January 4th, 1.2013).
Kingping IK., and Mudge M., (2001) Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats. In SSYM 01, Proceedings of the 10thUSENIX Security Symposium, pp. 30–35. (2001).
Liang, T.P., Yeh, Yi.H., Effect of context on the continuous use of mobile services: the case of mobile games, (2011), Pers. Ubiquit. Comput. Vol. 15, pp. 187–196.
Maitland, C., Thomas (Trey) III, H.F., Ngamassi Tchouakeu, L.M., 2012. Internet censorship circumvention technology use in human rights organizations: an exploratory analysis. J. Inform. Technol. 00, 1–17.
Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., 2011. Smartphone security evaluation – the malware attack case, SECRYPT, 2011. SciTePress Spain 2011, 25–36.
Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D., 2013a. Smartphone sensor data as digital evidence. Comput. Secur. 38, 51–75.
Mylonas, A., Theoharidou, M., & Gritzalis, D. (2013b). Assessing privacy risks in Android: A user-centric approach. Preprint. Springer-Verlag Berlin Heidelberg, pp. 65-78, 2013 (45) Proxify web proxy. https://proxify.com/ (accessed May 2012).
Price, B., Adam, K., Nuseibeh, B., 2005. Keeping ubiquitous computing to yourself: a practical model for user control of privacy. Int. J. Hum. Comput. Stud. 63 (1–2), 228–253.
Proxify web proxy. https://proxify.com/ (accessed May 2012).
Statcount, (2012) http://www.Statcounter.com/ (accessed May 7th 2012).
Straub, D.W., Nance, W.D., 1988. Uncovering and disciplining computer abuse: organizational responses and options. Inform. Age 10 (3), 151–156.
Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Q. 22 (4), 441–469.
Tor, (2012) https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf (accessed June 18th, 2012).
UN Report on Human rights and Internet access, 2011, A United Nations report:" Disconnecting people from the Internet is a human rights violation and against international law".
Wustrow, E., Wolchok, S., Goldberg, I., and Halderman, J. A. (2011) Telex: Anticensorship in the network infrastructure, 20th USENIX Security Symposium, Proceedings, 2011, pp. 45–57.
Zafar, H., Clark, J.G., 2009. Current state of information security research in IS. Commun. Assoc. Inform. Syst. 24, 572–596.
Zhen, Y., Conghul, L., Valterri, N., Gualianf, Y., 2013. Exploring the impact of trust information visualization on mobile application usage. Pers. Ubuquit. Comput. http://dx.doi.org/10.1007/s00779- 013-0636-4.
Zhou, Y., Wang, Z., Zhou, W., and Jiang, X, Hey, (2012) Get off of my market: Detecting Malicious applications in Official and alternative Android markets, In the Proceeding of the Network and Distributed System Security Symposium, 2012 (NDSS), pp. 217–2023.