

EVALUATION OF USER DATA PROTECTION AND PRIVACY PROVISION IN MOBILE NETWORKS WITH CASE STUDIES

Cormac Callanan

Doctoral Dissertation
Jožef Stefan International Postgraduate School
Ljubljana, Slovenia

Supervisor: Prof. Dr. Borka Jerman Blažič, Jožef Stefan Institute, Ljubljana, Slovenia

Evaluation Board:

Asst. Prof. Dr. Tomaž Klobučar, Chair, Jožef Stefan Institute, Ljubljana, Slovenia

Asst. Prof. Dr. Rok Bojanc, Member, ZZI d.o.o. and Jožef Stefan Institute, Ljubljana,
Slovenia

Prof. Dr. Tomaž Turk, Member, Faculty of Economics, University of Ljubljana,
Ljubljana, Slovenia

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
JOŽEF STEFAN INTERNATIONAL POSTGRADUATE SCHOOL



Cormac Callanan

EVALUATION OF USER DATA PROTECTION AND
PRIVACY PROVISION IN MOBILE NETWORKS WITH
CASE STUDIES

Doctoral Dissertation

VREDNOTENJE VARSTVA UPORABNIŠKIH
PODATKOV IN ZAGOTAVLJANJE ZASEBNOSTI V
MOBILNIH OMREŽJIH S ŠTUDIAMI PRIMEROV

Doktorska disertacija

Supervisor: Prof. Dr. Borka Jerman Blažič

Ljubljana, Slovenia, October 2017

*To Karmen and Tara
and in memory of Renee Callanan,
Deirdre Seachoy (nee Callanan) and Cormac Seachoy*

Acknowledgments

I would like to thank Prof. Dr. Borka Jerman Blažič who I was very fortunate to meet in 2010. She has guided me through the complexity of researching, testing, verifying and writing this doctoral dissertation. Her commitment to high standards has made this whole project both interesting and important. We discovered afterwards that we had both concurrently worked in different countries on the embryonic European internet during its early years in a disconnected Europe. We only got to share our similar experiences about this later in life. It is remarkable how connected the peoples of Europe are now and it is wonderful to have contributed in a small way to that change and to be part of it all.

I am grateful for the patience, encouragement and support from Karmen who listened and encouraged throughout the whole ‘project’. My most special appreciation goes to Tara. She will no longer need to ask me why I am working so much. It is I who regrets the lost time. I would like to thank Martin Smyth for supplying endless motivation and encouragement and for his excellent skills as a proof reader.

The study was partly supported by the US Freedom House and Broadcasting Board of Governors. Sincere thanks goes to Hein Dries for his support of the mobile device testing.

Abstract

This dissertation presents the results of a study of the availability of security provisions in the smartphones most frequently used to access the Internet in communities from different parts of the world. These areas differ in terms of their level of development and the degree of mobile-phone market control and state-enforced regulations. The level of development of mobile services was investigated. The most popular mobile phone devices in use were identified and then tested. The user skills levels and their assessment of the privacy and security risks they incur during use of smartphone were investigated.

The results of this extensive study are presented. The results profile user attitudes to mobile-phone network services, their level of awareness of threats to privacy, the opportunities for self-protection and their trust with respect to major players in the mobile network. The survey data collected from the user communities was analysed and the dependencies between the level of the mobile market development, the country's wealth, the affordability of the technology, the level of user skills and the understanding of privacy threats, and the expressed concerns regarding Internet-content blocking and traffic monitoring, in addition to the level of trust with respect to major players on the mobile-network market, are evaluated and discussed.

The technical testing confirmed that not every identified threat can be overcome since some smartphone systems do not contain secure technology for personal data protection. The influence of parameters such as the country wealth, the state religion and availability of high technology on user attitudes were explored and discussed. The answers confirmed the need for improved user understanding of the safety and security challenges in order to become more capable to manage the protection of their privacy. The user level of trust towards different actors on the mobile markets was found to differ depending on the country wealth and the market level development.

The countries were selected because of their developed mobile market combined with a reputation for insufficiently democratic governments. The studied sample has some limitation due to the restriction imposed by some governments regarding carrying user surveys.

This dissertation fulfils an identified need to study privacy and security risks in mobile usage in countries which have poor records in human rights and were not so far subject of a study in the existing literature. It confirms the challenges faced by users to understand their privacy and the possibilities to act for better personal protection.

Key words: Smartphone security, Traffic filtering and Internet-content blocking, Mobile communication networks, User privacy and Self protection

Povzetek

Ta doktorska disertacija predstavlja rezultate raziskave o razpoložljivosti varnostnih določb glede pametnih telefonov, najpogosteje uporabljenih za dostop do interneta v skupnostih iz različnih delov sveta. Ta območja se razlikujejo po stopnji razvoja in stopnji nadzora nad trgom mobilnih telefonov ter po državno uveljavljenih predpisih. Raziskana je bila stopnja razvoja mobilnih storitev. Prepoznani in preizkušeni so bili najbolj priljubljeni modeli mobilnih telefonov. Raziskane so bile stopnje usposobljenosti uporabnikov in njihova ocena tveganj v povezavi z varnostjo in zasebnostjo, ki nastanejo pri uporabi pametnih telefonov.

Predstavljeni so rezultati te obsežne raziskave. Rezultati orisujejo odnos uporabnikov do omrežnih storitev mobilne telefonije, njihovo stopnjo zavedanja glede groženj zasebnosti, priložnosti za samozaščito in njihovo zaupanje v povezavi z glavnimi akterji v mobilnem omrežju. Analizirani so podatki, zbrani z anketami v skupnostih uporabnikov, ki so ocenjeni, nato pa je opravljena razprava o odvisnosti med stopnjo razvoja mobilnega trga, bogastvom države, cenovno dostopnostjo tehnologije, stopnjo usposobljenosti uporabnikov in razumevanjem groženj varnosti ter izražanjem pomislekov glede blokiranja internetne vsebine, nadzorom prometa in stopnjo zaupanja v povezavi z glavnimi akterji na trgu mobilne telefonije.

Tehnično testiranje je potrdilo, da vsake prepoznane grožnje ni mogoče preseči, ker nekateri sistemi pametnih telefonov nimajo varne tehnologije za zaščito osebnih podatkov. Opravljena je raziskava in razprava o vplivu parametrov, kot so bogastvo države, državna religija in razpoložljivost visoke tehnologije, na odnos uporabnikov. Odgovori so potrdili domnevo, da morajo uporabniki boljše razumeti varnostne izzive, da bi bili zmožni bolje upravljati varovanje svoje zasebnosti. Ugotovljeno je, da se raven zaupanja uporabnikov do različnih akterjev na trgih mobilne telefonije razlikuje v odvisnosti od bogastva države in stopnje razvoja trga.

Države so bile izbrane na podlagi razvitosti trga mobilne telefonije ter slovesa nezadostno demokratičnih vlad. Raziskovalni vzorec je nekoliko omejen zaradi omejitev nekaterih držav v povezavi z izvajanjem anket med uporabniki.

Doktorska disertacija zapolnjuje prepoznano potrebo po raziskovanju tveganj v povezavi z varnostjo in zasebnostjo pri uporabi mobilnih telefonov v državah, kjer je spoštovanje človekovih pravic slabo, v razpoložljivi literaturi pa še niso bile predmet raziskave. Potrjuje izzive, s katerimi se srečujejo uporabniki, da bi razumeli svojo zasebnost, in ponuja možnosti, da ukrepajo za boljšo osebno zaščito.

Ključne besede: Varnost pametnih telefonov, filtriranje prometa in blokiranje internetnih vsebin, mobilna komunikacijska omrežja, zasebnost uporabnikov in samozaščita.

Contents

Acknowledgments	vii
Abstract	ix
Povzetek	xi
Contents	xiii
List of Figures	xvii
List of Charts	xix
List of Tables	xxi
Abbreviations	xxiii
Symbols	xxvii
1 Introduction	1
1.1 Description of the Problem	4
1.2 Motivation and Research Questions.....	6
1.3 Hypotheses.....	7
1.4 Methodology	8
1.5 Contributions.....	9
1.6 Thesis Organization	10
2 Background and Related Works	13
2.1 Regulatory Environment.....	14
2.2 Mobile Communications Standards.....	14
2.3 Security standards in mobile communication.....	18
2.4 Mobile Internet Access.....	20
2.5 The Impact of the BYOD Paradigm.....	20
2.5.1 BYOD Security Risks.....	22
2.6 Privacy and Security Issues in Mobile Internet	23
2.6.1 Threats and Attacks.....	24
2.6.2 Network and Devices Vulnerability Assessment.....	24
2.6.3 Data Privacy and Protection Approaches	25
2.7 Internet Filtering and Blocking.....	28
2.7.1 Background.....	28
2.7.2 Filtering and Blocking: the Cases of Non-Liberal Regimes	30
2.8 Circumvention Technologies	35
2.9 Security Risk Mitigation Issues for BYOD	37

3	Mobile Devices Assessment	39
3.1	Device Selection.....	40
3.1.1	Apple iPhone 4	41
3.1.2	Nokia N8	42
3.1.3	HTC Radar.....	42
3.1.4	HTC Desire.....	43
3.1.5	Blackberry Curve 8520	43
3.2	Mobile Operating Systems.....	44
3.2.1	Google Android.....	44
3.2.2	Apple IOS	45
3.2.3	Nokia Symbian.....	45
3.2.4	RIM Blackberry	46
3.2.5	Microsoft Windows Phone	47
3.3	Laboratory Test Environment.....	47
3.4	Laboratory Test Criteria and Assessment	48
3.5	Device Evaluation Approaches.....	52
3.5.1	Physical Access to Mobile Phones	52
3.5.2	Initial Execution Environment.....	52
3.5.3	Run-Time Environment	53
3.6	Evaluation Outcomes	54
3.7	Results and Discussion	55
4	User Communities Survey	57
4.1	Questionnaire Design and Data Collection.....	58
4.2	Community Profiles and the Mobile Markets.....	59
4.2.1	Country Classification	60
4.3	The Structure of the Questions	61
4.4	The Studied Country Profiles.....	62
4.4.1	Republic of Azerbaijan.....	62
4.4.2	Republic of Belarus.....	63
4.4.3	People's Republic of China	63
4.4.4	Islamic Republic of Iran.....	64
4.4.5	Sultanate of Oman.....	64
4.4.6	Kingdom of Saudi Arabia	65
4.4.7	Syrian Arab Republic	66
4.4.8	Tunisian Republic.....	66
4.4.9	Republic of Uzbekistan	67
4.4.10	Socialist Republic of Vietnam	68
4.4.11	Summary.....	69
4.5	Overall Results of the User Survey	69
4.6	Mitigating Filtering and Blocking and User Trust.....	74
5	Data Analysis	81
5.1	Research Hypotheses	81
5.2	Methodology.....	82
5.2.1	Factor Analysis.....	82
5.2.2	Regression Analysis.....	84
5.3	Results and Findings	87
5.3.1	Hypotheses H1 and H2	87
5.3.2	Hypothesis H3.....	89
5.3.3	Hypothesis H4.....	90

5.3.4Hypothesis H5	92
5.3.5Hypothesis H6	92
5.4 Discussion	96
5.4.1Tolerance towards Internet Content Blocking.....	96
5.4.2Privacy Views Different Between User Communities.....	98
5.4.3The Wealth of a Country	99
5.5 Findings and Conclusion.....	100
6 Conclusions	103
6.1 Findings	103
6.2 Research Completed.....	105
6.3 Dissertation Contributions.....	105
6.4 Future Work	106
Appendix A	109
References	113
Bibliography	127
Publications Related to the Thesis.....	127
Journal Articles.....	127
Conference Paper	127
Published Books.....	127
Reports	127
Other Publications	128
Biography	129

List of Figures

Figure 2.1: Model of Typical Mobile Network.	18
Figure 2.2: Responsibility of Security Provision in Mobile Station.	19
Figure 3.1: Apple iPhone 4.	41
Figure 3.2: Nokia N8.....	42
Figure 3.3: HTC Radar.	42
Figure 3.4: HTC Desire.....	43
Figure 3.5: Blackberry Curve 8520.	43
Figure 3.6: Diagram of Laboratory Test Platform.....	48
Figure 5.1: Independent Variables.....	84
Figure 5.2: Combined Independent Variables.....	86
Figure 5.3: Final completed conceptual model.....	96

List of Charts

Chart 4.1: Market Indicators for Azerbaijan from user survey.....	62
Chart 4.2: Market Indicators for Belarus from user survey.	63
Chart 4.3: Market Indicators for China from user survey.....	64
Chart 4.4: Market Indicators for Iran from user survey.	64
Chart 4.5: Market Indicators for Oman from user survey.	65
Chart 4.6: Market Indicators for Saudi Arabia from user survey.	66
Chart 4.7: Market Indicators for Syria from user survey.....	66
Chart 4.8: Market Indicators for Tunisia from user survey.....	67
Chart 4.9: Market Indicators for Uzbekistan from user survey.....	68
Chart 4.10: Market Indicators for Vietnam from user survey.....	68
Chart 4.11: Q3 PrePaid/PostPaid	70
Chart 4.12: Q4 Mobile Internet	70
Chart 4.13: Q5 Internet access.....	70
Chart 4.14: Q16 Who Pays?	70
Chart 4.15: Q15 Smartphone?	70
Chart 4.16: Q7 Handset Manufacturer	72
Chart 4.17: Q8 Phone OS.....	72
Chart 4.18: Q11 ‘Jail-broken’?.....	72
Chart 4.19: Q12 Firmware Upgraded	72
Chart 4.20: Q10 Share with Bluetooth	72
Chart 4.21: Q13 Skill Level.....	72
Chart 4.22: Q18 Mobile Usage.....	73
Chart 4.23: Q21 Detailed Billing	73
Chart 4.24: Q19 Mobile Internet Time	73
Chart 4.25: Q20 Mobile Content	73
Chart 4.26: Q14 Encounter blocked websites.....	74
Chart 4.27: Q22 Who monitors?.....	75
Chart 4.28: Q13 What is your skill level as a mobile internet user?.....	76
Chart 4.29: Q12 Have you ever updated the firmware on your mobile phone?	77
Chart 4.30: Q9 Where do you download apps for your mobile phone?	77
Chart 4.31: Q14 How often blocked websites are encountered on mobile Internet.....	78
Chart 4.32: Q22 Respondents view on who filters or monitors mobile internet.....	79
Chart 4.33: Q23 Who do you trust to protect the privacy of the mobile internet communications?	80

List of Tables

Table 2.1: Registrations at 3GPP TSG-SA meetings 1999-2013.....	16
Table 2.2: The place of blocking and circumvention tools effectiveness.	34
Table 3.1: Security Criteria for App Scoring.	50
Table 3.2: Resilience Criteria for App Scoring.....	51
Table 3.3: Usability Criteria for App Scoring.....	51
Table 3.4: Analysis of application effectiveness on smartphone OS platforms.....	56
Table 4.1: Mobile Market Size and market penetration (studied countries 2012)	60
Table 4.2: Operator ownership type and Mobile internet market (2012).....	60
Table 4.3: GNI (Gross National Income) in the studied countries.	61
Table 5.1: Correlation between GNI and Mobile Market penetration and IDI.....	82
Table 5.2: Country Level Independent Variables.	83
Table 5.3: Independent User-level Variables from user survey.	85
Table 5.4: Dependent variables from user survey.	85
Table 5.5: Overview of Independent and Dependent Variables.	87
Table 5.6: Factors associated with frequency of encountering blocked content.....	88
Table 5.7: Factors associated with opinion on state role for filtering Internet content ..	90
Table 5.8: Factors associated with opinion to whom user trust.....	91
Table 5.9: Factors associated with “jail-broken” phone and updating phone firmware..	92
Table 5.10: The ranking of the entities who user’s trust (all countries).....	93
Table 5.11: Ranking of entities whom users trust in group of seven countries.....	94
Table 5.12: Ranking of entities whom users trust in the group of three countries.	94

Abbreviations

3G	... Third Generation Mobile Networks
3GPP	... 3rd Generation Partnership Project
4G	... Fourth Generation Mobile Networks
A3	... GSM authentication algorithm
A5	... GSM encryption algorithm
A8	... GSM key generation algorithm
A.2DP	... Advanced Audio Distribution Profile
AES	... Advanced Encryption Standard
AKA	... Authentication and Key Agreement
API	... Application Programming Interface
ARIB	... Association of Radio Industries and Businesses
ASP	... Access Service Provider (ASP)
ATIS	... Alliance for Telecommunications Industry Solutions
AUC	... Authentication Centre
BBG	... Broadcasting Board of Governors
BES	... Blackberry Enhanced Server
BIS	... BlackBerry Internet Service
BSS	... Base Station Subsystem
BT	... British Telecom
BYOD	... Bring Your Own Device
BYOS	... Bring Your Own Software
CAGR	... Compound Annual Growth Rate
CCSA	... China Communications Standards Association
CDMA	... Code Division Multiple Access
CEO	... Chief Executive Officer
CI	... Confidence Interval
CIA	... Commonwealth of Independent States
CIO	... Chief Information Officer
CoIT	... Consumerization of IT
CSO	... Chief Security Officers
CSP	... Commercial Service Provider
CTR	... Currency Transaction Report
CYOD	... Choose Your Own Device
DACAS	... Data Assurance and Communication Security Research Center
DHCP	... Dynamic Host Configuration Protocol
DLNA	... Digital Living Network Alliance
DNS	... Domain Name System
DPI	... Deep Packet Inspection
EDGE	... Enhanced Data rates for GSM Evolution
EDR	... Enhanced Data Rate (Bluetooth)
EGPRS	... Enhanced GPRS. Also known as EDGE

EPOC	... EPOC is a discontinued family of graphical operating systems developed by Psion for portable devices, primarily PDAs. EPOC came from epoch, the beginning of an era. Succeeded by Symbian in 1998
ETSI	... European Telecommunications Standards Institute
EU	... European Union
EUR	... Euro
FBI	... Federal Bureau of Investigation
FIU	... Financial Investigation Unit
GAA	... Generic Authentication Architecture
GBP	... Great British Pounds
GCHQ	... Government Communications Headquarters
GDPR	General Data Protection Regulation
GEA3	... GPRS Encryption Algorithm 3
GNI	... Gross National Income
GNP	... Gross National Product
GPRS	... General Packet Radio Service
GPS	... Global Positioning System
GSM	... Global System for Mobile
GSMA	... GSM Association
GUI	... Graphical User Interface
HLR	... Home Location Register
HSDPA	... High Speed Downlink Packet Access
HSPA	... High Speed Packet Access
HTC	... High Tech Computer Corp of Taiwan
HTML	... Hyper Text Markup Language
HTTP	... Hyper Text Transfer Protocol
ICANN	... Internet Corporation for Assigned Names and Numbers
ICCID	... Integrated Circuit Card Identifier
ICT	... Information and Communications Technology
ID	... Identification Card
IDC	... International Data Corporation
IMEI	... International Mobile Equipment Identity
IMSI	... International Mobile Subscriber Identity
IOS	... Apple's mobile operating system
IP	... Internet Protocol
IPSec	... Internet Protocol Security
ISO	... International Standards Organisation
ISOC	... Internet Society
ISP	... Internet Service Provider
IT	... Information Technology
ITU	... International Telecommunications Union
JPEG	... Joint Photographic Expert Group
JTC1	... Joint Technical Committee 1
KB	... KiloBytes (1024 or 1000 bytes)
KSA	... Kingdom of Saudi Arabia
L2TP	... Level 2 Transport Protocol
LAN	... Local Area Network
LG	... Lucky Goldstar / LG Electronics.
LTE	... Long Term Evolution
MAC	... Media Access Control
MAM	... Mobile Anti-Malware

MB	... MegaByte (1024 or 1000 KB)
MCC	... Mobile Country Code
MCM	... Mobile Content Management
MDM	... Mobile Device Management
MEID	... 'Mobile Equipment IDentifier
MMS	... Multimedia Message System
MNC	... Mobile Network Code
MSIN	... Mobile Subscription Identification Number
MTS	... Mobile Telephone System
NCH	... National Children's Home. Now Action for Children
NGO	... Non-Government Organisation (a non-for-profit and/or a charity)
NIST	... National Institute of Standards and Technology
NSA	... National Security Agency
ODPC	... Office of the Data Protection Commissioner (Ireland)
OR	... Odds Ratio
OS	... Operating System
OSI	... Open Standards Institute
OSI	... Open Society Institute
OVI	... Nokia's Internet services
P2P	... Peer-to-peer protocol and applications
PAF	... Principal Axis Factoring method
PAN	... Personal Area Network
PDA	... Personal Digital Assistant
PPTP	... Point-to-point Tunneling Protocol
PRISM	... (Acronym) Planning Tool for Resource Integration, Synchronization, and Management - program of National Security Agency to collect and analyze private data stored on servers operated by Internet service providers
RAM	... Random Access Memory
RIM	... Research in Motion Corporation
SA	... Security Association
SIM	... Subscriber Identity Module
SIS	... Software Installation Scrip
SMS	... Short Message System
SOCKS	... SOCKetS
SPOF	... Single Point of Failure
SS7	... Signaling System 7 (telephony)
SSH	... Secure Shell
STR	... Suspicious Transaction Report
TCP	... Transmission Control Protocol
TDMA	... Time Division Multiple Access
TIA	... Telecommunications Industry Association
TLS	... Transport Layer Security
TMSI	... Temporary Mobile Subscriber Identity
TO	... Telecommunications Operator
TOR	... The Onion Router
TSG	... Technical Specification Groups
TSP	... Telecommunications Service Provider
TTA	... Telecommunications Technology Association
TTC	... Telecommunication Technology Committee
TV	... Television
UFED	... Universal Forensic Extraction Device

UK	...	United Kingdom
UMTS	...	Universal Mobile Telecommunications System
UN	...	United Nations
URL	...	Uniform Resource Locator
US	...	United States
USB	...	Universal Serial Bus
USD	...	US Dollars
VPN	...	Virtual Private Network
WIFI	...	Wireless fidelity
WCDMA	...	Wideband CDMA
ZTE	...	Zhong Xing Telecommunication Equipment (China)
ZUC	...	The name of the stream cypher used in 3G and is named after a famous Chinese mathematician called Zu Chongzhi.

Symbols

p-value . . . The attained level of significance.

Chapter 1

Introduction

The International Telecommunication Union (ITU) is a specialized UN agency that is responsible for 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% (ITU, 2013). The fixed-broadband market is still growing compared to the mobile market. However, 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 increase in household Internet access has also accelerated over the last years, mainly in emerging economies, and reached a global penetration rate of over 40% by the end of 2013¹.

Mobile phones are sophisticated devices that include all the elements of an excellent covert monitoring tool. They are personal devices that usually spend most of their existence physically close to their owner, fully-charged and perpetually connected to a mobile network. This enables easy data exfiltration and extensive remote command and control capabilities. They include microphones, cameras, speakers and storage capacities for text messages, recordings, lists of contacts, calendar entries and activity logs, and copies of personal documents, including digital certificates for the digital signing of documents. With the rapid growth of mobile technology, mobile services have become indispensable in the daily lives of people all over the world.

Research on the use and impact of mobile services has increased substantially (Gebauer & Shaw, 2004; Liang & Yeh, 2011) in the last decade. Mobile phones and handsets enable the users to use network services virtually anywhere and anytime. The mobile phones are connected to a radio data network that is managed and controlled by the network operator. The operator can manage the network and the handsets remotely with little or no knowledge of the end-user (Cisco, 2014a) (Cisco, 2014b) by pre-installing operator-selected and configured software and by applying surveillance or interception tools (Mylonas, Dritsas, Tsoumas, & Gritzalis, 2011; Mylonas, Kastania, & Gritzalis, 2013; US Federal Bureau of Investigation, 2017; Bencie, 2013). A by-product of the design of mobile devices and networks is the easy access to large volumes of usage & profiling data, often collected from the network, and sometimes directly from every device that is in use on the network (Roskowski, Kolm, Ruf, Jaquet, & Othmer, 2009).

Since mobile technologies are in widespread use around the world, there are numerous manufacturers designing, developing and selling equipment that can monitor and

¹ Ibid.

intercept mobile communications, enabling the data content to be passed to mobile operators, states, companies and third parties. There is a vibrant, competitive landscape (Banuri, et al., 2012) for the manufacture and sale of these interception systems. In some countries, vendors or operators are legally bound to offer a “backdoor” device entry to the government intelligence agencies.

With the creation of user communication and movement monitoring tools in parallel with the use of circumvention tools to avoid content blocking among the general public, open source circumvention solutions became widely available, such as Tor (Dingledine, Mathewson, & Syverson, 2004). These tools are broadly used across the developed world, in countries with high levels of democracy and human-rights protection (Maitland, Thomas, & Tchouakeu, 2012). Nevertheless, studies have shown that even in these countries, most users do not have sufficient technical knowledge or skills to download and use privacy protection tools (Felt, Egelman, & Wager, 2012a).

Freedom House (FreedomHouse, 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 were from the Asia-Pacific and African regions. Blocking access to information such as religious content, foreign news, or selected national news sources, as well politically sensitive content, is a problem that directly challenges freedom of speech. In addition, the interpretation of what constitutes hate speech or terrorist content differs from one country to another.

The development of security and safety strategies for mobile network users in less developed countries with lower levels of human-rights protection proved to be complicated. Traffic monitoring and Internet-content blocking are frequently applied, but insufficiently studied due to the difficulties in surveying the user communities. The national restrictive measures such as content blocking which have been implemented are mainly justified by a state strategy (Wustrow, Wolchok, Goldberg, & Halderman, 2011) that acts to restrict information flows. These measures include limitations to 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 designed to provide communication security, protect privacy, and circumvent censorship.

The advanced technological features of smartphones (and other mobile devices) manufactured today certainly empower developers to build very attractive and innovative smart phone applications offering services which use SMS, MMS, sensors, cameras, movies and location-based services which use the Global Position System (GPS). The use of such personally sensitive resources prompts the users to protect their privacy during legitimate use of the services available. Users expect the base framework of mobile devices to be sufficiently secure or, at least, sufficiently transparent about the negative risks and also capable of informing the user about these potential risks. Users certainly expect clear information regarding malware intrusion risks or about interception tools that can be undesirably included within downloaded mobile phone applications. Similar concerns apply for user expectations regarding trust in the neutrality of the service and the network operators (Yan, Liu, Niemi, & Yu, 2013).

Running applications when the handset is used as a communication and a working tool connected to a mobile network is by far the most important area where users are exposed to threats (Fleizach, Liljenstam, Johansson, Voelker, & Mehes, 2007). Not only are they exposed to various potential attacks with malicious code, the main privacy threat on mobile networks is the collection of real-time activity data generated from the use of the mobile phone (Bellens, Vlassenroot, Verstraeten, & Guatama, 2011; Vlassenroot, Gillis, Bellens, & Gautama, 2015). It is not only text and voice services

which are at risk but also location data and other forms of online communications are the main target of many monitoring or blocking operations performed by specialized agencies or telecommunications operators themselves.

It should not be forgotten that physical access to mobile phones is, conceivably, the most intrusive of all threats. As a result of gaining physical access to a mobile device an attacker exposes the mobile device's storage media, creating possibilities to extract stored data and confidential credentials. Close-proximity access such as near-field communications, tethered connections and Bluetooth, can yield similar results.

Privacy in ubiquitous computing environments was studied very early by Bellotti and Sellen (Bellotti & Sellen, 1993). They discussed the threats and classified them in two categories: technological threats and network design threats that are coupled with end-user social behavior characteristics. Both types of threats are important to understand the level of privacy provision in mobile devices as recommended by Price et al. (Price, Adam, & Nuseibeh, 2005). According to them the key enablers of privacy provision are reasonable and fair information practices and technologies for supporting these practices such as the anonymization of user identity records and the protection of data generated during their use of the mobile devices and the storage of the data on mobile devices. Similar aspects for privacy provision have been identified by Adams and Sasse (Adams & Sasse, 1999) and by Bellotti and Sellens² that have classified the areas where the user can control the disclosure of his/her data and consequently their privacy. In their studies, Joinson and others (Joinson, Reips, Buchanan, & Schofield, 2010) confirmed that privacy and trust have a symbiotic relationship and that users demonstrate reduced privacy concerns when they are confronted with a trusted data requestor.

This is further complicated by the rise in the Bring-Your-Own-Device (BYOD) paradigm in the workplace. Modern smartphone and tablets have been widely adopted in our personal lives because they offer a comprehensive solution to mobile IT communications needs and are fully expandable through the apps store. According to Kinsey research in 2013 almost 80% of Chief Information Officers (CIOs) will authorise mobile access to company data & applications (Disterer & Kliener, 2013). It is significant that this reverses the usual trend where IT innovation formerly progressed from commercial organisations into private space. In 2014 IDC estimated (Akuity, 2014) that over 65% of 480 million smart mobile devices shipped by 2016 would be used as BYOD in companies. MarketsandMarkets (MarketsandMarkets, 2014) expect that by 2019 the BYOD market will develop to over USD 266 billion. In 2016, IDC forecast (BusinessWire, 2015) that the U.S. mobile worker population will increase years from 96.2 million in 2015 to 105.4 million mobile workers from 2016 to 2020. By 2020, IDC expects that three quarters (72.3%) of the total U.S. workforce will be mobile workers. In the BYOD concept, individual users choose technology based on a complex range of personal preferences (Hansen, 1972) and based on their own level of competency and trusted recommendations from friends. In the past such devices would be researched and selected by qualified IT experts after a complex, comprehensive review of available configuration options and necessary functionalities including privacy protection, reliability, features, security and cost. As a result, innovation is now being driven by unskilled user demand and modelled using widely understood consumer models. According to Gartner (Gartner, 2013), in 2016 over 38% of companies plan to stop providing devices to workers. They expect employees to provide their own devices and many companies will only offer partial reimbursement for the device purchase. In 2016, a Gartner (Gartner, 2016) survey on mobile device adoption found that the majority of

² Ibid.

smartphones used in the workplace were personally owned devices and only 23 percent of the employees surveyed were issued with business smartphones. According to Syntonic (Syntonic, 2016) in 2016, 87 percent of companies rely on their employees using personal devices to access business apps and 60 percent companies had a BYOD-friendly policy in place. The employer increasingly covers the cost of the mobile communications cost rather than the individual devices.

The collection and processing of personal data about individuals has become a profitable aspect of online commerce. (Forbes Magazine, 2012) Internet companies have adopted a complex range of policies and protocols relating to this collection and processing of personal private data to enhance online profiling and advertising revenue. (The New York Times, 2012).

1.1 Description of the Problem

Security and trust issues in smart phones are becoming more threatening in the last years as the volume of malware or other spoofing tools has increased significantly (Jamaluddin, Zotou, Edwards R., & Coulton, 2004; Bury, Ishmael, Race, & Smith, 2010; Wang, Streff, & Raman, 2012a; Enck, Ongtang, & McDaniel, 2009). Recent disclosures of monitoring and blocking of internet traffic transmitted over mobile networks increased the additional concerns regarding privacy and data protection (OpenNet Initiative (ONI), 2012). Security and safety strategies and data-protection tools are also widely developed by professionals and manufacturers, but they have tended to find a market for their products in developed countries with a high level of democracy. However, developing security and safety strategies has additional complexity for users of mobile networks in countries with fewer protections for human rights.

Currently, there are only a small number of studies (Mylonas, Theoharidou, & Gritzalis, 2013) about privacy risk assessments for smartphone users that were implemented in countries (Greece and the UK) that are subject to Council of Europe and European Union traditions, conventions and directives protecting human rights, including privacy. The findings from the small subset of studies pointed to security complacency, where users disregard security when downloading and installing applications from official manufacturers and non-official application stores.

The problem of privacy and data protection in mobile networks still needs special focus and research for assessing the capabilities of user devices (which include built-in applications and tools in the respective operating systems) and the mobile network technology that enables the use of different circumvention tools. The challenge of privacy and data protection in mobile networks which implement traffic blocking and monitoring is still not an adequately addressed research problem and is additionally hampered by the rapid evolution of mobile devices and mobile communications.

The problem is two dimensional. Firstly, there are the technologies and tools used for security and circumvention. Secondly there are the attitudes of the user communities and their understanding of the risks and threats. An additional complication of the problem relates to the level of protection of human rights in different regions of the world with different regimes due to the increased level of state based regulation of the telecommunications market.

This dissertation identifies, accurately and comprehensively, the potential threats of mobile technologies that are used in regions with highly developed mobile markets which are not signatories to the European Convention for the Protection of Human Rights and Fundamental Freedoms. The purpose of the dissertation is to evaluate and assess user/personal data protection and privacy provision in mobile networks with case studies

of users' communities belonging to different countries regarding the level of technological development and the telecommunication market.

The dissertation explores the level of user awareness of the misuse of personal and traffic data by state-mandated blocking and monitoring and the level of trust associated with the mobile-network stakeholders that are operating in the mobile markets in twelve selected countries: Arab Republic of Egypt, Kingdom of Saudi Arabia, Socialist Republic of Vietnam, People's Republic of China, Republic of Azerbaijan, Republic of Belarus, Islamic Republic of Iran, Socialist People's Libyan Arab Jamahiriya, Sultanate of Oman, Syrian Arab Republic, Republic of Tunisia and Republic of Uzbekistan. These countries have higher levels of state regulation and ownership of their mobile networks (Wustrow, Wolchok, Goldberg, & Halderman, 2011) than previously studied European markets (Mylonas, Theoharidou, & Gritzalis, 2013).

In addition, the dissertation considered the effectiveness of the technology used to empower users to manage their private data and to enable protections against state-sponsored or malicious code attacks. The dissertation evaluated the use of circumvention tools for traffic monitoring and content blocking on the most frequently used mobile devices in the markets of these selected countries. This focused on the role of particular factors, such as wealth, religion and availability of high technology, on user attitudes towards content blocking and traffic monitoring. It explored the level of user trust regarding state-owned entities in the mobile market. Technology is not the only aspect of the very important issue of security and data protection. Another aspect of the studied problem of privacy provision and data protection is the level of awareness, knowledge and understanding of the threats by the end-users.

The countries have been selected based on market characteristics that enabled a deep analysis and evaluation of the components influencing the level of user trust to particular stakeholders in the mobile communication market. A common aspect of all these geographically dispersed countries is a regime with strong regulation of the mobile telecommunications market and a history of lower levels of human rights protection but at the same time they also exhibit significantly high levels of usage of mobile devices and networks. The selected user communities from a specific country differ regarding culture and values, the state supported religion, citizen wealth, the level of mobile market development, the presence of the latest mobile technology and handsets, the availability of circumvention tools and the level of user awareness and experiences. The interdependence between these factors and user safety requires deep and exhaustive study. This study is complemented by a study of the technical security properties of the devices and the network itself. A good review of both the operating system security properties and the separately developed security tools to be used on both sides of the telecommunications system are also part of the research in this dissertation. The evaluation of the available security solutions and the study of the differences in the level of user capabilities to use self-protection applications enabled the exploration of the notion of trust towards the main stakeholders in the telecommunications market. These findings are expected to contribute to the understanding of the current and emerging mobile communication technology and market development.

The main purpose of the dissertation is to provide an up-to-date assessment and evaluation of the existing security and safety tools provided within the operating systems of the most frequently used smart phones and to analyse the technical characteristics of the mobile networks in the studied countries regarding the possibility of using technology that enables circumvention in case of traffic blocking and monitoring. The results of the technical analysis and the information collected from the studied user communities provide guidance and recommendations about the technology to be developed and international actions to be taken for the implementation of the required worldwide

Internet security and user privacy protection which are the most hotly researched problems today.

The goal of the dissertation is to develop a conceptual model that follows from known methodologies used in this area of research (Mylonas, Dritsas, Tsoumas, & Gritzalis, 2011; Enck, Ongtang, & McDaniel, 2009) for evaluation of the security and safety provision in user mobile devices. Additional goals are to explore the possible interdependencies between the level of development of telecommunications technology in a country, the wealth of the country and its citizens, the availability of applications to circumvent traffic blocking and monitoring and consequently the market and the level of trust in the main actors governing the state based mobile telecommunication market. The goal of the dissertation is to propose good processes, guidelines and recommendations regarding the evolution of circumventions tools and solutions that can more closely protect user and data privacy regardless where the mobile devices are used across the world.

1.2 Motivation and Research Questions

The current mobile operators that control the mobile network in a particular country or region can manage the network and connected handsets remotely with little or no knowledge by the end-user through the pre-installation of operator selected and configured software and by applying lawful surveillance or interception tools to enable complex traffic and user profiling. In addition to risks associated with text and voice data, location and environment data (GPS, compass, movement sensors, proximity sensors, etc) and other forms of online communication are also the target of traffic monitoring and blocking operations performed by the operator or specialized agency.

Considering these conflicting elements, the problem that needs to be investigated is the influence of the information society development indicators on public awareness about security threats and user attitudes towards state-imposed Internet content censorship especially in the developing or emerging economies with a lower level of human rights protection.

The research questions associated with the dissertation for these countries are:

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 present in order to enhance a user's capacity to recognize content blocking and monitoring?
3. How is the affordability and accessibility of security technology related to user capabilities to use smartphone applications for better privacy protection?
4. Which entity is recognized 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 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?

To answer these questions, hypotheses were established. Objectives of the research followed both sets. They were:

- Assess the global inter-dependency between mobile smartphones, the Internet and the mobile telecommunication networks
- Develop a technical test model and report on the results of a technical assessment of the different existing hardware and software components in use in the operating systems and apps of mobile devices in terms of user security and data protection
- Identify the issues relevant to a comprehensive risk assessment which each user should conduct about their national activities and expose the risks and threats for users of mobile devices and networks in the studied countries
- Develop a structural model that assesses the level of technology development, knowledge of end users and their level of skills to mitigate security risks
- Identify the key risks for users that will improve awareness and increase the level of user safety in mobile networks
- Identify the interdependence between the level of technology in use, the wealth of a country, the level of the telecommunications market, and the user trust to particular authorities or operators

In addition, a research contribution is the identification of the differences in the users' understanding of security and privacy among emerging and developing economies. The answers to research questions were derived from the body of data collected through an exploratory study carried out in Africa (Tunisia, Egypt), the Middle East (Iran, Libya, Oman, Syria and Saudi Arabia), Asia (Azerbaijan, China, Uzbekistan and Vietnam), and Europe (Belarus). These 12 countries were selected on the basis of the human rights-related criteria developed by Freedom House, an independent nongovernmental organization dedicated to the protection of human rights around the world (FreedomHouse, 2013) and by the Broadcasting Board of Governors (BBG). They were also involved in the data collection and management for the purposes of this study (Callanan & Dries-Ziekenheiner, 2012).

1.3 Hypotheses

The research questions were reformulated into these hypotheses that governed the research they need to be confirmed or rejected by the data analysis.

- H.1: A greater user awareness of Internet content restrictions is associated with higher levels of information society development.
- H.2: The user level-of-skill positively correlates with user capability to recognize traffic monitoring and content blocking.
- H.3: A higher level of information society development contributes to greater user awareness that content blocking and monitoring is performed by state owned agencies.
- H.4: 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.
- H.5: Skilled users are more likely to have jail-broken phones and to have updated the firmware on their phones which enables them to improve their privacy protection.
- H.6: User tolerance of content blocking and the user trust in state-owned agencies as entities that care about their privacy are correlated with a high level of information society development, the availability of technology, and the wealth of a country.

The structural model that was designed after the survey data evaluation was used to confirm or reject the six hypotheses.

Another important objective of the study is to investigate if there are any differences between the chosen communities in terms of their attitude towards state Internet content restrictions, communications 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 respect for human rights is not questionable, such as France and Italy.

The hypotheses will be proved or rejected with the following research methodologies:

1.4 Methodology

A comprehensive study of the current research activities in this space will be completed with a review of the current approaches and methods for providing security and data protection to users of mobile devices. This will also identify the main strengths of the specific approach adopted for this dissertation – the technical assessment, the in-country expert survey and the in-country user survey combined with comprehensive up-to-date research on the mobile markets in the selected countries. The following research methods were applied:

a) Experimental Technical Assessment

A specially designed network with mobile telecommunications access functionality with all relevant components and internet access was set up for technical assessment and detailed forensic analysis of the major phone platforms used in the selected user communities. Mobile devices with at least five different operating systems (OSs) in widespread usage throughout the studied user communities were studied. One of the data sources was the global StatCounter website (StatCounter, 2012), which tracks mobile OSs of the devices on a number of websites throughout the world.

The testing environment was set by a known engineering method and consisted of a Wi-Fi router (with controlled access to a DNS) and a 3G connection to a UMTS-capable mobile network. In order to further influence certain parameters of the VPN connections used by the various operating systems, a VPN service was configured on a dedicated server running Linux OS on a remote network.

The resilience of mobile-phones to direct data extractions by persons with direct physical access to the phone was tested with the Cellebrite mobile-forensics solution known as UFED (Cellebrite, 2012) and the Oxygen mobile-handset forensic suite (Oxygen Forensics, 2012).

For each application/service installed on the mobile handset, each of the parameters defining the security was investigated in three primary categories:

1. Security (OS requires Rooting to ensure security, App “permissions” proportional, Anonymity, Prevents tracking, Range of Apps supported, Cryptography on the connection link, Cryptography on stored data,
2. Resilience to blocking, Plausible deniability, System fingerprints, Carrier loss - turn WiFi off, other carrier present, Carrier change - forced on WiFi-router); and
3. Usability (Ease of Installation, GUI, Documentation, Languages Supported, Speed). Each of these parameters will be scored for each application tested.

Not all mobile handsets were available in every market.

b) Survey study

The user communities in 11 countries found in Europe, Middle-East, Asia and Africa were selected based on the differences in characteristics that are assumed to influence the level of user trust they were approached with a questionnaire that was administered in the national market. A separate survey of mobile users was conducted by the individual in-country experts. The purpose of the survey was to add interviews as a supplement to the knowledge gained from the experimental technical assessment aimed to provide a richer understanding of the mobile usage patterns and the user capability to manage the security. The survey results were elaborated with known statistical methods and analytical insights are outlined.

c) Data Analytics

In order to confirm the defined hypotheses, which were based on the research questions, data analysis was implemented on the information collected in the user survey. This analysis enabled conclusions to be drawn regarding the factors that influence user attitudes towards mobile services privacy threats and their trust in the studied countries that have more restrictive regimes and strongly controlled mobile markets. This provides input on the most effective and significant impact approaches to raise awareness about security risks and to develop processes to encourage and stimulate an increase in safer use of mobile devices

The results of the user survey were compared with the GNI indexes and with the affordability of mobile technology in the studied countries as measured by ITU (ITU, 2012) as a percentage of Gross National Income (GNI) per capita for each country. The analysis enabled the development of a structural model which supports future research initiatives in the specialist area of user security and privacy in the increasingly mobile dependent world.

1.5 Contributions

The scientific contributions of the dissertation are important and are part of the ICT mobile security area. The security and personal data protection risks faced by end users of mobile devices and mobile networks are clearly identified. This dissertation accurately and comprehensively identifies the potential threats of mobile technologies which are used in regions with different levels of mobile market developments and different telecommunication market regulation.

1. The research includes detailed analysis and findings about the capabilities of modern mobile devices regarding security applications that provide data and privacy protection. It also considers the availability of ease-to-use tools for circumvention of blocking systems in order to access blocked content and upload sensitive information to online services. The work of the dissertation identifies necessary system capabilities required in order to protect the personal data of mobile data users and the conflicts this causes with government national security.

The completed research provides a better understanding of the current situation, as a precursor to the adoption of new, advanced and affordable security ICT applications in the developing world. Significant difficulties were overcome to obtain information about the emerging and developing countries' perception of security and their fears about personal data privacy abuse. This is important for the development of 'off-the-shelf' protection tools. The research findings also contribute to the provision of secure network services, which are a prerequisite for the growth of the information society globally. Researchers gain a baseline

analysis of inherent privacy and personal data threats and risks associated with the use of mobile technologies. It becomes clear how such issues are a design feature of the mobile ecosystem and difficult to mitigate.

2. The research includes good analysis and findings about the level of user understanding of mobile device technology, awareness about internet blocking and filtering and skill level of the approached user communities regarding protection of personal data. It identifies the challenges users are faced with state actors.

The challenges they face depend critically on the design of the hardware, the design and implementation of the operating system and the range of applications which are installed, and the regulatory environment where the mobile network operates. These properties are evaluated in semi-real and experimental environments.

The level of security provision in mobile networks depends on the skill level of the user in addition to capabilities of the hardware and software of the mobile device. This required onsite studies in different environments especially in those that were not studied and evaluated previously due to some restrictions. The dissertation determined the best tools available today to be applied by the end users for their own privacy protection in areas where end users fail to do so due to factors beyond their control. Knowledge about user attitudes and understanding of self-protection capabilities regarding privacy will be included as this provides important knowledge and research regarding future technology and market development.

3. A structural model was developed that defines the influence and the dependencies between the level of information society development, the affordability of ICT technology, user skills and the level of user protection capacity, awareness of internet blocking and filtering, awareness that these activities are initiated by the state & government and the differences regarding the tolerance toward this type of monitoring and blocking. The wealth of countries and their user communities show similar attributes as western developed countries such as the USA and Europe.

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

1.6 Thesis Organization

Chapter 1 is this section which provides an introduction to the area of research, including the motivation and purpose of the thesis, a problem statement and an outline of the contributions. Chapter 2 provides a comprehensive background and related works including mobile communication networks, privacy and security issues in mobile networks (threats and attacks, network and devices vulnerability assessments, bring-your-own-device in the workplace, user awareness), standards and regulations, technology evolution and modern mobile devices and open security issues. Chapter 3 describes the mobile devices assessment including a description of the laboratory technical testing environment, the creation of the laboratory test criteria, and the results of the assessment. Chapter 4 describes the user survey including the selection of the methodology and the applied approach. It covers the community profiles and the mobile markets, the specification of the questionnaire and elaboration of the survey results.

Chapter 5 analyzes the collected data and proves the research hypotheses through a comprehensive analysis of the results of the research and the study including discussion and analytical analysis of the regression models, develops a conceptual model based on the data analysis and concludes with the findings and conclusion. Chapter 6 provides a concise conclusion and identifies future work in this area.

Chapter 2

Background and Related Works

According to the Internet Society Report for 2013 (Internet Society, 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. In May 2015 the internet society (Internet Society, 2015, p. 44) noted that in 2013 global 3G and 4G capable phone and mid-screen device connections reached 1.97 billion, a penetration of 28%. Global penetration was forecast to grow quickly towards a maximum of 71% in 2019. The Internet Society Global Internet Report 2016 (Internet Society, 2016) report does not cover mobile internet broadband trends but focuses on data breaches. 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 enabled through a mobile broadband network via a fixed wireless network or a satellite is often the only alternative to a fixed network infrastructure. Studies (ITU Broadband Commission for Digital Development, 2013a; ITU Broadband Commission for Digital Development, 2013b; Cisco, 2014a) 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 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 in a mobile device introduce many new services. However, they create new challenges relating to 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 (Yan, Liu, Niemi, & Yu, 2013).

Although, literature defines different aspects of trust (Ažderska & 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 & Blažič, 2012; Ažderska & Jerman Blažič, 2011). This is similar to the institutional trust as defined by Grefen et al. (Gefen, Karahanna, & Straub, 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.

2.1 Regulatory Environment

There are many stakeholders with different areas of responsibility in the mobile network industry. Most countries have a government department for information and communications technologies (ICT) responsible for implementing government telecommunications market policy, facilitating the delivery of broadband Internet and administering the electromagnetic spectrum for communication and broadcasting. A robust, modern and efficient telecommunications infrastructure is considered to be vital for the national economy. As a consequence, most 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 in 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 should be an independent body not directly controlled by the state. However, this is very often not the case. This body is often responsible for the regulation of 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 telecommunications operators (TO) – or a telecommunications service provider (TSP) - which operate in the state-regulated market environments. They provide telecommunications services, such as telephony and data communications access, to consumers and businesses. Mobile handset manufacturers are responsible for the design, development, and manufacture of devices, in compliance with internationally adopted technical standards for mobile networks. These are then, subject to state approval, sold in different mobile markets around the world. Often manufacturers adapt handsets for different markets depending on the requirements of the state in which they are sold. Mobile operating systems (OS) developers create the required interfaces installed on mobile handsets enabling the communication with the country networking infrastructure.

The mobile communication market is a fast changing and highly volatile area. In China alone, over 30 million additional subscribers were added to the mobile networks in the first three months of 2012. The Kingdom of Saudi Arabia is remarkable for having achieved over 195% penetration of mobile subscriptions in the mobile market – an average of almost 2 mobile subscriptions for every person in the country. Similar trends are present in other markets e.g. The Sultanate of Oman fluctuates between 160-190% market penetration of mobile adoption. These trends are related to the developed technology based on international standards.

2.2 Mobile Communications Standards

The standards developed in this area are achieved either through an open public processes or through a restricted access environments based on membership fees and sometimes in individual private companies conducting research and winning patents and copyright on their intellectual property. The convergence of mobile capabilities with mobile internet services creates a challenge to the different processes of standards development as adopted by internet organizations and those processes traditionally used by the global telecommunications industry. Most of the mobile communication technology originated in the western part of the world and the relevant standards were adopted in standard organizations with predominately western-based membership. However, the phenomenal breakthrough in world markets with ICT and mobile handsets

industry and other mobile technology in some Asian countries have changed the scene. This is certainly the case in countries such as South Korea, Japan, China and Taiwan.

The widest adopted standard technology in the mobile communications is certainly GSM. The GSM^{TM3} (Global System for Mobile Communications) is a set of standards developed in the 1990's by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile handsets. ETSI is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe and the final specification set was completed in 1996 and enhanced over the subsequent years. The GSM standard originally described a digital, circuit switched network optimized for full duplex voice telephony. This was expanded over time to include data communications, first by circuit switched transport, then packet data transport via GPRS (General Packet Radio Services) and later EDGE (Enhanced Data rates for GSM Evolution or EGPRS).

In 1998, ETSI⁴ agreed that a partnership project with US, China, S. Korea and Japan - called the Third Generation Partnership Project - would be formed with other interested regional standards bodies, allowing a common system for the third generation (3G) cellular technology to be developed for Europe, Asia and North America. The 3rd Generation Partnership Project (3GPP^{TM5})⁵ brings together six telecommunications standard development organizations including Association of Radio Industries and Businesses (ARIB), Japan, Alliance for Telecommunications Industry Solutions (ATIS), USA, China Communications Standards Association (CCSA), Telecommunications Technology Association (TTA), South Korea and The Telecommunication Technology Committee (TTC), Japan, which are known as organizational partners. The 3GPP enables members of those organizations to produce reports and specifications that define 3GPP technologies. This structure has created third generation (3G) UMTS standards followed by fourth generation (4G) LTE Advanced standards.

3 "GSM" is a trademark owned by the GSM Association (formed in 1995)

4 <http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/cellular-history> (last accessed 2-May-2013)

5 www.3gpp.org (last accessed 2-May-2013). The terms 3GPPTM, LTETM, and UMTSTM are registered Trade Marks of ETSI.

Table 2.1: Registrations at 3GPP TSG-SA meetings 1999-2013.

3GPP Registrants 1999-2013	TSG-SA	Meeting	
Organisation/ Partner	SA	WG3	LI
ETSI	5,654	2,260	737
ARIB	1,128	233	4
ATIS	839	349	146
CCSA	647	295	11
TTA	540	52	
TTC	500	38	
Other*	379	57	39
TIA	1	2	2
	9,688	3,286	939
* Research, Manufacturing, Admin, no affiliation			

The Service and Systems Aspect Working Group#3 is responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols. WG3 also ensures the availability of cryptographic algorithms which need to be part of the specifications. The sub-group SA3-LI provides the requirements and specifications for lawful interception in 3GPP systems. Table 2.1 shows that there has been active participation mainly by many Asian companies from China, Japan and Taiwan. It is relevant to note the level of participation of Chinese participation since it is one of the selected countries for the research. There have been 61 meetings of the TSG-SA with over 9,266 registered to attend those meetings. SA-WG3 had 71 meetings to April 2013 with 3,286 registrants. There were 49 meetings of the SA3-LI subgroup with over 939 registrations to attend their meetings. During this period, there were 15 attendees registered to attend the LI subgroup from companies registered with the CCSA. A large organization such as HuaWei Technologies Co. is affiliated to several organizational partners (directly or through subsidiaries) in the major world standard organization including ETSI, CCSA, ATIS, ARIB and TTA. From 1999 to 2013, 243 attendees registered for TSG-SA meetings from HuaWei Technologies Co (Huawei, 2017) 169 registered for WG3 meetings and 3 for WG3-LI meetings. ZTE Corporation (ZTE, 2017) is the second highest organization represented (134 attendees) at WG3 meetings, yet is at number 10 on the TSG-SA meetings and is not in the top 10 for the WG-3 LI subgroup meetings. It is affiliated to both ETSI and CCSA. In short, with exception of China it is reasonable to state that no interest or any other activities are present in the studied countries in this area of standardization.

An important design element in the mobile communication market is the International Mobile Station Equipment Identifier (IMEI) (3GPP, 2009; GSMA, 2011) There is a regulatory requirement⁶ for each mobile device to have a unique identifier and the International Mobile station Equipment Identity (IMEI) is used for that purpose. The GSM Association allocates IMEI number ranges to all manufacturers of 3GPP compliant devices to ensure that no two devices use the same IMEI, and it records all of

⁶ Example of UK legislation in this area includes the Mobile Telephones (Re-programming) Act 2002 <http://www.legislation.gov.uk/ukpga/2002/31/section/1> (last accessed 14-May-2013)

the IMEIs that are allocated to mobile device manufacturers in the IMEI DB. The GSM Association maintains a global central database containing basic information on serial number (IMEI) ranges of mobile devices (e.g. mobile phones, laptop mobile data cards, etc.) that are in use across the world's mobile networks called an IMEI Database⁷ (IMEI DB). The network operators TOs and TSPs use the information in the IMEI DB to determine what types of devices are being used by their customers on their networks, and what features the devices support, so they can offer the latest services to their customers through their networks if this is a part of their policy.

The other important identifier is the International Mobile Subscriber Identity (IMSI). The number is hard-coded in the SIM card for GSM, UMTS and LTE network. It is also used for acquiring other details of the mobile user in the home location register (HLR) or is locally copied in the visitor location register. To mitigate interception attempts identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible and a randomly generated TMSI (Temporary Mobile Subscriber Identity) is usually sent instead. The ITU E.212 (ITU, 2008) numbering standard⁸ specifies the structure of an IMSI number. An IMSI is usually presented as a 15 digit long number where the first 3 digits are the mobile country code (MCC), followed by 2 or 3 digits for the mobile network code (MNC) and the remaining digits are the mobile subscription identification number (MSIN) within the network's customer base. IMSI analysis examines a subscriber's IMSI to determine which network the IMSI owner is subscribed to, and whether subscribers from that network may use a given foreign network. ITU Recommendation E.214 (ITU, 2005) provides a method to convert the IMSI into a number that can be used for routing to international fixed-line telephone (SS7) switches.

The combination of IMSI and IMEI links a unique subscriber account to a unique physical device and it is possible to monitor which handsets an IMSI is used in and which handsets have been used with different IMSI numbers. Lawful interception is protected through the use of authorization and authentication protocols and unlawful interception is prevented through the implementation of mobile network encryption technologies. Unlawful interception is not a research issue covered in the dissertation. Instead the focus is on extensive use of lawful interception by some regimes which might be considered inappropriate by the democratic standards in countries where personal freedoms are considered a fundamental human right.

A mobile device has many unique identifiers for the handset and the user. As previously stated the handset has an IMSI (subscriber identity) and an IMEI (mobile device) identifier. In addition the device has a unique ICCID (Integrated Circuit Card ID) which uniquely identifies the specific SIM card (which can be reprogrammed for a different IMSI on a different network), a MAC (media access control) address for each of WIFI and Bluetooth LAN and PAN network interfaces, a mobile equipment identifier (MEID) and a manufacturer serial number. Even without these listed unique identifiers a combination of supplementary data elements (combination of nearby wifi networks, combination of nearby Bluetooth devices, location information, broadcast modem and device software installed, unique combination of applications installed, time/date configuration, regional settings including default dictionary and keyboard selected, social network accounts) can identify an individual from others among a crowd who use a similar type of mobile device. A device model number, modem firmware, OS version and

⁷ <http://www.gsma.com/technicalprojects/fraud-security/imei-database> (last accessed 14-May-2013)

⁸ E.212 - The purpose of Recommendation ITU-T E.212 is to define a unique international identification plan for public fixed and mobile networks providing users with access to public telecommunication services. The plan is hierarchical and identifies geographic areas, networks and subscriptions.

language and regional settings in combination can significantly identify a specific user. Of course, the software apps often contain further information including app store registration details, email addresses, twitter accounts, linked-in accounts and Facebook accounts. Payment accounts are also part of the mobile devices.

2.3 Security standards in mobile communication

Security standards based on encryption algorithms (Lo & Chen, 1999) are an essential part of a technology to ensure effective and secure authentication, as well as to provide data integrity and protection in order to prevent fraud and unauthorized access to public and private telecommunications networks and protect user data privacy. There are several algorithms specified in the 3GPP™ Confidentiality and Integrity Standard Algorithms. GSM uses three different security algorithms called A3, A5 (GSMA, 2000), and A8. In practice, A3 and A8 are generally implemented together (known as A3/A8⁹). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centers. It is used to authenticate the customer and generate a key for encrypting voice and data traffic. An A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy. An A5 algorithm is implemented in both the handset and the base station subsystem (BSS).

The GSM Association is a custodian of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS, that have been developed through the collaborative efforts of the 3GPP Organizational Partners. The A5/3 and GEA3 algorithms are based on the 3GPP ciphering algorithm (F8), for which Mitsubishi Electric Corporation holds essential patents. The A5/4 (3GPP, 2012) and GEA4 encryption algorithm specifications are also available.

ETSI is custodian of the 3GPP™ Confidentiality and Integrity Algorithms (ETSI, 2012), UEA1 & UIA1 which were developed through the collaborative efforts of the European Telecommunications Standards Institute (ETSI), the Association of Radio Industries and Businesses (ARIB), the Telecommunications Technology Association (TTA) and the T1 Committee. The UEA1 & UIA1 specifications (3GPP, 2007) can be used only for the development and operation of 3G Mobile Communications and services. Mitsubishi Electric Corporation holds essential patents on the Algorithms and DACAS China holds essential patents on the ZUC algorithm confirming significant commitment to mobile standards in Asian countries.

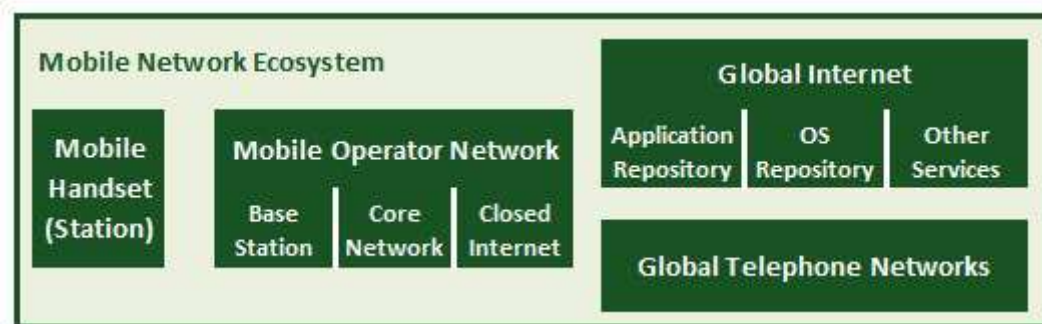


Figure 2.1: Model of Typical Mobile Network.

⁹ http://www.3gpp.org/ftp/Specs/archive/55_series/55.205/ (last accessed 15-May-2013)

The Generic Authentication Architecture (GAA) (3GPP, 2015) and the Authentication and Key Agreement (AKA) is a key security protocol used in 3G networks and is used for one-time password generation mechanism for Digest access authentication. AKA is a challenge-response based mechanism that uses symmetric cryptography. The GSM network authenticates the identity of the subscriber through the use of the challenge response protocol. Each subscriber is given a secret key, one copy of which is stored in the subscriber identity module (SIM) card in the mobile handset and the other in the authentication center (AUC) in the network. The SIM contains the ciphering key generating mechanism algorithm (A8) which is used to produce 64 bit ciphering key.

Other security standards applied in mobile networks for internet access have been developed within the Internet Engineering Task Force, which is supported by the Internet Society and in the respective ITU and ISO JTC1 SC27 Committees. They are commonly applied in fixed and in mobile networks in line with TCP/IP implementations and related applications.

The research in the chapters that follow provides results about the most popular mobile devices in a given country market with a given legal environment and the availability of technology to prevent or allow the use of the circumvention tools. Figure 2.1 illustrates the mobile network ecosystem and Figure 2.2 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 from the application stores. Operational functionality of these features depends on the network capability and functionality which falls within the operators' domain.

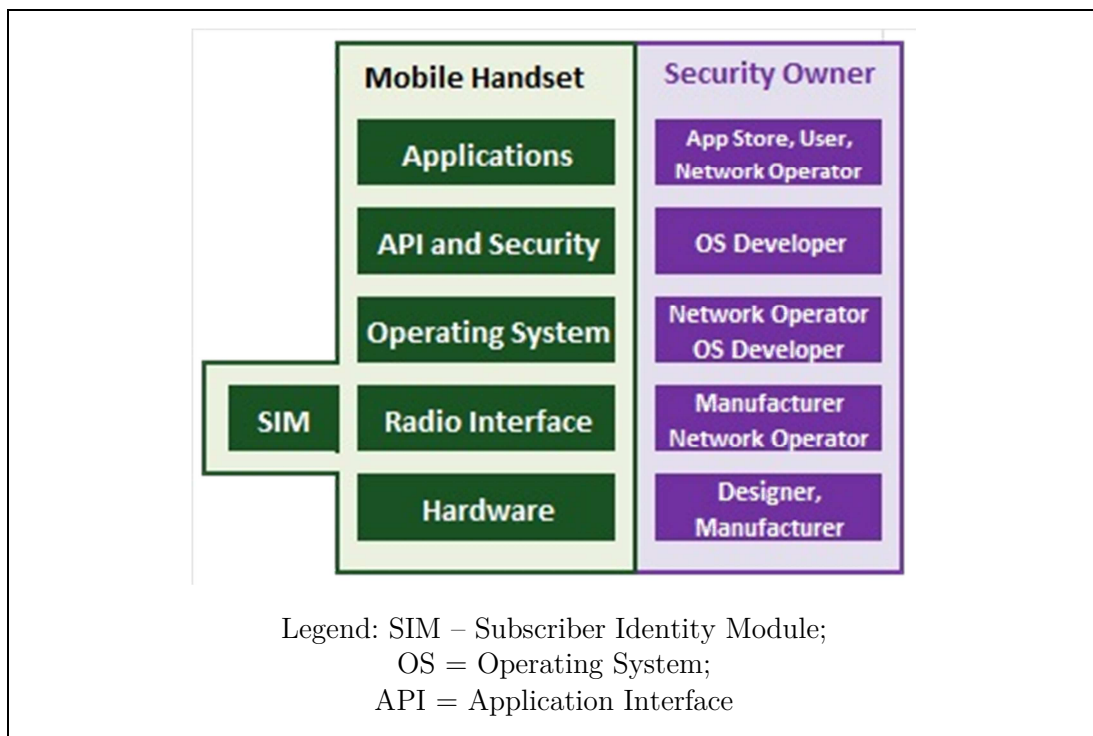


Figure 2.2: Responsibility of Security Provision in Mobile Station.

2.4 Mobile Internet Access

Access to the Internet through mobile networks typically involves the use of smartphones or tablets. These mobile devices can be connected to a variety of communications networks (most notably to Wi-Fi and mobile networks provided by telecommunications operators using a range of mobile communication protocols) which enable Internet applications to be operated on these devices. Executing applications and using the mobile device as a communication tool when connected to a mobile network is by far the most important aspect where users are exposed to threats (Fleizach, Liljenstam, Johansson, Voelker, & Mehes, 2007; Toyssy & Helenius, 2006; Hypponen, 2006). They are not only exposed to diverse potential attacks from malicious code, as is evident from the survey of Wang, Streff and Raman (Wang, Streff, & Raman, 2012b) but today the main threat associated with mobile networks is the rampant collection of real-time user-related private data that is collected while the mobile phone is being used (Bellens, Vlassenroot, Verstraeten, & Guatama, 2011) through the use of mobile monitoring tools. Text and voice data records are not the only risks since sensor data (Mylonas, Meletiadis, Mitrou, & Gritzalis, 2013) including location data and other types of online communication (instant messenger, social networking, etc.) form the primary focus of many monitoring or content-blocking operations.

Physical access to mobile phones remains the most intrusive of all threats, since by gaining physical access an attacker exposes the mobile device's storage media, leading to the possibility to extract stored data and credentials (Gold, 2011) despite the capabilities of the security technologies such as encryption. Close-proximity access (such as near-field communications, tethered connections and Bluetooth) can yield similar results.

2.5 The Impact of the BYOD Paradigm

Modern tablets and smart devices are very popular in our personal lives because they deliver a comprehensive solution to mobile personal communications requirements including voice, email, calendaring, contacts, messaging and are readily expandable through the online apps store. The innovative technological features of current state-of-the-art smart phones and other mobile devices enables developers to build user-friendly, multifaceted and advanced smart phone applications to utilise modules including sensors, camera, movement and location based services using GPS.

Mobile devices are also used in a range of professional situations and in a wide variety of innovative roles including academically qualified and certifiable distance-learning (Massive Open Online Course (MOOC)), collecting payments in small retail companies and accessing shared databases in private and public clouds. This changes the previous trend where IT innovation traditionally progressed from commercial environments into private arena. IDC estimated that in 2016 (Akuity, 2014) over 65% of 480 million smart mobile devices shipped will be used as BYOD in the office and in business environments. MarketsandMarkets assume that in 2019 the BYOD market will grow to over \$266 billion (MarketsandMarkets, 2014).

In the BYOD model, individual users choose technology based on subjective criteria and their own level of technological skills and individual experience. In the past such mobile devices would be selected by the company IT specialists after a comprehensive, impartial research of available configuration options and necessary features including privacy protection, reliability, functionality, security and cost. As a result, innovation is now driven by unskilled user demand and the devices are modelled using widely adopted consumer models. The ultimate selection of mobile devices is managed by corporate IT

specialists through administration of an approved-device list or with device selection guidelines¹⁰. Currently BYOD is most popular in large companies with greater than 2,000 employees and have large IT sections. It is significant that over 38% of companies intend to stop offering devices to employees in 2016 with many organisations contributing only partial financial compensation for the device purchased (Gartner, 2013). Increasingly the business covers the cost of the mobile communications costs rather than the purchase cost of devices which are then bought and funded by the employee.

Unfortunately, companies can unintentionally compromise their corporate security and confidential business data by permitting personal devices to associate with the corporate network (Beckett, 2014). Security is the highest concern and the subsequent risk of a data breach of commercially sensitive data records. In some markets, such as the financial sector, data breaches and security failures can result in high impact regulatory penalties and substantial reputational damage. Companies are susceptible to data loss when unregulated access to public cloud services and social media services is tolerated since confidential data can be easily published. This is aggravated when BYOD is widely supported and encouraged in the organisation. Advanced network security strategies and data-protection tools are being developed by security professionals and mobile device manufacturers to respond to these risks.

It is estimated that by 2016 there will be over 200 million users using their personal mobile devices for work activities. Research by Kinsey suggests that 80% of chief information officers will allow remote access via mobile devices to company data and applications (Disterer & Kliener, 2013). Romer estimates that the typical employee who uses mobile devices owns more than 3.5 devices (Romer, 2014). Employees use their own private mobile devices for job-related activities and are allowed to access business data and perform work activities using their own devices. Over 80% of workers use personally purchased mobile devices for work-related functions (Morrow, 2012). Personal desktop computers are used by 47% employees, 41% use personal laptops, 24% use smart phones and 10% use tablets. It is evident from any research results that the BYOD revolution is increasing and offers significant benefits and challenges to both employers and employees.

The standard company IT strategy where the company purchases IT services and equipment for staff in line with widely accepted IT security rules and procurement rules is no longer considered the optimal IT solution. The equipment selected in this process is now considered too constricting on innovation and efficiency where employees now believe that technology which is available to consumers is of higher quality than technology provided by the company. When the employee can personally select the most appropriate device, each employee may decide to use different mobile platforms or operating systems. This new paradigm has created a new term called “consumerization of IT” (CoIT) which has been adopted to describe the use and spread of consumer market devices into the work place (Zahadat, Blessner, Blackburn, & Olson, 2015; Disterer & Kliener, 2013). The extensive research confirms that adoption of the BYOD paradigm improves work-place effectiveness because employees are more content and effective in using their personally selected devices (Zahadat, Blessner, Blackburn, & Olson, 2015; Vignesh & Asha, 2015). BYOD has been the accepted practice for many years in other industries. It was initially adopted to encourage employees to protect and properly maintain their own tools and this is the same motivation in IT. Personally selected mobile devices with remote access to corporate networks supports flexible work patterns and results in a significant increase in employee flexibility and mobility. However, the boundaries between business and home life become more distorted due to flexible work

¹⁰ An approved list of acceptable devices for a company enables CYOD – Chose Your Own Device

patterns. This often results in higher expectations on employee availability outside normal working hours. For some professions there are unique benefits and challenges.

a) Law Enforcement

The Association of Chief Police Officers (ACPO) in the United Kingdom published Guidelines on the Safe Use of the Internet and Social Media by Police Officers and Staff (ACPO, 2013, pp. 7-8) which offer important indicators on the complexity of employee security in an increasingly mobile world. For example, it is recommended that they request 'Google maps' to remove photos of their home, car or family members from their site and ensure privacy and security settings for social media accounts are configured to the highest possible level; As regards social media accounts they should be observant and report if they become the victim or target of online abuse linked to their occupation or if a false social media account is creating claiming to be used by the police officer, or if their real social media account is duplicated, attacked, or subsumed by someone else.

b) Health Care

Healthcare (West, 2012) is a key area which significantly benefits from broad adoption of mobile devices where patients can use personal mobile devices (sometimes in combination with specialized sensors and software) to track the state of their own health and even access their medical consultants and facilities.

Physicians who have adopted BYOD respond faster to medical results, and have fewer mistakes in prescriptions and demonstrate improved record-keeping skills. (Zahadat, Blessner, Blackburn, & Olson, 2015).

c) Academia

In the academic environment, staff and students have a higher expectation of data privacy relating to the use of personal mobile devices in the academic environment especially relating to data protection and employee monitoring and tracking. (JISC, 2015a).

There are legal risks associated with BYOD where there is potential for a high volume of unsuitable or illegal material being uploaded or distributed on the network. There is an increased risk of lost personal or confidential data (JISC, 2015b).

2.5.1 BYOD Security Risks

Despite the widespread adoption of BYOD, many IT security professionals remain concerned about allowing employees to use personal devices for work related activities or alternatively, the use of company purchased mobile devices for personal use due to security concerns and risks associated with regulatory compliance responsibilities. There are justifiable anxieties caused by unauthorized data disclosures and risks associated with stolen devices including subsequent loss of both sensitive data and access credentials. Personal devices such as smart mobile phones are not sufficiently designed with relevant corporate privacy and security requirements and they struggle to match well established corporate security paradigms.

Data pollution is also a concern where company data becomes blended with private data and personal data being unintentionally backed-up to company storage networks or the company cloud. Increased risk is present when company confidential data is uploaded to higher risk, consumer cloud accounts with associated regulatory compliance risks.

The security concerns also relate to the conflicting aims of employer policies in this area which often strive to restrict which additional software apps can be installed and which users can use the mobile device outside the office and what the device can be used for. It would be desirable that it is only used by trusted and trained persons with reasonable knowledge of the potential security risks but this is not always practical. For example, can the mobile device be used to test and develop new high-risk software applications? Can other family members store private medical information or family videos on the device? As a result of all these security risks the meaning of the acronym BYOD is often changed to “Bring Your Own Danger” (Romer, 2014; Kargl, Lawrence, Fischer, & Lim, 2008).

There are a wide range of risky home network devices that might also track and record network related communications without clear consent or permission to unauthorized third parties. Users might also use document scanners which keep detailed log records, consumer products such as Samsung SmartTV (The Telegraph, 2015; theGuardian, 2015; Samsung, 2015), Mattel Barbie children’s toys¹¹ (the Register, 2015; Sophos, 2015) which keep voice recordings or printers (O'Connor, 2006). All these are risks for network intruders and data leakage.

BYOD is about the user selected and purchased device. However, company IT specialists recognize additional risks associated with other devices in the BYOD communications channel. Remote employees achieve access to corporate networks using consumer internet accounts, across routers and wireless access points which are often configured, managed and monitored by consumer internet access providers. These providers have increased regulatory liabilities to retain internet traffic and subscription records and identify internet malware or possible illegal activities.

Consumer smartphones are often configured to backup data stores on the device into unencrypted, unsecured consumer cloud to protect against the event of a complete failure of the mobile device. These backups have private access records for WIFI hubs, including secure passwords associated with SSID in addition to GPS location-based data. This means that any unauthorized access to cloud stores data is a risk.

Applications installed by the employee for personal use such as gaming, gambling or social networking applications could leak data which might be commercially sensitive or legally privileged. For example employees located in unpublished client offices can leak location information and therefore disclose the identity of clients. Doctors might unintentionally leak private sensitive data when they conduct patient home visits and even police investigations can collapse through inappropriate use of social network services.

2.6 Privacy and Security Issues in Mobile Internet

The risk of a privacy breach during a communication (run-time) is high, but (Lo & Chen, 1999) regular SMS text and voice, from the privacy point of view, are neither protected nor secured. Some of the replacement services for SMS and voice often run on phone devices with specific Internet services, e.g., secure e-mail or voice-over-IP, which make it possible to bypass the service provider’s infrastructure. In all cases the services provide

¹¹ “Hello Barbie is equipped with a microphone and Wi-Fi connection that’s engaged when you hold down a button on the doll’s belt. When a child talks to Hello Barbie, the conversation is recorded and sent (encrypted) to a server where it’s interpreted by speech-recognition software, and the doll “talks back” to the child with pre-programmed responses”. (Sophos, 2015)

protection by applying cryptographic techniques, and in most cases, offer more applications than just the text messaging and voice communications.

Current developments in Internet technologies offer many simple circumvention tools for privacy provision, and also for 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 & Nance, 1988; Straub & Welke, 1998; Dhillon & Torkzadeh, 2006; Dinev & Hu, 2007; Zafar & 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 & 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, Thomas, & Tchouakeu, 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.

2.6.1 Threats and Attacks

Like SMS text messages, the voice service on the average GSM network is also susceptible to snooping (Schmidt, et al., 2009). Saltaformaggio and his colleagues developed a tool called Netscope that uses traffic behavioral clues to detect fine-grained user activities from the fingerprints left behind by the apps they use and the wireless network traffic’s behavior (Saltaformaggio, et al., 2016). At present, in terms of the widely implemented technology in some countries, no options exist for encrypting GSM voice-traffic applications without the use of special hardware. However, alternative connections can be made with proxy servers (UpsideOut, 2012) or with the use of software-based encryption for bypassing blocking and monitoring, such as the use of VPN (Virtual Private Network) technology. Rather than bypassing the censor at a per-application level, it is also possible to capture and reroute the mobile device’s entire Internet connection (Levine & Shields, 2002; Born & Gustafson, 2010).

2.6.2 Network and Devices Vulnerability Assessment

There are many simple applications available for increasing the level of secrecy for personally identifiable traffic data, including the use of proxy services or tunnels to and through unfiltered locations. Examples include Proxify, Psiphon (Manning, Gomes, & Rahimi, 2014), Global Pass (Smart, Tedeschi, Meakins, Hannay, & Bolan, 2008), SSH tunnels (Dusi, Gringoli, & Salgarelli, 2008) Corporate VPNs, Freerate (Dynamic Internet Technology, 2016) and Ultrasurf (Appelbaum, 2012). Furthermore, since these proxy and tunnel hosts are easily discovered and blocked, some proxy services manage to cycle the hosts through a range of IP addresses to avoid blocking systems that use blacklists of proxy servers. The effectiveness of this evasion technique depends on the number of available IP addresses and their distribution across the IP-address space. At a high level, this is the mechanism used by popular services such as Tor (Dingledine, Mathewson, &

Syverson, 2004), Global Pass, and anonymizer. Although these proxy services use different techniques (VPNs, SOCKS proxies, HTTP proxies, content forwarders) they are categorized as a circumvention proxy or just a proxy. Researchers have also developed the means for covertly burying traffic inside communication channels intended for use with other types of communication (such as web servers, images, and video files) via steganography or similar methods. Such techniques are complementary to decoy routing¹², as they could be used for covert signaling between the client and the decoy router, as suggested by Karlin et al. (Karlin, et al., 2011).

The security of mobile devices is still the main concern for many researchers; however, most of the recent studies deal with malware discovery in downloaded applications (Grace, Zhou, Zhang, Zou, & Jiang, 2012; Zhou & Jiang, 2012). The tools needed to remedy these concerns were to a large extent neglected (Felt, Egelman, & Wager, 2012a; Felt, et al., 2012b). A number of other authors went on to investigate a variety of vulnerable device interfaces, including Bluetooth (Bose & Shin, 2006) and the multimedia messaging subsystem (MMS) (Guo, Wang, & Zhu, 2004). They argued more generally that connecting unprotected smart devices to a mobile network could be problematic, but they only discussed attacks equivalent to local wireless jamming, denial of service on call centers (e.g., endpoints) and spamming. While the malware targeting (Jamaluddin, Zotou, Edwards R., & Coulton, 2004) of such devices has increased in line with the evolution of smartphones, some authors, including (F-Secure, 2005a) and (F-Secure, 2005b), claim that the widespread infection with malware, like that seen on the fixed Internet, has yet to be witnessed. A good overview of the risk-assessment methods relating to smartphone security was recently provided by Theoharidou, Mylonas and Gritzalis (Theoharidou, Mylonas, & Gritzalis, 2012).

Given that such devices continue to lack sufficient protection mechanisms, the most popular, widely adopted devices in the user communities in some of the selected countries were studied and tested in terms of aspects that were not covered by existing research. This includes the availability of circumvention technology for avoiding content blocking and traffic-data monitoring. To complement the analysis, the attitudes of the mobile-network users regarding their skill levels for managing their devices regarding security and privacy protection were studied. Their ability to update the functionalities of their mobile handsets to provide better privacy protection was evaluated. Finally, their awareness about privacy threats through blocking and monitoring, their resistance to or acceptance of their telecommunications operators' restrictions (e.g., jail-broken phone) and their trust in the stakeholders of the countries' mobile markets were investigated.

2.6.3 Data Privacy and Protection Approaches

The collection and processing of personal data about individuals is an increasingly significant aspect of online communications. All internet companies have adopted a range of comprehensive policies and detailed protocols relating to the collection and processing of personal data. The informed consent of all users is required and users have the right to access their own personal data or to request such data to be deleted.

Birnhack identified over 77 countries across the world which, over the last 40 years, have already adopted data protection legislation (Birnhack, 2008). Countries that need to exchange personal data with European countries within the EU or signatories of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 1981) are required to have an acceptable

¹² Decoy routing was proposed by Karlin et al. and has similarities to proxy technologies except that the proxy routing is performed at the IP level. It is described in more detail at the end of Section 2.8

level of data protection. The data protection regulations affecting multinational corporations trading in Europe cover issues relating to employees, customers (including potential customers) and to the transfer of personal data between Europe and other locations across the world. Hallinan and colleagues identified that notions of privacy and data protection are highly valued by citizens across Europe but they have little practical knowledge on data protection (Hallinan, Friedewald, & McCarthy, 2012). Wong concludes that a Data Protection framework is important for “*the protection of fundamental rights including privacy*” and “*the free flow of personal data.*” (Wong, 2011). She emphasises the need for clarity in the collection of personal data and the need for informed consent from the data subject. Acquisti and Friedman and Telang are concerned whether companies have sufficient incentives to protect personal data and they measured the impact of security and privacy breaches from 1999 to March-2006 and the reaction of companies to data breaches. (Acquisti, Friedman, & Telang, 2006). Although there is a substantial negative impact on data privacy failures, this reputational impact has short duration. In fact, attacks against a small number of organisations significantly influence the negative outcomes when the reputation of larger companies can be substantially damaged by high profile reports about privacy failures.

Over the last decades, Europe has made significant commitments to human rights and protection of personal data. The OECD first published data protection principles as recommendations called Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and TransBorder Flows of Personal Data in 1980 (OECD, 1980). The recommendation was published caused by concerns relating to the increasing use of automatic data processing and the impact of such processing on personal data and privacy. The Council of Europe convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108 (Council of Europe, 1981) was the first legally binding international instrument addressing personal data protection. It entered into force in October 1985 and there are now 47 states which have acceded to the convention. Parties to the Convention are required to take the necessary steps in their national legislation to apply the data protection principles which the convention specifies in order to ensure respect in each country for the fundamental human rights of all individuals.

It is important to understand and practice the principles on which Data Protection national legislations are based. In the OECD guidelines (OECD, 1980) these fundamental principles are listed as the collection limitation principle, the data quality principle, the purpose specification principle, the use limitation principle, the openness principle, the individual participation principle, the accountability principle and the basic principle of international application.

There are comparable elements in the EU Data Protection Directive 95/46/EC. In Europe data protection is complex with EU directives specifically addressing data protection which are then transposed into national law by the national parliaments. In October 1995, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (European Parliament and the Council of the European Union, 1995) was adopted by the European Parliament and the Council of the European Union. It was drafted with the specific intention to protect personal data collected for or about European citizens of the countries in the EU, especially as it relates to processing, using or sharing data.

Directive 2002/58/EC concerns the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Directives 2009/136/EC and Directive 2002/22/EC on universal service

and users' rights relating to electronic communications networks and services are specifically relevant to mobile networks.

In April 2016 the European Union published the final text of the General Data Protection Regulation (GDPR) Regulation EU 2016/679 (EUR-Lex, 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) in order to harmonize data privacy laws and will be applicable as of 25th May 2018 in all EU member states. It clearly states the principles relating to the processing of personal data and conditions relating to consent, access, rectification, erasure and transparency. It reinforces the rights of the data subject and applies to 'controllers' and 'processors' where the controller decides why and in what manner personal data is processed and the processor legally acts on behalf of the controller. The GDPR applies to data processing performed by organisations operating within the EU and also applies to organisations outside the EU that offer goods or services to *individuals* in the EU. The GDPR applies to 'personal data' but the definition is more detailed. It refers to sensitive personal data as "special categories of personal data" The Article 29 Working Party (European Commission, 2016) has published guidelines on Breach notification, automated individual decision-making and Profiling and on imposing administrative fines.

There have been some interesting and relevant decisions by the European Court of Human Rights. In *Copland vs The United Kingdom*, the European Court of Human Rights decided that phone communications, e-mails and personal internet use when on college premises are considered part of "private life" and "correspondence" for the purposes of Art 8. (*Case of Copland v. The United Kingdom*, 2007) The court decided that the employee had a reasonable expectation of privacy because the employer had not given prior notification of company monitoring. There were no provisions in national law or in the governing instruments of the college where she was employed which would indicate the conditions in which employers could monitor the use of electronic communications including telephone calls, e-mail messages and other internet use by employees.

In Ireland, where many US service providers are based in Europe (Apple, Google, Facebook, LinkedIn, etc.) this directive was transposed into Irish law called the Data Protection (Amendment) Act 2003 (Houses of the Oireachtas, 2003) which amended the Data Protection Act of 1988 (Houses of the Oireachtas, 1988). The Office of the Data Protection Commissioner (ODPC) operates a Code of Practice for Personal Data Security Breaches (Data Protection Commissioner, 2011) which requires notification of illegal access to personal data to be informed to the ODPC and to the Irish police and to the data subject. It can also necessitate the application of risk mitigation measures for the victims.

There are several categories of data which are retained by mobile service providers including subscriber data (name, address, service plan details, etc.), traffic data (date, time, duration, source, destination, etc.), content data (content of communications – voice, text, etc.) and billing data (detailed billing records, payment method, etc.). Personal data is not just specific data elements that can directly and immediately identify specific individuals. Data is also considered 'personal data' when a person can be uniquely and distinctly identified from within a large population by using combinations of data elements or other identifiers. Data records of online internet or mobile activities of users are distributed, mingled, persistent and multifaceted and any data that is collected must have the clear and unambiguous consent of the user subjects. Unfortunately, it is not always evident if users have a sufficient understanding of which personal data is collected nor if they realize how the data elements are technically selected and how collected data elements are processed inside profiling algorithms. It is

extremely difficult to comprehend how third party personal data from related persons (family, colleagues, friends and/or competitors) is blended with the previously collected data inside profiling processes. Finally, personal data from online activities is supplemented by data from real-world databases (credit reputation, health, insurance, etc.) creating significant growth in the area of predictive analytics and user profiling.

Duhigg writes how Target Corporation uses databases of information collected about their customers to perform complex predictive analytics relating to their shopping habits and behaviours (The New York Times, 2012). Target knows that consumer shopping habits change radically when a baby is born to a family and can be very profitable for stores who can actively market their products to such families. The marketing and I.T. specialists in Target created an analytics program to precisely identify women who were pregnant but had not publicly announced their condition. Target wanted to promote specific products to these families before their competitors. Unfortunately, this did result in one damaging public relations episode when Target directed unsolicited advertising to an underage high-school student about baby clothes and cribs on the prediction that she was pregnant – even though she was a minor. On this occasion, the Target Corporation profiling was correct and the student was later confirmed pregnant by her parents (Forbes Magazine, 2012).

There are also risks for companies who suffer data breaches when they are sued by employees for reputational damage caused by inadequate security measures. In October 2015, Sony settled a lawsuit with former senior employees (BBC News, 2015) in relation to a hack¹³ on Sony's computers, at a cost of \$8m because of the loss of embarrassing personal email data (Variety, 2015; Reuters, 2015).

2.7 Internet Filtering and Blocking

2.7.1 Background

The primary objective of Internet filtering is to prevent internet users from accessing, receiving or viewing specifically targeted content. Often the blocking system implemented prevents users inside one country from communicating with internet sites outside that country's borders. Such systems can also provide complex monitoring, logging and playback capabilities for authorized agencies. Internet filtering includes a broad range of policies, hardware, software and services. However, it is incorrect to consider all types of Internet filtering are the same or equally effective, legally equivalent or even that one system can easily be for blocking or filtering different types of content.

Personal filtering and network filtering are the two main styles of systems which are in everyday use. **End-user filtering** enables the user to decide which type of content is filtered based on criteria assigned to each individual computer user and can be individually tailored and configured for different categories of users (parent, child, teacher, student, etc). This type of filtering is the most specific but does not prevent users from accessing content which, though maybe illegal, it can still be accessed and downloaded. As regards **network-based Internet filtering**, the service-provider (Internet access provider, employer, club, etc) can determine which type of content or activity will be filtered for ALL users of the service, at least with regard to content accessed directly via the upstream network equipment of the provider where the blocking

¹³ In November 2014 Sony Entertainment was hacked and large volumes of commercial and personal data were stolen (Wired Magazine, 2014) along with embarrassing emails of senior employees.

technology is implemented. (Sometimes the system can be tailored to decide the blocking criteria based on identified users).

Ignoring the need for social debate about **why** society should filter content, two challenges are inherent to these filtering systems including **how** to technically specify what should be filtered and **who** should select what should be filtered. All Internet blocking systems are subject to false-negatives¹⁴ and false-positive¹⁵ problems and these are minimised during the design of the blocking technologies. Systems are then evaluated and compared based on these measures.

According to the members of the European Parliament, unimpeded access to the Internet without interference is a right of considerable importance. The Internet is “*a vast platform for cultural expression, access to knowledge, and democratic participation in European creativity, bringing generations together through the information society*” and is protected by the right to freedom of expression, even when it is not currently considered as a fundamental right in itself (European Parliament, 2008).

The first internet filtering initiative (also known as blocking) at state-level in a European state was announced in June 2004 by the Martin Bright, Home Affairs Editor of UK The Guardian newspaper in the UK, when an article¹⁶ was published. In this article he leaked pre-release information about a pilot project of British Telecom (BT) to prevent users of the BT internet services from accessing known images of Child Pornography. The idea for the project was attributed to Mr. John Carr, internet advisor to the Children’s charity NCH. The article highlighted the fact that blocking websites is a highly controversial approach in information control and until that moment was associated only with oppressive regimes such as Saudi Arabia and China, which have censored sites associated with their political dissidents. Many in the field of child protection believe that the explosion of paedophile sites justifies the crackdown towards control of free information flow. The internal project code-name was “BT Cleanfeed” – referring to a cleaned Internet feed that was further described in an article which published on The Guardian website by Mr. John Carr¹⁷. The BT Cleanfeed system uses a hybrid blocking technology developed by BT and targeted a list of fully specified uniform resource locators (URL). The list of URL’s was generated by the Internet Watch Foundation a non-profit non-governmental organisation combating online child-abuse material. BT offered the technology to other operators in the British market.

This was the first time that internet filtering systems were used in a democratic country to prevent all citizens from accessing a specific type of content. The announcement was the start of a very complex and extended debate on the rights and failures of network based content blocking systems used at a national level by internet access providers. The debate argued the technological effectiveness of such content blocking systems, the collateral and direct damage to rights of free speech, the commercial and non-commercial motivations behind such systems and the impact on child protection processes. There was extensive debate on the subject of which type of rejection/blocking/failure message to issue. One proposal, which was initially adopted, was to issue a message “http 404” that indicates that the requested HTML page is not available inaccurately suggests that the sought content was “not found”. The second proposal, which was later adopted more widely, was to issue a so-called “stop page” in

¹⁴ A false-negative is when content is not blocked by the filter when it should be blocked.

¹⁵ A false-positive is when content which should not be blocked but is blocked by the filter. Since the positive result is incorrect it is called a false-positive.

¹⁶ Martin Bright, Home Affairs Editor, The Guardian, BT puts block on child porn sites, 6 Jun 2004 Pg 7

¹⁷ John Carr, The Guardian, Turning a corner in online abuse?, 7 June 2004

HTML stating that the content was found but considered to be illegal. The other issue of major concern was whether the IP addresses of those who had tried to access the illegal content and were therefore blocked from accessing that content should be reported to law enforcement. BT then decided that such details would not be passed on to law enforcement. Callanan, Gercke, De Marco and Dries-Ziekenheimer (Callanan, Gercke, De Marco, & Dries-Ziekenheimer, 2009) describe many of the issues and challenges relating to internet blocking. (McIntyre, 2011)

2.7.2 Filtering and Blocking: the Cases of Non-Liberal Regimes

The survey of UK public opinion confirmed that there is broad agreement for specific blocks to be developed and implemented to uphold various aspects of public policy where the functionality of the Internet cause (international) enforcement issues. The subject matters vary from the availability of hostile speech (e.g. Yahoo banned online sales of Nazi memorabilia in France in 2001¹⁸) on specific sites connected to online marketplaces with gambling websites hosted in countries with liberal regimes in relation to online gambling. Similarly, states with less open information regimes are using blocking tools as a technical resource for extending their practice of information control into the online world. Clayton (Clayton, 2006) highlights the weaknesses of such blocking systems and how they can be used to reverse engineer the list of web sites being blocked. He claims that BT's Cleanfeed was designed as a low-cost very-precise system for blocking Internet content. To keep costs under control this was achieved by treating some types of traffic specially and this special treatment can be detected by end users.

The preservation of human rights such as freedom-of-expression or right-to-privacy—which are in conflict with an internet blocking measure, i.e. the right to privacy or to freedom of expression - are considered as intrinsic to democracy. Internet blocking systems operated by states have the capacity to interfere with citizens' fundamental human rights.

Strategies to disrupt circumvention tools are diverse. They include technical measures to prevent accessing circumvention tools or using the circumvention tools, disrupting the process of accessing blocked content, monitoring tool use and identifying the parties involved. The strategies also include legal and self-regulatory measures to sanction circumvention or prevent distribution of tools and the promotion of distrust and stimulating fear and uncertainty about the security of circumvention tools combined with high profile success stories which promote and exaggerate the effectiveness of monitoring and blocking systems.

Zittrain and Palfrey (Zittrain & Edelman, 2002) tracked 2,038 blocked pages from the Saudi-installed filtering systems. According to their research all web traffic in Saudi Arabia is transferred through a group of central proxy servers operated by the Governments Internet Services Unit, which implements Internet content filtering across the high-speed data links that connect the country to the international Internet. In 2011, F-Secure reported (F-Secure Labs, 2011; Egyption Chronicles, 2011) that protesters in Egypt took over the Headquarters of the Egyptian State Security and gained access to a large volume of confidential state documents including an offer for an intrusion and spying software product called FinFisher sent to the Egypt State Security Investigation Department. FinFisher included multiple components, including an "infection proxy" and

¹⁸ In November 2000 a French court said Yahoo must block French users from accessing sales of Nazi memorabilia on its US-based auction pages. The decision set a precedent that Web companies operating on the global Internet can be required to tailor their practices to the laws of a particular country. <https://www.wsws.org/en/articles/2001/01/yaho-j05.html>

various network intrusion tools. F-Secure confirmed that they have never received a request from any police force or intelligence organization to prevent detection of known “Trojan code”. Nonetheless, in 2009 HBGary with General Dynamics planned to develop and install stealth software on a target laptop without the owner's knowledge (Anderson, 2011). HBGary stated they could develop multiple laptop-access techniques using less than 1 kilobyte of memory each. A basic rootkit sold for \$60,000 and HBGary expected to sell this new product for “around \$240k”.

Internet industry players had come from a position of self-regulation and providing support and advice to governments and law enforcement to proactive and reactive strategies on many aspects of cybercriminal activity.

Steps taken to filter illegal activity on the internet vary from democratic judicial-oversight to state-sponsored filter of internet communications has significantly evolved since 2001. Today, there are many strategies to attempt blocking of internet content and also to disrupt internet blocking with circumvention tools. Technical measures were developed to attack information systems, create rogue SSL certificates for man-in-the-middle attacks, disrupt usage, prevent access to content, monitor usage and, where possible, identify the parties involved. There are legal and self-regulatory measures to sanction circumvention or prevent distribution of such tools. To block content, identifiers are needed whereby a blocking decision can be implemented. These identifiers can be an IP addresses, Domain names and DNS, fully specified or shortened URLs, file content and/or filename, keywords and content signatures (hash values). Different identifiers are required for different types of internet services. The variety of blocking options and the assessment of effectiveness and complexity are summarised in Table 2.2.

Network based blocking is implemented in several methods:

- Internet Protocol (IP) address Blocking
The easiest systems are DNS and IP blocking. Illegal content is linked to an IPv4 address on the internet and the routers of the internet access provider are then configured to block access to that IP address. For example an IPv4 address of 123.456.789.123 would be blocked in the international links of an internet access provider and customers would not be able to access any content on that IP address. As regards web traffic using the http protocol the user would receive a HTTP 404 error (which means that the server is not found) IP blocking can be very broad since an IP address can refer to a collection of machines (though load balancing servers) and/or domains (using virtual hosting of content) and all services/protocols operating on those machines including email, web, etc. In these situations therefore, there is significant over-blocking (Table 2.2).
- Domain Name System (DNS) blocking
Illegal content is linked to a specific domain name which is then blacklisted. The DNS system of the internet access provider or the local DNS server (if operating behind a firewall or inside a commercial network) would block access to the black listed domain. For example, a domain name such as `aconite.com` is resolved to an IPv4 address (123.456.789.123) using the Domain Name system. To block access to this domain the domain name system is configured to redirect the valid address to a white listed address instead. Where `aconite.com` correctly resolves to an IP address of 123.456.789.123 the black listed domain will connect instead to 111.222.333.444 instead. At that address it is possible to host a notification page alerting the user that the content has been blocked. Of course such redirections often happen on the internet for legitimate technical reasons. Once the user is redirected to the new location, it is possible to record the requesting IPv4 address of the user.

INTERPOL provides a list of domains containing child sexual abuse content to any (Internet) Access Service Provider (ASP) who decides to block such domains on the Web. The "Worst of"-list includes domains that contain the most severe child sexual abuse material. Participation is voluntary where Internet traffic is redirected away from child sexual abuse material to a "stop page" hosted on an ASP server. The "stop page" provides a mechanism to receive complaints about the blocking of a domain. (INTERPOL, 2017)

- URL Blocking

A major weakness of both IP blocking and Domain Name blocking is the significant over-blocking that is likely to occur and the negative impact on legal content using such systems. URL blocking attempts to address this issue by creating a two phase system of blocking content that targets clearly specified content on the internet. It has the potential for under-blocking since the URL string is very specific and small changes can prevent blocking.

A URL is designed to specify exactly an element of online content and it includes a protocol specification, a domain name, a subdomain name, an IP port and a hierarchy of folders which host a specific file of a specific file type. For example a URL which is written as: `http://www.dub.aconite.com:8080/mainfolder/subfolder/illegalimage.jpg` indicates that the TCP/IP protocol used is HTTP, the domain name is `aconite.com`, the subdomain is `dub.aconite.com`, the host in that subdomain is `www.dub.aconite.com`, the port is 8080, the file hierarchy is `/mainfolder/subfolder`, the filename is `illegal_image.jpg` and the image type is JPEG. The objective of the filtering system is to block this specific file while it does not block a file with the url of `http://www.dub.aconite.com:8080/mainfolder/subfolder/legal_image.jpg`.

The technical system designed to implement this type of blocking is complex. Each individual URL is first divided into two parts. First the domain and IP address are identified and are installed in a DNS / routing system which diverts all requests destined for these domains to a dedicated URL reviewing system. This method minimizes the impact of the blocking system on unblocked content. The reviewing system performs a detailed comparison on the complete URL. (BT, 2017; Clayton, 2006) If the URL matches the specified URL then the URL is redirected to a notification page (for transparency reasons) or a http 404 error is returned to the client. Other URL requests on those domains are allowed to progress unimpeded.

- Keywords

A range of keywords are identified which relate to illegal content. This enables the creation of a variety of taxonomies for different illegal categories. Such taxonomies are most often used by search engines but can also relate to file names on p2p networks or on public websites. They are used to identify accesses to illegal content and when there is a positive hit on a file or a search for an illegal category, the search engine response will not return links to that content or the file will not be returned to the requesting client.

- File Signatures/ File Fingerprint/Hash Code

It is possible to create specific file signatures (also referred to as file fingerprints and hash codes) which uniquely identify a single targeted file. For example a text file called "white-list.txt" can have an MD5 hash which looks like: `d41d8cd98f00b204e9800998ecf8427e`. If a single character is changed in the contents of the file the md5 hash code will also change to a different string

such as b39bfc0e26a30024c76e4dcb8a1eae87. A list of hash codes are generated against known illegal content (usually child abuse images). Organizations can generate a hash code for each document and file stored, uploaded or downloaded from their systems and without knowing the content can compare the generated hash with a list of known illegal content. When a match is achieved the organization can chose to block the content or report the incident to relevant stage agencies.

Although, it is possible to identify illegal images if they are exact copies of known illegal image files, the images are not detected if they changed even slightly (including a single pixel change). In 2009, Microsoft partnered with Dartmouth College to develop PhotoDNA software tools (Microsoft, 2015). PhotoDNA works by converting images into a grayscale format, creating a grid and assigning a numerical value to image sub-section. Those numerical values represent the “hash” of an image, or its “PhotoDNA signature.” This hash is computed such that it is resistant to alterations in the image, including resizing and minor color alterations

- Dynamic - Image Analysis

A problem with all previous blocking systems is that they only work with previously identified illegal documents and images. New files/images will not be detected and cannot be blocked by the blocking system. Dynamic analysis uses technologies to analyze unknown files and to automatically predict the content of the file using heuristics and complex image analysis. This technology is evolving but exhibits low accuracy and is not in widespread use.

It is clear that the participation of industry is critical and the role of modern mobile devices is a special area of internet. Industry responsibility, the impact of modern, commercially-traded malware and the effect of mobile platforms on these systems require supporting research and investigation. In addition, practical experiences and lessons learned from the Arab Spring demonstrations and protests provide invaluable insight into the strategies of state directed oppression of Internet and mobile communications systems.

Table 2.2: The place of blocking and circumvention tools effectiveness.

Medium	Blocking	Effectiveness				Blocklist		DPI
		OVER-blocking	UNDER-blocking	Resources required	Circumvention	Maintenance effort	Identifier	
Web	DNS	VERY LIKELY	LIKELY	LOW	EASY	MEDIUM	Domain name	-
	Domain	VERY LIKELY	LIKELY	MEDIUM	MEDIUM	MEDIUM	IP address to domain name	-
	URL	LESS LIKELY	VERY LIKELY	MEDIUM	MEDIUM	HIGH	URL	+
	IP	VERY LIKELY	LIKELY	LOW	MEDIUM	MEDIUM	IP address	-
	Dynamic	VERY LIKELY	VERY LIKELY	HIGH	MEDIUM	LOW	Keywords, graphics recognition technology or other	+
	Signatures	LESS LIKELY	VERY LIKELY	HIGH	MEDIUM	HIGH	Hash	+
	Hybrid (IP+signature/URL)	LESS LIKELY	VERY LIKELY	MEDIUM	MEDIUM	HIGH	IP and Hash or URL	+
Email	Dynamic	LIKELY	LIKELY	MEDIUM	HARDER	LOW	Keywords or other	-
	URL	LIKELY	LIKELY	MEDIUM	HARDER	HIGH	URL	-
	IP address	VERY LIKELY	LIKELY	MEDIUM	HARDER	HIGH	IP address	-
	Signatures	LESS LIKELY	LIKELY	HIGH	HARDER	HIGH	Hash	+
Usenet	Per Group	LIKELY	LIKELY	LOW	EASY	LOW	Group name	-
	Per hierarchy	VERY LIKELY	LESS LIKELY	LOW	EASY	LOW	Group hierarchy	-
Search	Keyword	VERY LIKELY	VERY LIKELY	HIGH	EASY	MEDIUM	Keywords	-
P2P	Per protocol	VERY LIKELY	LESS LIKELY	MEDIUM	HARDER	LOW	Protocol recognition	+
	Per file (signature)	LESS LIKELY	VERY LIKELY	HIGH	HARDER	HIGH	Hash	+
	Per file (dynamic)	LIKELY	VERY LIKELY	VERY HIGH	HARDER	LOW	Advanced algorithms	+

Abbreviations used in Table 2.2.

DNS: Fully specified domain name in Domain Name System Blocking

Domain: Second Level domain name only

IP: Internet Protocol Address blocking usually IP version 4 but can include IP version 6

URL: Fully specified Universal Resource Locator

Signatures MD5, SHA1 or other hash of file contents which precisely define a specific file irrespective of location

Hybrid: Combination of several techniques indicate above

P2P Peer-to-peer protocol

Dynamic: Refers to analysis of target content when requested using advanced algorithms to decide estimated nature of content.

2.8 Circumvention Technologies

In April 2011, Freedom House published a review of censorship circumvention tools (Callanan, Dries-Ziekenheiner, Escudero-Pascual, & Guerra, 2011) to help Internet users in selected Internet-restricted environments assess a range of circumvention tools and choose the tools that are best suited to their needs. The product review determined how well different tools work in circumventing Internet filters and assesses each of the tools through surveys in the selected countries of Azerbaijan, Burma, China, and Iran. Technologies with the potential to open up access to government blocking and promote transparency can be hijacked by governments to crush dissent and deny human rights¹⁹. Such actions contravene the Universal Declaration on Human Rights, which tells us that all people have the right “*to seek, receive and impart information and ideas through any media and regardless of frontiers.*” (United Nations Humans Rights Council, 2011; Kravets, 2011).

Callanan et al.²⁰ focused in their study on computer based solutions to circumvent state-level network filtering. Eleven tools were evaluated, including VPN tunnels and proxy servers. Results of the evaluation provided information how each of the tools performed from all the tests and surveys. The Gpass, Psiphon, ToR, and the generic VPN category tools displayed very good results from the technical testing of security. When attempting to access blocked web text content Google products (Google Reader, Google Translate, and Google Cache), UltraSurf (UltraReach Internet Corp, 2012) and Your Freedom were used widely. However, in 2011 the Berkman Center (Gasser, Heacock Jones, Faris, Roberts, & Zuckerman, 2011) confirmed that only a small number of bloggers residing in the Middle East and North Africa understood or implemented best practices related to online security. Design and ease-of-use, rather than security-related features were considered to be the most important features in choosing safe online platforms.

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, Goertz, Kunz, Muller, & Nitzsche, 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, Thomas, & Tchouakeu, 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.

Circumventing network based blocking is achieved using methods including bypassing DNS-based blocking, using proxy technology/decoy routing and virtual private networks. Circumvention activities often involve implementation of several simultaneous methods in order to ensure robustness, reliability, confidentiality and privacy.

DNS blocking can be bypassed using two methods. Firstly, if the IP address of the remote server is already known the user can simply access that IP address directly without using a domain name. Secondly, if the IP address is unknown or changing regularly, the user can reconfigure the client network connection to submit DNS requests

¹⁹ Hillary Rodham Clinton, US Secretary of State, The Newseum, Washington, DC, January 21, 2010. Available at <http://www.state.gov/secretary/rm/2010/01/135519.htm> .

²⁰ Ibid.

to a DNS server which does not implement the blocking regime. Often the DNS servers operated by Google are publicly available using IP address 8.8.8.8 and 8.8.4.4. It is also possible to use any of the many free DNS servers on the global internet. The proper functioning of the internet needs reliable DNS servers to operate and is a protocol which is rarely blocked at the router level. If the IP address of a remote content hosting server or DNS server is blocked in local routers then it will be necessary to use a different form of circumvention such as VPN or proxy technology

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 by creating an encrypted channel between the user and the server. Although encryption is commonly used as a part of this technique, encryption is not always enabled by default. This circumvention strategy 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 unusual handset application functionality. 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. 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, Gringoli, & Salgarelli, 2008) Corporate VPNs, Freegate, Ultrasurf, and Guardster (Dynamic Internet Technology, 2016; Guardster, 2012). Since the proxy computers are easily discovered and blocked, some proxy services deliberately randomly change the Internet Protocol (IP) address used by their computers through a range of 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, Mathewson, & Syverson, 2004), Global Pass and other tools enabling user device anonymization. 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., 2011). For the operation of the latter, 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. (Burnett, Feamster, & Vempala, 2010) Some examples of the covert channels include TCP-over-DNS (AnalogBit, 2012), Infranet (Feamster, Balazinska, Harfst, Balakrishnan, & Karger, 2002) (Feamster, Balazinska, Wang, Balakrishnan, & Karger, 2003) and CovertFS (Baliga, Killian, & Iftode, 2007).

Callanan et al, (Callanan, Dries-Ziekenheiner, Escudero-Pascual, & Guerra, 2011) recommended that users should carefully plan their internet access profiles according to their internet usage and risks assessment and the capabilities and the nature of the regime they live under. Users need to be aware of other aspects of computer and network security to protect their activities online since circumvention tools are not all tools that are adequately designed or coded with appropriate privacy and security in mind. Safety and security needs to be a way of life for activists.

2.9 Security Risk Mitigation Issues for BYOD

Companies are more likely to recruit and to retain high-skilled employees if they support and embrace IT strategies which encourage and support the use state-of-the-art consumer focused technologies. (Thielens, 2013) This can be promoted and accelerated through the adoption of a wide-ranging, effective long-term BYOD strategy to manage the cyber-risks resulting from personal devices owned by employees used as part of their work activities. BYOD has become the principal means of accessing company databases (arsTechnica UK, 2015) and not just a supplementary method to remotely access company computer networks. As a result relevant corporate IT policies need to be rewritten since the scale of impact of consumer-focused technology on corporate IT is significant. Such policies include risk evaluation and risk mitigation using encryption. There is a need to educate and support a culture of security and responsibility, providing mobile device training and adopting rules to prevent or discourage device ‘rooting’.

There are tools available for use in BYOD environments which validate, remotely manage and enhance the security of the employee’s physical mobile devices. They support organisations to configure mobile devices and manage profiles for each device permitted to access the network. This responsibility can create a significant workload for cyber-security specialists since there is frequent churn in the type, functionality and applications of personal mobile devices on the corporate network. Tools such as HP’s Touchpoint Manager (HP, 2015), IBM MaaS (IBM, 2016), MobileIron (MobileIron, 2017) and VMware Airwatch (VMware, 2017) empower companies to provision and protect mobile data access using encryption and device management.

As a result of the increasing number of mobile device models, platforms and operating system versions available, Mobile Content Management (MCM) solutions focus on the content data itself and securing the data wherever it is located in the organization. Related IT trends including cloud storage, the pervasive adaption of browser based file sharing applications and SaaS solutions have further encouraged this transition. In the MCM paradigm, company data is provided to mobile devices through precisely designed corporate API interfaces. The mobile applications installed on employee mobile devices using these API interfaces reduce or prevent on-device data storage and provide encryption on the data which is stored and offer access controls. If the mobile device is lost or the employee stops working for the organization then access for related devices is disabled (Thielens, 2013; Morrow, 2012; Romer, 2014). As a result of MCM, IT access controls are focused on the effectiveness of the API interfaces when accessing corporate data. This methodology offers more possibilities for employees to choose their favorite device and their ideal software solution (Van Leeuwen, 2014). The methodology reflects state-of-the-art in cyber-risk mitigation and IT governance standards relating to data controls and security. To develop the API’s the organisation must first define which data elements are stored, describe the data schema, the semantic links between data elements and then determine what data access mechanisms are approved.

Another significant motivation for the implementation of remote mobile access to commercial IT systems is the demand generated by consumers wanting to have 24x7 access to their online data records at any time from any location – this includes airline and hotel reservation systems, online financial transactions, bank accounts, online marketplaces and social network providers including Facebook and Twitter.

G-Data reports that over 440,000 new Android malware streams were detected in the Q1 of 2015 and that mobile malware is increasing exponentially. In 2014, over 1.5 million new malware infections were identified (G-Data, 2015). In 2016, McAfee reported (McAfee, 2016, p. 10) that they detected over 1.5 million unique mobile malware samples collected by McAfee Labs - 24% increase from Q3 2015. McAfee determined (McAfee, 2016, p. 8) that there are over 120 million apps over multiple app stores around the globe with 9 million pieces of malware were identified, 9 million apps with suspicious behavior (but not malware) were identified and 1million apps with a bad trust score (apps known to share your info with 3rd parties, etc.)

A company Chief Security Officer (CSO) is responsible for the security strategy on corporate information assets. Today they have the ability to segregate data access requirements based on the level of user authorization, the type of remote mobile device, the geo-location of the user or the device and depending on the time of day or day of the week. Security is enhanced by implementing comprehensive audits of collected mobile-devices records and network logs which are constantly scrutinised to identify and prevent network intrusions. They also deploy anomaly detection systems to determine unauthorized access to corporate data (Morrow, 2012).

Chapter 3

Mobile Devices Assessment

Kingpin and Mudge (Kingpin & Mudge, 2001) were among the first to discuss the lack of security in the Operating Systems (OS) of the early handheld mobile devices. Other researchers have since investigated a variety of vulnerable mobile devices, but their research was focused on the malware imported through downloaded applications (Mylonas, Meletiadiis, Mitrou, & Gritzalis, 2013; Grace, Zhou, Zhang, Zou, & Jiang, 2012; Zhou, Wang, Zhou, & Jiang, 2012). They did not focus on the privacy provision and user data protection. In this chapter the research focuses on the mobile device security assessment and findings are presented. The properties of the most frequently used smart phones in selected countries were investigated in order to find out, if this technology is available and can be used by interested users for their protection.

The technical testing was conducted in January 2012 and repeated in August 2012 to support the design of the study of the user communities in the surveyed countries. The testing was designed to provide base-line technical knowledge on the technical capabilities and weaknesses unique to each selected handset used by the selected user communities. There were seven steps in this process.

1. Select the handsets for each country from information provided by the global handset tracking websites (Section 3.1).
2. Review the operating systems in use on these mobile devices and identify their differentiating features and assess the available app stores (Section 3.2).
3. Design and implement a test environment where the applications and the handsets can be evaluated (Section 3.3).
4. Design the laboratory test criteria against which the applications would be assessed and assign these to the key categories of use (Section 3.4). The relevant applications which can provide risk mitigation for users were identified.
5. Design the laboratory technical tests to investigate and identify the key phases of interest in the lifetime of owning a handset and the varying risks identified (Section 3.5).
6. Implement the tests and record the results. Where possible, perform physical forensic access against the selected handsets to determine what digital artefacts are available to adversaries if they achieve direct hardware access (Section 3.6).
7. Discuss the results of the technical tests and identify conclusions (Section 3.7).

3.1 Device Selection

A mobile device is often a personal device which has been extensively specified and chosen by the owner or employer according to pre-determined requirements and functionalities. These requirements are based on available options offered by national mobile operators which include technical capacities, screen size & quality, storage capacity, telecommunications standards (3G, 4G, etc.) and the needs of the user's lifestyle. Mobile operators offer and combine packages (service plus device) in both pre-pay and post-pay environments which include a pre-determined volume of voice, text and data.

It was not feasible or reasonable to test all relevant handsets which were of interest. Mobile handsets are developed and released on a continuous development cycle and handsets variants are often released regionally across the world. The primary markets for the most advanced handsets are in high GNP/wealthy countries but these handsets were not widely adopted or available in all countries selected for the study. The final selection needed to be representative of the range of operating systems identified during the research phase and later confirmed during the expert survey and in-country user-surveys.

The statistics available from StatCounter (StatCounter, 2012) were available for the selected countries. The in-country surveys collected information on the handsets used by respondents to the survey. The basic technical configurations were selected to be more representative of the average citizens of the selected countries rather than high-end specifications with larger high-resolution screens or higher storage capacities.

Detailed examination of public source documentation on the popularity of different mobile handsets in the target countries yielded 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 following mobile devices were selected since they covered all the relevant smartphone categories and operating systems in use in the selected countries.

- The IOS Apple iPhone 4 (released in June 2010 and operating on IOS4)
- Nokia N8 (released in October 2010 and operating on Nokia Symbian^3)
- HTC Radar (released in October 2011 and operating Microsoft Windows Phone 7.5 Mango)
- HTC Desire (released in March 2010 and operating Android OS v2.1 Eclair & v2.2 Froyo)
- Blackberry Curve 9360 (released in August 2009 and operating Blackberry OS 5.0)

Only the Blackberry Curve did not have a GPS option. All the others offered A-GPS as an option.

The results of the Expert Survey were combined with a detailed examination of the public source documentation on the popularity of different mobile handsets in the target countries (StatCounter, 2012).

The following mobile devices were selected:

- Apple iPhone 4
- Nokia N8
- HTC Radar
- HTC Desire
- Blackberry Curve 9360

They covered all the relevant smartphone categories and operating systems in use in the selected countries.

Details and specifications on the selected mobile devices are listed below.

3.1.1 Apple iPhone 4

Features²¹	
Released:	June 2010
Screen Size:	3.5"
Screen Resolution:	640 x 960
Camera:	5MP
RAM:	512MB
Flash Memory:	8/16/32GB
WIFI	802.11b/g/n hotspot
Bluetooth:	V2.1 A2DP
GPS	A-GPS
Battery	1420mA Li-Ion
OS	iOS4



<http://www.ebay.com/itm/Apple-iPhone-4-8GB-WiFi-Verizon-Wireless-Black-Smartphone-/201211843829>

Figure 3.1: Apple iPhone 4.

²¹ http://www.gsmarena.com/apple_iphone_4-3275.php

3.1.2 Nokia N8

Features ²²	
Released:	October 2010
Screen Size:	3.5"
Screen Resolution:	360 x 640
Camera:	12MP
RAM:	256MB
Flash Memory:	16GB
WIFI	802.11 b/g/n
Bluetooth:	v3.0 A2DP
GPS:	A-GPS
Battery	1200mA Li-Ion
OS:	Nokia Symbian^3



<http://www.clickbd.com/bangladesh/653976-nokia-n8-fresh-condition-full-boxed-with-tv-cable.html>

Figure 3.2: Nokia N8.

3.1.3 HTC Radar

Features ²³	
Released:	October 2011
Screen Size:	3.8"
Screen Resolution:	480 x 800
Camera:	5MP
RAM:	512MB
Flash Memory:	8GB
WIFI	802.11 b/g/n, DLNA
Bluetooth:	V2.1 A2DP, EDR
GPS:	A-GPS
Battery	1520mA Li-Ion
OS:	Microsoft Windows Phone 7.5 Mango



<http://static.trustedreviews.com/94/000020ddd/eebe/HTC-Radar.jpg>

Figure 3.3: HTC Radar.

²² http://www.gsmarena.com/nokia_n8-3252.php

²³ http://www.gsmarena.com/htc_radar-4131.php

3.1.4 HTC Desire

Features ²⁴	
Released:	March 2010
Screen Size:	3.7"
Screen Resolution:	480 x 800
Camera:	5MP
RAM:	576MB
Flash Memory:	4GB microSD
WIFI	802.11 b/g, hotspot
Bluetooth:	V2.1 A2DP
GPS:	A-GPS
Battery	1400mA Li-Ion
OS:	Android OS v2.1 Eclair & v2.2 Froyo



<http://cdn2.gsmarena.com/vv/pics/htc/htc-desire-silver.jpg>

Figure 3.4: HTC Desire.

3.1.5 Blackberry Curve 8520

Features ²⁵	
Released:	August 2009
Screen Size:	2.46"
Screen Resolution:	320 x 240
Camera:	2MP
RAM:	256MB
Flash Memory:	32GB microSD
WIFI	802.11b/g
Bluetooth:	V2.0 A2DP
GPS:	No
Battery	1150 Li-Ion
OS:	Blackberry OS 5.0



<http://www.trustedreviews.com/BlackBerry-Curve-8520-photos>

Figure 3.5: Blackberry Curve 8520.

²⁴ http://www.gsmarena.com/htc_radar-4131.php

²⁵ http://www.gsmarena.com/htc_radar-4131.php

The selected devices were identified and then purchased from an online distributor based in the Netherlands. These devices can be purchased by any traveller through major international transport hubs in Europe. The devices were purchased as SIM-unlocked and purchased in a democratic country where it was not expected any device tampering would occur. SIM-unlocked refers to mobile devices which will operate with different mobile operators and difference SIM configurations. It is important to note that mobile handsets which are purchased in one of the selected countries is likely to be SIM-locked to a specifically regulated and licensed mobile operator in that country. In that situation it could be pre-altered to match specifications mandated by the target country or the specific operator.

3.2 Mobile Operating Systems

3.2.1 Google Android

Android is an operating system developed by Google based on the Linux kernel, employs a virtual machine layer to run an operating system called the Dalvik Virtual Machine. Android users depend on their network provider, as well as the hardware manufacturer, for updates to the phone's core operating system. The Google application store is called Google Play and is universally installed on Android phones. Applications installed through Google Play can be revoked and uninstalled from a central location. Applications deployed on the Android Market have to be digitally signed, but there is no requirement that the code be signed by a third (trusted) party.

To create a more secure environment, applications have limited access to other installed applications, to the core OS and to other phone components such as contact or location data. Applications are executed with their own username (ensuring they can only access a limited part of the phone's file system) they are also restricted in communicating with other applications or other mobile phone components by the security design of the OS. In order to achieve "inter component" communication the applications need to negotiate access through a variety of APIs. At install time applications need to make their intentions known through a so called manifest file. This contains the permissions the application requests from the OS. The user can then decide if they are willing to trust the application with these resources. Only when a matching entry is found for the specific component can the Application succeed in its intent of contacting that specific resource. In other cases the operating system should disallow the communication. Google refers to this as the Application Sandbox and Permissions model.

To bypass certain security features of Android OS (and the phone hardware) the user sometimes needs to gain "root" access, (called "rooting") and this allows the user to install applications that access the phone's functionality that is normally only available to the core operating system and unavailable through APIs.

Android displays some of the highest scores in the security test analysis. As a clear test winner, the Orbot application (The ToR Project, 2012) offered best-of-breed censorship circumvention and anonymization options for the mobile users – meaning good privacy provision. Android is otherwise a platform where much development work is still taking place (SELinux Project, 2013). A number of tested applications stem from the Guardian Project (Guardian Project, 2012), which may indicate an early success on their part in meeting development goals for securing the use of this OS by average user. Unfortunately, these applications have no equivalent in other operating systems, restricting users to use less secure general-purpose circumvention applications, or to use

other means to secure their communications. These findings are presented in detail in Section 3.4

3.2.2 Apple iOS

iOS is the operating system that drives Apple's iPhone, iPad, iPod touch, and Apple TV products. The version released in June 2012 was iOS 5.1.1 and it is not uncommon for Apple users to maintain older iOS versions on their devices for long periods of time. Permissions management for iOS is less focused around the installation process (as in Android). Permission for access to certain resources is specifically requested from the user where sensitive data is involved, such as access to location data services or a user's contact list. iOS 5 implemented file system encryption by default, and manages the keys required to unlock files on the device in different key chains. The risk of someone accessing these protected files while the OS is running but locked is mitigated to some extent by unlocking these keychains only when needed for the functioning of certain apps.

Applications can only be downloaded from the Apple App Stores and in the Apple App Store are tested by Apple and only accepted under strict conditions. There is a requirement that a developer submit his/her photo ID before being permitted to submit apps. However, the BootROM of most iOS versions can be hacked, enabling customizations and replacement of the core operating system that would otherwise be impossible. This is known as "Jail-breaking" and is, in effect similar to "rooting" the phone as is done on Android devices.

IOS displayed approximately the same characteristics as Android, with the exception that most of the tools tested were either OS-based or made by independent developers. Although the overall structure is reliable, VPN technology leads to problems and may not provide any protection without the user realizing. The use of OpenVPN requires "rooting" of the phone which poses an additional security risk. (Rooting is a process where the user installs a different version of the OS which allows them to have total administrative access to the OS environment.) However, the generally positive outlook is not a confirmation of the overall level of user safety. This will depend on the user's behaviour and knowledge as it does on the platform.

3.2.3 Nokia Symbian

Symbian was a mobile OS series developed by Nokia which is based on an operating systems (the EPOC series) developed by Psion and it has existed longer than both Android and iOS. Symbian was most popular OS for Nokia smartphones before they were bought by Microsoft, and was still the most widely distributed smartphone OS in many of the markets studied in this research. Symbian's base operating system operates in a less protected environment as compared to Apple or Android, which means that it is more susceptible to attack by mobile viruses. The Symbian design is known for efficient memory and resource usage which makes Symbian a reference operating system in terms of multitasking capability (the capacity to simultaneously run several applications in real time while sharing system resources). This functionality also had difficulties in early version of Android and iOS.

The base OS of Symbian executes in a slightly less protected environment as compared to Apple and Android, making it more susceptible to attack by mobile viruses. Some of the first mobile viruses had broad distribution emanated from this platform. An example is Cabir (F-Secure, 2004) which was released in 2004 and simply displayed the text "Cabir" on startup but was otherwise deemed harmless. It does have separate storage permissions per application but lacks a dedicated virtual machine for the OS. It

was the first smartphone OS to be successful at multitasking, and had seen significant development over the years – so many different versions were marketed.

In comparison to other smartphone OS's, it is common for Symbian applications to be distributed outside of the manufacturer's marketplace (the "OVI" store). Applications are often installed from external sources using specific install files (SIS files for Symbian). Symbian does have code-signing requirements, and manufacturer-signed code is a requirement for access to certain capabilities. However, most permissions can be granted by the user during the software installation process. Nokia currently signs most Symbian apps at no cost. Development can be done in several languages.

Although a very popular operating system in countries with a medium-to-low national income, Symbian has a severe lack of circumvention options for its users. With only one, user-unfriendly, VPN system, only Skype and SIP provided a safe voice or text messaging service. There was currently significant scope for improvement of the circumvention tools for this platform.

3.2.4 RIM Blackberry

BlackBerry (Research in Motion (RIM), 2012) is the operating system for all RIM BlackBerry devices which was designed and developed with (corporate) security in mind. Large corporations initially adopted the technology but Blackberry was later the preferred platform for text-based communication for non-business users. RIM promoted the concept of secure communication between its services network and the BlackBerry hardware.

In order to achieve better security for data communications over the relatively insecure data channels of the mobile network, RIM promoted the concept of secured communications between its services network and the Blackberry hardware. For email and calendar sync (the most predominant apps in the Blackberry spectrum) RIM provided a push mechanism through which messages can get delivered to a Blackberry device upon delivery to the (provider or corporation based) Blackberry/RIM server. The option for non-corporate Blackberry users was called BIS or Blackberry Internet Service. The corporate "Blackberry Enterprise Server" integrates similar technology into corporate networks).

RIM Blackberry provides many security features, and uses a strong public-key encryption as the basis for its security design. However, the business model of the BIS and BES services creates significant shortcomings in these models for users of BlackBerry technology. In many cases BlackBerry still possesses the keys required to decrypt text messages (such as BlackBerry Messenger messages using the global key) and hence does not provide similar protection to its BIS users. For this reason various alternatives to the standard BlackBerry applications were tested.

Users of Blackberry devices in many countries are allowed to use the BIS service on the condition that the email server they connect to resides inside the user's country, thereby enabling local physical access to the data, subject to national legal access rules. So whilst intra-Blackberry-service-traffic may be secured and the device is generally well encrypted, security is only achieved if it is implemented end-to end.

Blackberry uses code signing and various other security features to secure its mobile operating system. In comparison to Android and Apple it is not easy, nor common, to "jail-break" or "root" Blackberry devices. They implement encryption both for data in transit (the Blackberry internet service) and on the device (file system encryption is used when the device is locked). Applications can be developed in multiple programming languages.

No alternative circumvention methods were found, with the exception of those built into the VPN, which can only be set up through the BES service. This is not likely to be available to non-business Blackberry users, so it was excluded from the test. The Opera mini browser is the only viable tool in that category.

3.2.5 Microsoft Windows Phone

Microsoft Windows Phone was the successor to Microsoft's Windows Mobile series of mobile phone and PDA operating systems. Today, these are now sold on the common platform called Microsoft Windows. The Windows Phone OS uses the concept of sandboxed application execution which means that Windows Phone Applications have to use a strictly defined and restrictive API and do not have direct access to the data of other applications, nor to most core phone functions - such as location services or address book entries. Windows Phone uses code signing and is strictly limiting app distribution to the Windows Phone Marketplace. Applications can be developed using the Microsoft .NET platform. A key design feature introduced in Windows phone 7 was real time information displayed in tiles on the start screen. This interface (known as the Metro interface) was later introduced in Desktop Windows 8.

With no circumvention options and limited support for secure voice applications, Windows phone was by far the least secure choice from the five major mobile operating systems. The only mitigating factor may be that sale volumes of Windows phone in the studied countries was extremely low.

3.3 Laboratory Test Environment

The test platform was set up as a wireless networking environment to test the traffic on the network and not the mobile network itself which is available only to licensed regulated mobile network providers. It was assumed that the device architecture was designed along the lines of the OSI network model where the behaviour of the OS and the application would be similar and equally relevant regardless of the network transmission medium.

The smartphones were tested in a specially created testing environment following an established research method (Mirkovic, et al., 2010). The testing environment consisted of a Wi-Fi router (with controlled access to a DNS) and a 3G connection to a UMTS-capable mobile network. A monitoring port on the switch connecting the Wi-Fi router was used to capture the traffic to and from the mobile device to allow further analysis. For this purpose, the TCPDump application (TCPDump & LibPCap, 2012) was used on a computer with an installation of Ubuntu OS. Packet-capture files were then analyzed in Wireshark (Wireshark Foundation, 2012).

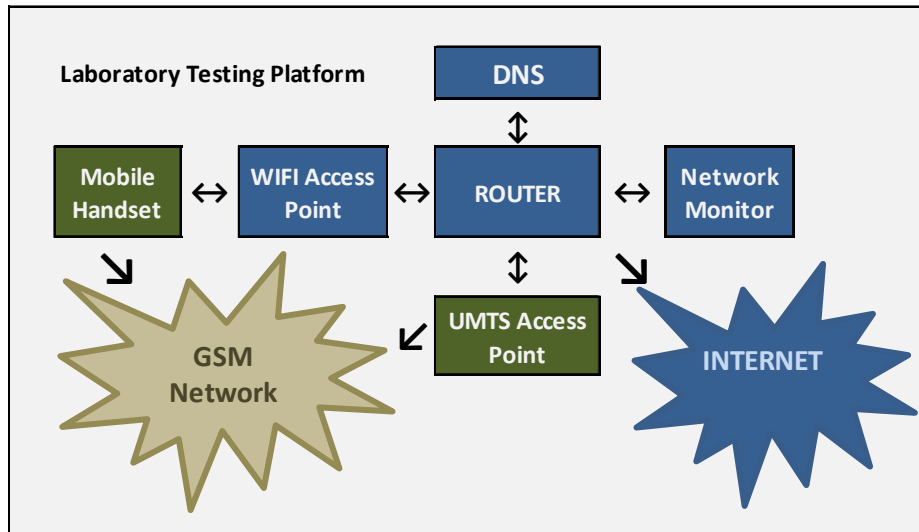


Figure 3.6: Diagram of Laboratory Test Platform.

Since an encrypted VPN (Virtual Private Network) is a key strategy to evade traffic monitoring and content blocking imposed at the state level, a highly configurable VPN service was managed on a dedicated server running Linux OS called CENTOS (Membrey, Verhoeven, Angenendt, de Bruijn, & Singh, 2009) on a different network. To determine the most effective VPN application, a selection of applications was tested for the provision of the VPN services, including the OpenSwan IPSEC router offering the IP protocol with security/encryption for IP packets (Wouters & Bantoft, 2006; Openswan, 2012), the Poptop application (Ramsay, 2000; Bauer, 2005; Howarth, Cameron, & Gillham, 2012) enabling secure point-to-point connectivity (PPTP), Xl2tpd (OpenWrt, 2012), and the OpenVPN application (OpenVPN Technologies, 2012; Feilner, 2006) for the VPN service.

DNS servers were provided locally by DHCP (Alexander & Droms, 1997; Internet Systems Consortium, 2012) using dnsmasq software (Kelley, 2008). The VPN server had separate DNS servers not used by the test clients. In some test scenarios a firewall was introduced into the local network in order to enable the blocking of specific IP addresses or for blocking DNS queries.

To determine the offline risks associated with data stored (disclosure of call records, location records, messages, etc.) on the smartphone, which could be extracted by people with direct physical access to the phone, the selected devices were tested with the Cellebrite mobile-forensics solution known as UFED (National Criminal Justice Reference Service (NCJRS), 2012) and the Oxygen mobile-handset forensic suite (Hone & Creutzburg, 2011). The combined hardware and software forensics solutions were used for the extraction of the file images from the mobile phone.

3.4 Laboratory Test Criteria and Assessment

The technical assessment was performed in a controlled laboratory test environment in order to identify the unique risks associated with user-traffic monitoring and device-tracking of the most common mobile handsets used in the selected countries.

The technical capacities of the selected devices to implement circumvention technologies and to avoid content blocking were explored. The devices and mobile operating systems which were in widespread use were identified. The applications/tools

for each particular operating system under study were assessed in three primary groups: general aspects, security capabilities and usability.

In addition, certain properties of these devices were studied; 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 (anonymization 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.

In terms of possible security measures provided by the manufacturer of the device, generic measures were identified, which are expected to be in place in the mobile device. The applications selected in the research all provided a form of security by design, mainly a basic circumvention capability.

Therefore, applications with no security mechanism (or only weak security) were not tested since the outcome was easy to predict. For example, some services were deliberately omitted from the research as they were known to be susceptible to relatively simple man-in-the-middle attacks (Serpanos & Lipton, 2001) on the SSL/TLS handshake protocols.

As regards the secure tunneling of IP packets, the VPN connections were considered to be software applications enhanced through the use of a foreign proxy. Using this technique a user can request access to a foreign proxy Internet server. As long as that foreign proxy is not being blocked itself, the user can gain access to the content and bypass the local filtering.

The testing criteria were selected for each application/service installed on the smartphone and each one of the parameters defining the criteria was rated in the three primary categories using several sub-categories which shared common characteristics:

- Security (OS requires rooting to ensure security, Application requires “permissions” to be installed, Anonymity for preventing tracking, Cryptography on the connection link, Cryptography on the stored data, (Table 3.1)
- Resilience to blocking including plausible deniability, system fingerprints (Table 3.2)
- Usability including Ease of Installation, Documentation, Languages Supported (Table 3.3)

The applications were scored on several dimensions.

Table 3.1: Security Criteria for App Scoring.

Security							
Score	Requires Rooting	App “permissions” granularity	Anonymity	Prevents tracking	Secure Apps supported	Crypto - on the wire	Crypto - storage
1	Full Root	Full Set	It is easy to Retrieve and Disclose the User ID	No Facility to Prevent Common Tracking Technology	Apps are Individually Secured but there is Only One App	Plain Text	None
2	Full Root with Logging	Narrow Range of Permissions	It is possible to Retrieve the User ID but this is Logged	Tracking Attempts are Logged	Apps are Individually Secured but There are only Two Apps	Low Security Crypto	Low Security Crypto
3	Intermediate Forms (e.g. Limited Root)	Works with Limited Permissions	Some Measures Protect Users Identity	Some Features Blocking Tracking	Apps are Individually Supported but there are over 3 Apps Supported Directly	Some Unlisted Crypto Used	Unlisted Type, Not Reviewed
4	Limited Root with Logging	Wider Range of Permissions	User ID Not Accessible	False answers possible	Apps are Individually Supported but there are a Wide Range of Apps Supported	High Level Crypto Available	High Level Crypto
5	Runs as/on Stock OS	Very Proportional Permissions	Full Anonymity	Advanced blocking of tracking (cookies)	All Apps are Secured by Protecting all Network Traffic	Peer Reviewed Crypto Available	Listed, Peer Reviewed Strong Crypto

Table 3.2: Resilience Criteria for App Scoring.

Resilience Criteria					
Score	Resilience to blocking	Plausible deniability	System fingerprints	Carrier loss (turn wifi off, other carrier present)	Carrier change (forced on wifi router)
1	Single IP or DNS Name: SPOF	Not Present	Many	Loses Connection, No Warning	Loses Connection, No Warning
2	Small Number of IP Addresses or Domain Names	Possible Through App Deletion	<2 Identified	Attempts to Switch to Alternative Carrier Without Confirmation	Attempts to Switch to Alternative Carrier Without Confirmation
3	Independent of DNS	Can be Achieved - Not Easy	<3 Identified	Crashes With Warning	Connection Crashes Without Warning
4	Using range of Network Sockets	Manual Delete Records on Request	<4 Identified	Leaks IP on Switch/ Limited Warning	Loses Connection with Warning but Leaks IP on Normal Internet
5	Independent of Single IP and DNS	Easy	None Identified	Stops and Shuts Down Network Traffic	Connection Survives forced WIFI change

Table 3.3: Usability Criteria for App Scoring.

Usability					
Score	Installation	Gui	Documentation	Language Support	Speed
1	Difficult (Needs Skills)	Not present	None	1 Language	Extraordinarily Slow
2	Basic Technical Skills	Basic Interface	Basic	>3	Ok for Text
3	Some Manual Steps	Rudimentary	Some provided - not Comprehensive	>5	Surfing & Text
4	Non-Technical Skills	Available but Not Intuitive	Comprehensive but Needs Improvement	>8	Video, Surfing Text
5	All Automated	Easy to Understand	Excellent	>10	Voice, Video, Surfing, Text

Circumvention applications were tested against a video service (to test high bandwidth transfers), a voice service (common usage) and website access (basic

requirement) in order to measure the speed of operation, with a view to audio-visual content and real-time content delivery.

A specific selection criterion for the set of applications tested was the requirement that they function across many smartphone platforms. Applications that work on only one platform often require users to employ other non-secure, services.

3.5 Device Evaluation Approaches

The key phases of owning a mobile smart device include buying a mobile device and operating the device for the first time, using the device during its effective lifetime and installing and using supplementary applications which run on top of the native operating system.

The mobile devices were evaluated in terms of the three possible threat scenarios during their use and the relevant security capabilities. These are as follows:

- The threats present in relation to direct physical access to the phone.
- The initial execution environment (which is present when, or straight after, purchasing the phone).
- The run-time environment (which are the threats when using the phone and installing applications).

3.5.1 Physical Access to Mobile Phones

Physical access to mobile phones is conceivably the most intrusive of all threats since by gaining physical access an attacker can extract the stored data and credentials. This is possible when the phone is captured in powered-on state (live forensics) and the stored data are not encrypted or the applied encryption is not based on strong encryption mechanisms (Mylonas, Meletiadiis, Mitrou, & Gritzalis, 2013). The possibility of extracting stored unencrypted live data was tested with several forensic tools listed at the end of Section 3.3. The handsets were connected to a forensics-laboratory retrieval system to determine what content could be retrieved from the handset.

3.5.2 Initial Execution Environment

The threats that appear during the initial execution environment of the smartphone are related to the execution of the installed software and downloaded applications.

During the phase of purchasing and taking possession of a mobile device, there are a number of risks which are important for the user to be aware of. The mobile device might be delivered with an operating system which has been tampered or altered which could enable abilities to track, record, store or report personal information about the activities of the owner. These type of manipulations are difficult to detect and counter since they require significant financial, and supply chain resources which are usually restricted to state-level actors. One possible solution is to re-install a trusted version of the operating system directly from the manufacturer. However, this requires significant technical knowledge and skills and is not always possible to re-install the operating system on the mobile device.

It would also be feasible to purchase a device which has not been modified for use in a specific country by purchasing such a mobile device outside the national market but such devices might not be approved for use by the national telecommunications regulator and can also be widely detected on the mobile network through the device IMEI (International Mobile Equipment Identity) number. The IMEI number is used by a mobile network to identify valid devices and therefore can be used for stopping a stolen

phone or unauthorised phone from accessing that network. It will most definitely be identified if a SIM card from a national operator is inserted into an imported device or an imported device is regularly using a foreign operator SIM. A phone using a foreign IMEI with a local IMSI (International Mobile Subscriber Identity) which identifies the user of the local cellular network and is a unique identification associated with all cellular networks would represent a person of interest. An imported mobile device using an imported SIM will still disclose location information and basic SIM details to a determined observer unless complex and consistent anti-surveillance techniques are used by the owner.

In addition, the mobile device might have programmable-hardware or SIM-modules which are difficult to detect and remove. The identified threats include programmable hardware, programmable SIM, rigged operating system (operating systems configured to support the interception or monitoring, which are installed before purchasing). Security measures preventing these threats include the secure-boot environment, the antivirus check and the OS and firmware scan.

The mobile device might be delivered to the end-user with pre-installed privacy-abusing applications installed. When smartphones were first available, some mobile operators installed applications which reported network quality information to the operator in order to improve the functioning of the mobile network. In some cases, the information collected from these applications was used to challenge customer complaints about network problems. Although it was previously possible to remove pre-installed applications, it is now possible to install applications which are invisible to the end user (except through the use of network traffic monitoring utilities) and cannot be deleted from the device. With regards to pre-installed, malicious software, it is known (Fleizach, Liljenstam, Johansson, Voelker, & Mehes, 2007) that this is difficult to detect since the software to check the handset needs to be installed on the platform that was initially infected. It would, therefore, be preferable to have an ability to scan the operating system using specialized applications, in order to check whether they are still in the original, manufactured condition.

When a mobile device is purchased in one of the selected countries the customer often needs to provide a wide range of personal details which are permanently linked to the hardware device which is purchased and the service purchased from the mobile operator. In some countries these details include their personal identification documents, their payment records (credit card, bank account, etc) their home and/or business address and sometimes even their finger print. Although these details can be reduced if a mobile device is imported, it could still be possible to identify payment records from financial records.

3.5.3 Run-Time Environment

Privacy threats are also present during the execution of applications (run-time environment). During the phase of using the mobile device the owner is subject to a number of specific threats and risks. The most widely known risk is that of monitoring which can be based on local targeted monitoring of a specific selected group of mobile devices. Monitoring can also be based on network monitoring and profiling the customer base for suspicious behaviour. This is achieved through big-data mining to identify individuals based on pre-determined risk indicators for additional intrusive monitoring. Similar strategies in financial intelligence units (FIU) to investigate potential fraud by detecting and investigating suspicious transactions reports (STR) or Currency Transaction Reports (CTR) which are used broadly in western democracies. These risks are based on the assumption that the mobile-network operator is not secure and that the

primary interest of the unsecure telecommunications-operators is in the real-time data generated during mobile-phone usage.

Detection and prevention of local network monitoring is difficult and requires the use of trusted hardware and further hardening of the device against manipulation or to force disclosure of such manipulations or monitoring. Network based profiling can be made more difficult through the use of circumvention tools (Callanan, Dries-Ziekenheiner, Escudero-Pascual, & Guerra, 2011) including voice and text encryption capabilities and safe browsing techniques. Some of these circumvention activities can be detected by the network operators even if the content of the activity cannot be detected and is still secure. The related traffic data can be detected and such detection would increase undesirable focus of attention on the owner of the mobile device.

Blocking access to content or to specific users is also a cause for concern which might be prevented through the use of circumvention software and international collaboration to bypass nationally-based content blocking systems. In addition to blocking & monitoring there remains the challenge of pre-installed applications which are difficult to detect, disable or circumvent. Many solutions to known risks rely on a trusted third service provider to disrupt, detect, disable and delete network based malicious activities and some of these trusted third parties might not be trustworthy, competent or reliable to provide services which will protect the end users from disclosure and risk.

In addition to only text and voice attacks, location data and other forms of online communication form the main target of many monitoring operations. The threats considered in the device testing in this area of use were: on-phone monitoring, data about third-party service suppliers, use of application repositories, data about permissions to upload applications and device ‘rooting’ – enabling administrator privileges at the operating-system level.

3.6 Evaluation Outcomes

As regards **direct physical access** to the mobile phone, in all cases it was possible to retrieve either a logical or a physical image of the mobile phone, with the exception of the HTC Radar device. This device was not (yet) well recognized in the studied countries possibly due to the recently released operating system it used (Windows Phone 7). The information that could be retrieved included text messages, the call history and information about contacts. Few applications encrypt the data stored and they relied on the system-wide encryption of backups to protect their data.

With regard to the **initial execution environment**, applications which scan the operating system, in order to check whether the operating files are still in the original manufactured condition were not found during the research. Therefore, it was not possible to detect if the operating system had been tampered or altered.

As regards the risks associated with the **run-time environment**, among the tested handsets, Apple was the only one (during the period of the testing) which did not make anti-malware software available in the Apple store. In terms of more granular access control, only the Linux-based Android OS contain more granular security enhancements available as an extension of the original OS. In particular, the applications developed in the NSA’s SELinux project (SELinux Project, 2013) have been ported to Android. This tool is only available as a reference implementation and was not analysed since it is not easy to install without specific technical knowledge about Android OS and is not available to users in the countries investigated in this study.

3.7 Results and Discussion

Anti-virus checks, code signing and enhanced security features (such as trusted path execution) are the most effective generic defences responding to attacks against mobile devices. Most of these are supported by all the studied operating systems. However, Apple handsets did not have any antivirus options in the App store or within the operating system itself.

The most important set of technical tests was designed to determine whether the circumvention tools for bypassing monitoring and content blocking are usable on the studied operating systems. The circumvention tools were divided into two categories, depending on the functionality they provide, e.g., whether they allow text or voice communications to be encrypted and transported through the use of “general circumvention tools” that simply reroute the entire Internet traffic of the device or the use of purpose-designed tools for specific types of circumvention. Most modern smartphones are capable of enabling the capture and rerouting of the smartphone traffic. For this to happen, two elements are required: one is an Internet service that is able to exchange traffic with a remote third-party service (i.e., it is not filtered or blocked), and the other is an overlay connection (e.g., a VPN) that is capable of carrying the actual data traffic that is being transported. Most of the tools which were tested created a VPN that relayed traffic to a location not visible to the monitoring organization. Although encryption is commonly used with VPN tunnels, it is not always enabled by default.

Each application was assessed for each operating system under the three categories of Security, Resilience and Usability and scored using the individual criteria listed in Table 3.1 for Security, Table 3.2 for Resilience, Table 3.3 for Usability. A comprehensive table was completed which listed the scores for application. An un-weighted average of several factors was used to create a score for the three groups of properties of the selected handsets. The exhaustive technical testing provided a deep insight into the capabilities of the five selected smartphones to provide reasonable security and privacy for their users. It can be seen from the table that using Skype for voice communication on Android scored 3 for security, 3 for resilience and 4 for usability. At the same time using WhatsApp for text communication on Windows scored 1 for security, 1 for resilience and 4 for usability. Orbot for circumvention use on both Android and IOS scored highly with a score of 4 for security, 4 for resilience and 4 for usability. The detailed list of findings is presented in Table 3.4.

Table 3.4: Analysis of application effectiveness on smartphone OS platforms Scoring between 1=Low; 5=High based on laboratory testing and subsequent scoring of range of selected features.

Sec= Security, Res = Resilience, Use=Usability ("-" = No App Available to test)

	OS =>	Android			IOS			Symbian			Blackberry			Windows		
	Tool Name	Sec	Res	Use	Sec	Res	Use	Sec	Res	Use	Sec	Res	Use	Sec	Res	Use
Voice	Skype	3	3	4	3	3	4	3	3	4	3	3	4	3	3	4
	Viber	2	3	4	2	3	4	-	-	-	-	-	-	-	-	-
	CsipSimple	3	2	4	-	-	-	-	-	-	-	-	-	-	-	-
	Acrobites	-	-	-	3	3	4	-	-	-	-	-	-	-	-	-
	Internal SIP	-	-	-	-	-	-	3	2	2	3	2	2	-	-	-
Text	Skype	3	4	4	3	3	4	3	3	4	3	3	4	3	4	4
	Viber	2	3	4	2	3	4	-	-	-	2	3	4	2	3	4
	Whatsapp	1	1	4	1	1	4	1	1	4	1	1	4	1	1	4
	TextSecure	4	3	3	4	3	3	-	-	-	-	-	-	-	-	-
Circumvention	OpenVPN Client	3	3	3	3	3	3	-	-	-	-	-	-	-	-	-
	FeatVPN	3	3	3	-	-	-	-	-	-	-	-	-	-	-	-
	PPTP native	2	2	3	2	2	3	-	-	-	-	-	-	-	-	-
	L2TP/IPSEC native	3	2	3	3	2	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	-	-	-

The results of the technical analysis enabled the identification of the areas where specific applications require further development, both in terms of type (voice, text or circumvention) and OS.

The assessment has shown that the overall basic security tools and data-protection facilities enable some level of privacy and are being implemented by the most prominent smartphone manufacturers. However, the assessment also found that additional capabilities, particularly for the circumvention of content blocking and monitoring, are not in place by default in the selected devices. They need to be downloaded as applications and tools and must be installed by the user, which requires some level of skill. The use of some of these tools is only possible when the underlying network infrastructure supports applications such as VPN or IPsec. This implies that the success in terms of privacy protection and the delivery of free content is very dependent on the level of user awareness and his or her skills for accessing and using the available tools. This also applies to the level of awareness required regarding the possibilities that offline data stored in the mobile phone can be accessed by others. In the cases when encryption is used, disclosure might only be possible using complex approaches to decryption.

These findings were applied in the design of the survey questionnaire targeting end-users. Two specific questions from the total of 23 (see Appendix A) directly address these concerns.

Chapter 4

User Communities Survey

The purpose of the user survey is to complement the knowledge gained from the comprehensive technical assessment presented in Chapter 3 on Mobile Devices Assessment with a deeper understanding of the mobile usage patterns and users' capabilities with respect to managing their privacy by collecting information directly from the user communities.

Managing the user surveys and collecting the data from the selected countries that relied on public sources was a very complex activity. Sometimes there was a need to ensure the safety of the people who were administering the surveys in each country, and this had higher priority than insisting on complete, detailed feedback and information about the day-to-day user experience when operating mobile handsets and networks.

When selecting the countries for this study, a selection of developing and emerging economies with substantial Internet content censorship initiatives were identified. Developing economies also have low GNI and underdeveloped telecommunications infrastructure. Emerging economies exhibit robust and continual economic expansion coupled with fast growth of new products and services to satisfy consumer demands. However, it should be noted that mobile communications services and their customers belong to an area with rapidly 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 & Dries-Ziekenheiner, 2012). Therefore, the situation in each selected country was carefully studied, and categorized each individually as a developing or emerging economy. Categorization was performed on the basis of:

- GNI
- the level of development of the telecommunications market
(This is reflected in the growth of new customers, new services, the availability of ICT, and the overwhelming success of mobile communications.)

A comparative evaluation of current human rights protection policies in the context defined by the UN Internet Report (United Nations Humans Rights Council, 2011; United States Government Accountability Office, 2013) and of countries' telecommunications market regulations, as well their consumer and workforce characteristics, led to the final selection of 10 countries: Azerbaijan, Belarus, China, Iran, Oman, Saudi Arabia, Syria, Tunisia, Uzbekistan, and Vietnam. Although Egypt and Libya were also selected, the data collected was not sufficient for data processing due to the serious political upheavals in 2012. In Syria, the data was collected just before the outburst of political upheavals. The user responses were collected in each country during late Spring 2012. The research study was designed and implemented from December 2011 to November 2012.

Despite the ongoing volatility in the regions being analysed, there were specific, major political upheavals and social unrest in several of the countries during the period of this study and especially in the Arab Republic of Egypt and the Socialist People's Libyan Arab Jamahiriya. Whereas it was possible to collect some information about the mobile markets in the Arab Republic of Egypt, it was not possible to collect adequate levels of data about the Socialist People's Libyan Arab Jamahiriya.

4.1 Questionnaire Design and Data Collection

The user community survey was carried out with help of in-country experts. The set of survey questions were available in the national language(s) and completed by the users in the selected countries.

The users were surveyed in order to assess their abilities to understand the mobile-related security threats they are exposed to and the security choices available to them in order to mitigate the identified threats and risks. This involved a 23-question survey.

More than 200 users were sought per country and this target was reached in most cases.

The group of selected national experts contributed additional findings based on their personal observations and local market research (Callanan & Dries-Ziekenheiner, 2012). Analysis of the expert survey results confirmed the existence of a range of state strategies for ensuring effective state control on mobile operators both in terms of which market participants are licensed and in terms of the business activities of those licensed market operators.

An Expert Survey was completed by a single individual for each country – a specifically identified and remunerated expert in each country and considered as the in-country expert in order to identify the scope and boundaries for the user survey. The purpose of the expert survey was to gain a description of the current mobile market based on local knowledge and language skills using a person with the ability to search relevant local-language websites, contact relevant sales offices and speak with other colleagues inside each country. The expert survey was designed to identify key operators and issues in each country, provide confirmation of the facts collected during the desk research and also provide a single in-country overview of likely results of the user survey.

If there were any disparities between the expert answers and the user survey, the user survey would supersede the answers provided by the selected experts but would also encourage further research and analysis. The survey questions are focused and technical and it was planned that the expert would be more knowledgeable on the range of technical issues which were addressed in the survey. The collected answers would provide additional background context for each country in order to develop the user survey and to understand and interpret the user survey responses.

The questionnaire was translated into national languages and was distributed by an in-country survey administrator. 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 answers were collected and entered into the survey tool. Once the online responses were collected, they were translated back into English. In each surveyed country, the local expert 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 consisted of $n = 1607$ respondents from ten countries: Azerbaijan ($n=97$), Belarus ($n=224$), China ($n=209$),

Iran (n=99), Oman (n=213), Saudi Arabia (n=154), Syria (n=227), Tunisia (n=202), Uzbekistan (n=83), Vietnam (n=99).

Respondents' identities were kept confidential. Survey participants were not misinformed about the true nature of the project since all country local experts received an introductory document outlining the research objectives. In most of the studied user communities, local experts 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 to 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 & Dries-Ziekenheiner, 2012).

The survey has some limitations. The data collected was not weighted to represent the general population, since the main objective of the 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 local experts were discreet when recruiting the study participants and operationalizing the survey instrument.

4.2 Community Profiles and the Mobile Markets

In most of the countries the user communities showed high levels of dependence on mobile communications, both voice and data. The fixed telecommunications infrastructure in most of the countries has received very low levels of investment and growth due to the overwhelming success of mobile technologies. For example, the Kingdom of Saudi Arabia is remarkable for having achieved nearly 200% penetration of mobile subscriptions in the mobile market, i.e., an average of two mobile subscriptions for every person in the country. The International Telecommunications Union ICT development-rating index for 2011 (ITU, 2012, p. 23) placed this country in fourth place among the 10 most dynamic countries.

In this context, information about the main market players, especially regarding their ownership, was considered to be relevant for the structural 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 whom are actively using mobile data services. In total, over 44 mobile operators were present; nine of them were 100% state-owned operators (the overall subscriber base for these operators was over 1.1 billion), and 35 had a mixed ownership structure. The survey data confirmed that the main focus of the mobile Internet users in these countries was on news and on other content mainly described as entertainment, relying on video content from sources such as YouTube and its national variants.

The country profiles including relevant data about the mobile market, operator ownership and the availability of mobile Internet are presented in Table 4.1 and Table 4.2 and presented in the text below. The statistics for Table 4.1 and Table 4.2 were sourced from different locations including ITU Measuring the Information Society (ITU, 2013), World Bank²⁶, UN World Statistics²⁷, from national statistics offices and annual reports from transnational and national mobile telecommunications operators.

²⁶ <https://data.worldbank.org/> (last accessed November 2017)

²⁷ <https://unstats.un.org/home/> (last accessed in November 2017)

Table 4.1: Mobile Market Size and market penetration (studied countries 2012)

Country (2012)	Mobile cellular subscriptions (millions)	Market Penetration (Percent)
Republic of Azerbaijan	9.1 m	99.0
Republic of Belarus	10.7 m	108.9
People's Republic of China	1,030.1 m	75.6
Arab Republic of Egypt	83.4 m	119.0
Islamic Republic of Iran (I.R.)	54.2 m	72.3
Libya	10.9 m	
Sultanate of Oman	4.9 m	177.6
Kingdom of Saudi Arabia	56.1 m	198.0
Syrian Arab Republic	11.9 m	57.7
Tunisian Republic	12.5 m	116.6
Republic of Uzbekistan	24.3 m	84.0
Socialist Republic of Vietnam	119.0 m	136.9

Table 4.2: Operator ownership type and Mobile internet market (2012).

Ownership (2012)	Number of Operators	Subscribers	Mobile Internet Subscribers
State	9	1,118.48 m	487.7 m
National	3	6.44 m	0.73 m
Foreign Owned	7	36.13 m	8.5 m
Combined Ownership	25	218.91 m	37.81 m
Total	44	1,379.95 m	534.74 m

4.2.1 Country Classification

The targeted countries were classified as developing or emerging economies on the basis of the GNI per capita data obtained from the World Bank Statistics (2012) listed in Table 4.3.

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 falls 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 level of mobile market development was determined on the basis of the mobile services penetration index, and affordability of the mobile broadband prices.

The countries were divided into two groups.

- Group 1 includes the Kingdom of Saudi Arabia, with a GNI of USD 30,160, the Sultanate of Oman with a GNI of USD 25,320, Belarus with a GNI of USD 14,950, Iran with a GNI of USD 12,895, Libya with a GNI of USD 11,936, Azerbaijan with a GNI of USD 10,365, Tunisia with a GNI of USD

9,650, and China with a GNI of USD 9,040, were categorized as a group of countries with high or moderate GNI and developed mobile markets.

The penetration index in these countries ranges from 99% in Azerbaijan to 198% in Saudi Arabia. Affordability of the mobile services (pre-paid and post-paid broadband mobile services) for this group ranges from 1.6 in Oman to 3.6 in China (ITU, 2013).

- Syria, with an estimated GNI of USD 5,100 (in 2011 before hostilities broke out), Uzbekistan with a GNI of USD 3,670, and Vietnam with a GNI of USD 3,620 formed the second group of countries. In this group, the mobile service penetration index ranged from 58% in Syria to 84% in Uzbekistan.

Table 4.3: GNI (Gross National Income) in the studied countries.

World Bank Statistics	Population	GNI (USD)
Republic of Azerbaijan	9.2m	10,365
Republic of Belarus	9.8m	14,950
People's Republic of China	1,351m	9,040
Arab Republic of Egypt		
Islamic Republic of Iran (I.R.)	75.0m	12,895
Libya	6.3m	11,936
Sultanate of Oman	2.9m	25,320
Kingdom of Saudi Arabia	28.4m	30,160
Syrian Arab Republic	20.5m	5,100 (2011) est
Tunisian Republic	10.7m	9,650
Republic of Uzbekistan	29.0m	3,670
Socialist Republic of Vietnam	87.1m	3,620

4.3 The Structure of the Questions

Many of the large operators are active in several countries and this provides a challenge to restrict the sale and use of dual-use technologies (e.g. networking monitoring systems which can be used in a positive way to ensure network efficiency and detect failures and can also be used in a negative way to monitor and profile specific users or devices). Due to a heavy reliance on mobile technologies, the need for access to an open and unfiltered Internet was found by the involved team of experts to be considered essential for all aspects of mobile Internet use.

Questions were formulated with the intention of collecting answers and data that would help build a structural model. The questionnaire consisted of 23 questions presented in Appendix A.

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), and 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 user downloads and mobile devices upgrades. This information is an indication of the user capability to download applications to protect privacy and enable security. This group of questions also addressed the issue of jail-broken phones (phones modified to allow users to install applications from other phone manufacturers' online 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 stakeholder categories were listed, and users had to choose from a Likert scale of Never-Trust=1 to Always-Trust=5 to describe how much they trust individual stakeholders.

Information sought in the survey included access to and use of a mobile service; operating system and device used; skills level accessing the internet via mobile applications; content sharing; and attitudes about privacy, content filtering and government monitoring on mobile networks.

4.4 The Studied Country Profiles

A very brief overview of the selected countries and the market share of known mobile telecommunications operators and other market characteristics follows:

4.4.1 Republic of Azerbaijan

With a population of more than 9 million the Republic of Azerbaijan is a mid-sized market for its three mobile networks. Mobile market penetration in Azerbaijan achieved 99%. The number of internet users exceeded 46% (4.2 million)²⁸.

In 2012, the Azerbaijani government introduced new regulations which require every mobile phone to be registered with the state communications authority.

All foreigners were also asked to register their phones and a non-registered phone did not have access to mobile services. With relatively high mobile and regular internet access availability, Azerbaijan was an opportune market for mobile internet privacy provision tools as limited use of circumvention technology is observed.

There were 3 active operators in the market with Android as the largest OS in use at 39% and 22% indicating that they don't know which OS they are using (Chart 4.1).

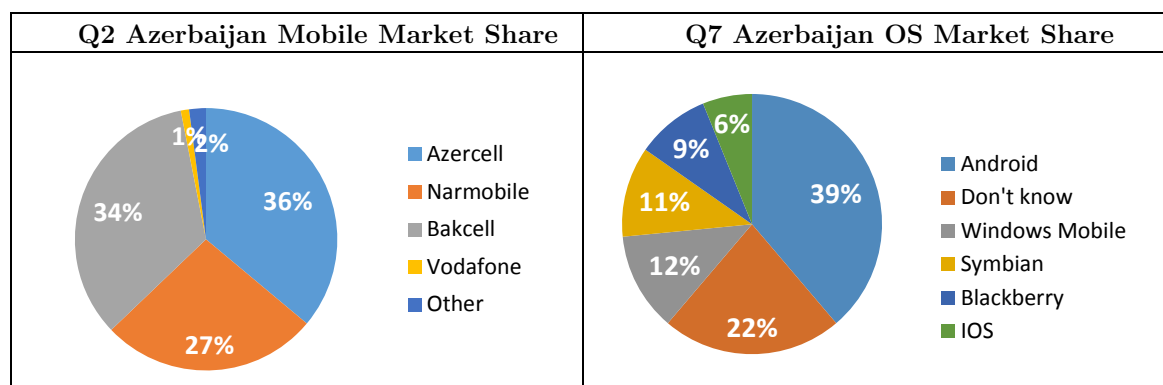


Chart 4.1: Market Indicators for Azerbaijan from user survey.

²⁸ <https://data.worldbank.org/> (last accessed May 2013)

4.4.2 Republic of Belarus

The Republic of Belarus²⁹ has a population of more than 9.5m³⁰ people and mobile penetration achieved 109% and internet penetration exceeded 47% in 2012 up from 29% in 2008.

There were 4 mobile operators in Belarus - **Velcom** with 4.5m subscribers offering voice/text/data and positioned as quality operator; **MTS Belarus** with 4.9m subscribers offering voice/text/data and positioned as fair-price operator; **Life** with 1.9m subscribers offering voice/text/data, entered the market later; **Belcel** (CDMA) with 0.2m subscribers focusing on data plans primarily, but also offering voice/text services and is positioned as a high-speed mobile internet provider rather than traditional mobile operator. One potential operator called **Yota** offered data only, using LTE standard.

From the user survey, 75% of respondents used mobile internet. Of these 20% used WIFI to access the internet with 47% paying for a limited volume of data with their subscription and a further 12% paying for usage. 16% indicated that they did not have access to the Internet from their mobile handset.

There were 2 active operators in the market with over 38% unaware of which OS they were using and 29% using Android. Of particular interest was the number of users who avail of services of multiple operators (Chart 4.2).

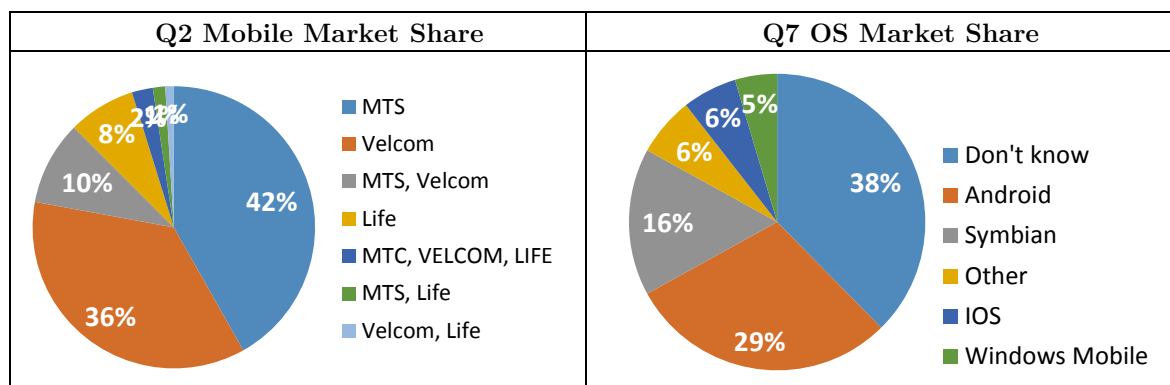


Chart 4.2: Market Indicators for Belarus from user survey.

4.4.3 People's Republic of China

The population of the People's Republic of China exceeded 1,351 million. The phenomenal size of the mobile market in the People's Republic of China is truly staggering. Mobile penetration had exceeded 76% and continues to grow.

The mobile operator China Mobile is the largest telecom company in the world. Considering the size of the market it was one of the least competitive markets with only three mobile operators.

Chinese state organizations also operate the largest internet monitoring and censorship system in the world.

There were 3 operators in the market with 50% using Android OS and 24% using IOS. Of particular interest is the market share 80% is managed by China Mobile (Chart 4.3).

²⁹ Ministry of Communications and Information of the Republic of Belarus
<http://www.mpt.gov.by/en/>

³⁰ National State Statistical Committee of the Republic of Belarus -- <http://belstat.gov.by>

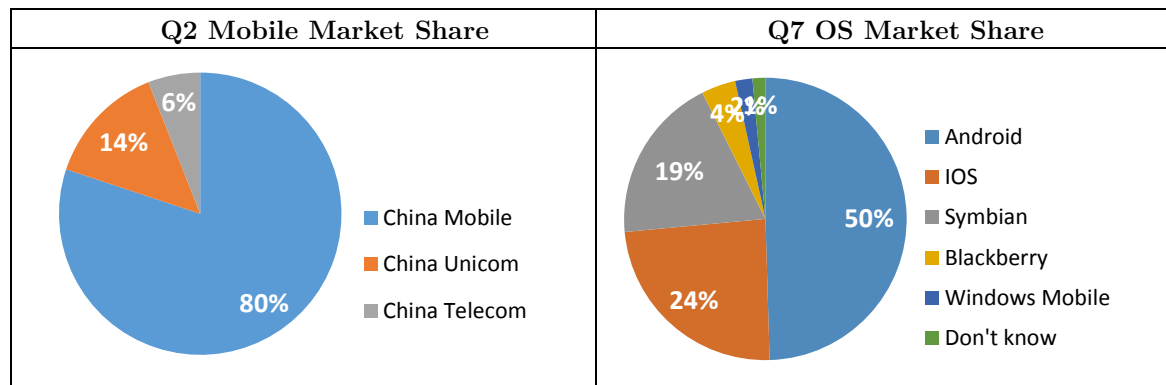


Chart 4.3: Market Indicators for China from user survey.

4.4.4 Islamic Republic of Iran

The population of the Islamic Republic of Iran exceeded 75 million. Market penetration had not kept pace with other countries in the region but there were a large number of subscribers. The Islamic Republic of Iran had one of the lowest mobile penetrations in the region at 72.3%. There were over 54 million mobile subscribers in the country.

Regulation of the mobile market in the Islamic Republic of Iran was very sophisticated and there is significant state ownership of the mobile operators with external involvement from organizations in South Africa and Malaysia.

Fixed broadband usage has amazingly low penetration in the market with only 0.7% of the population and an absolute volume of 1.7 million.

The Iranian Internet police require users of the Internet in cybercafés to produce an ID and cameras must be installed to monitor usage. The use of tools for circumvention of content filtering, VPN (Virtual Private Networks) and USB flash drives are banned. Web sites that carry forbidden content are closed and must be blocked.

There are 2 primary operators in the market with one provider servicing 50% of the market and with 25% using Android and 20% using Symbian. Of particular interest is that 28% respondents were not aware of which OS they were using (Chart 4.4).

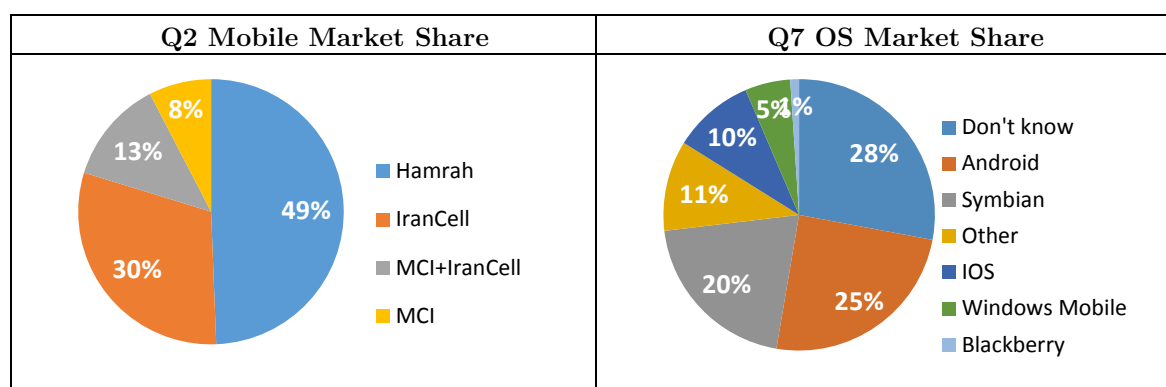


Chart 4.4: Market Indicators for Iran from user survey.

4.4.5 Sultanate of Oman

The population of the Sultanate of Oman exceeded 2.9 million. Mobile subscription penetration, in the Sultanate of Oman, almost reached 178% of population at the end of 2012 and continues to grow. In comparison there were less than 11% of fixed lines

installed offering less than 3.5% of internet broadband services. This means that the preferred delivery method for content was over mobile networks.

In Oman the use VoIP services which are not licensed was forbidden and Skype usage by subscribers was also blocked. Communication such as email, chat rooms and telephone is monitored and the list of forbidden network content was relatively long.

Two primary operators shared the market with 44% and 32% respectively. Apple IOS was used by 40% of the users, 29% use Google Android and 21% using Blackberry. Of particular interest is that 6% of respondents were using multiple providers and 3% were using Jordan Mobile for mobile services (Chart 4.5).

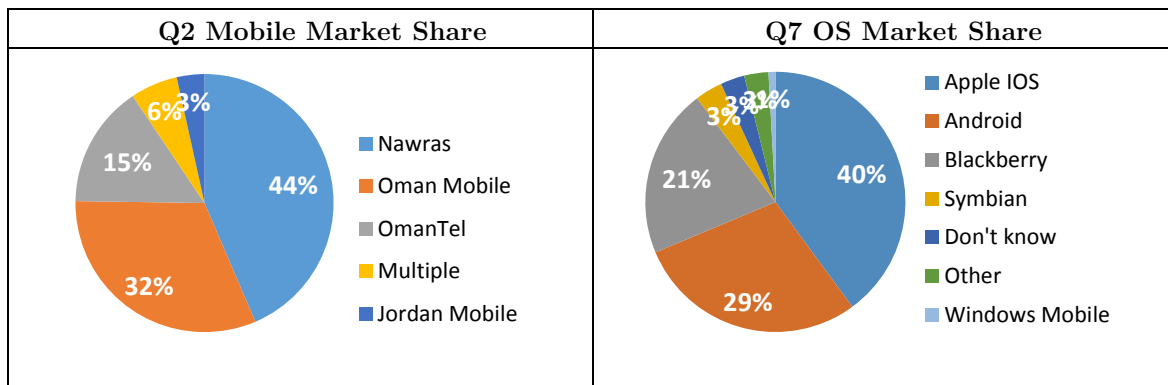


Chart 4.5: Market Indicators for Oman from user survey.

4.4.6 Kingdom of Saudi Arabia

The population of The Kingdom of Saudi Arabia exceeded 28.4 million. It is impressive because it had over 198% mobile subscriptions penetration and which is even more interesting due to the low penetration of fixed broadband (5.5%). Market regulation was strong and market competition is very healthy.

Almost 82% of users considered themselves intermediate users of mobile handsets and almost 92% of the mobile users in our survey have smartphones from the most recently manufactured range.

The internet is censored to a great extent and dedicated web page is set up for reporting any content that users believe should be blocked. KSA regularly censors pornographic content, and dissenting political or religious content along with websites focused on human rights issues. In 2009 hidden cameras were installed in internet cafes to record faces and names of all its users.

STC has 52% share of the mobile market followed by Mobily with 29% market share. Apple IOS is used by 41% of the users, 34% use Blackberry and 14% use Android. Of particular interest is that 4% of respondents were using multiple providers and the high levels of IOS and Blackberry use (Chart 4.6).

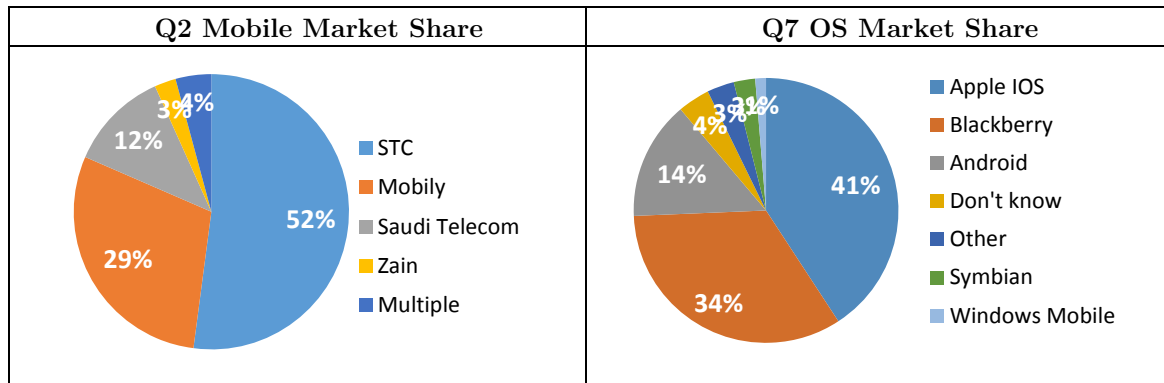


Chart 4.6: Market Indicators for Saudi Arabia from user survey.

4.4.7 Syrian Arab Republic

The population of the Syrian Arab Republic exceeded 20.5 million before hostilities started. It had the lowest level of mobile penetration (57.7%) in the region and among the lowest number of phone in use at 11.9 million subscribers. There were only two mobile operators active in the market and operators give a share of their profits to the state. With only two operators, the Syrian market did not have significant competition. The market is tightly controlled by organizations which are closely aligned with the government.

Syria used Ericsson technology to trace the GSM handsets of activists. The operators block many words sent using SMS (e.g. Freedom, Demonstration, Group, Revolution, etc.). Syria used blue coat technology (Blue Coat SG8100 Series) to filter the mobile internet and fixed line ISPs.

It is remarkable that there were only two operators in the market with SyriaTel having 58% share of the mobile market followed by MTN with 42% market share. This demonstrates the lack of choice and competition in the market. Symbian is the most popular OS at 25% and Apple iOS having 10% market share. Of particular interest is that more than 52% of respondents do not know what OS was installed on their phone (Chart 4.7).

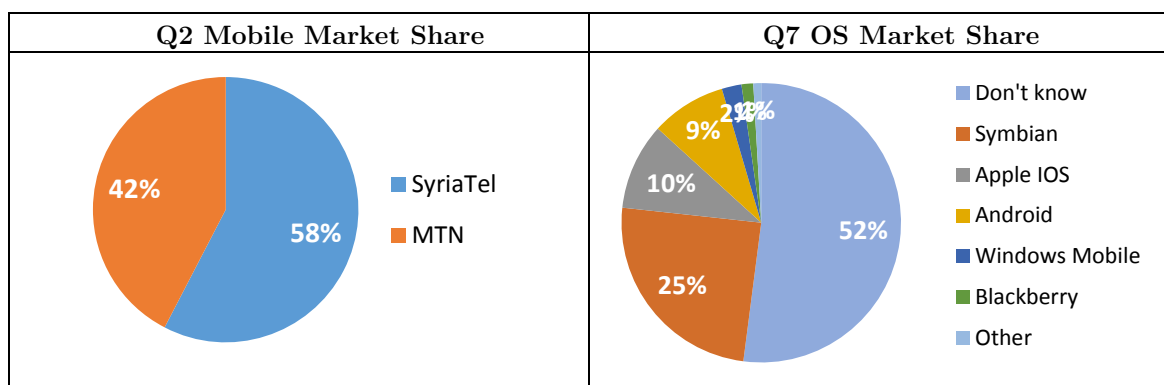


Chart 4.7: Market Indicators for Syria from user survey.

4.4.8 Tunisian Republic

The population of Tunisia exceeded 10.8 million and mobile phone penetration in Tunisia was approximately 117% with 12,5m subscribers. There were three market players called

Tunisie Telecom with 4.47m subscribers, Tunisiana with 6.82m subscribers and Orange Tunisie with 1.24m subscribers. The market was dominated by two main operators (Tunisiana and Tunisie Télécom). Only 2 operators offer 3G: Tunisie télécom and Orange Tunisie and the number of 3G users was 201 336 with an annual growth of 28%.

45% respondents used mobile internet and 48% did not use mobile Internet. 38% of mobile internet users used WIFI to access the internet with 15% paying for a limited volume of data with their subscription and a further 11% paying for usage. Over 33% indicated they had no access to the Internet using their mobile handsets.

Before the revolution the government was filtering every call especially for politicians, journalists and artists. It is believed that there was no calls interception after the revolution.

One mobile operator had over 75% share of the market with remaining operators sharing 25% market share. Android, Symbian, Windows Mobile, Apple IOS and Blackberry shared 31% of the market share. Of particular interest is that more than 69% of respondents did not know what OS is installed on their phone (Chart 4.8).

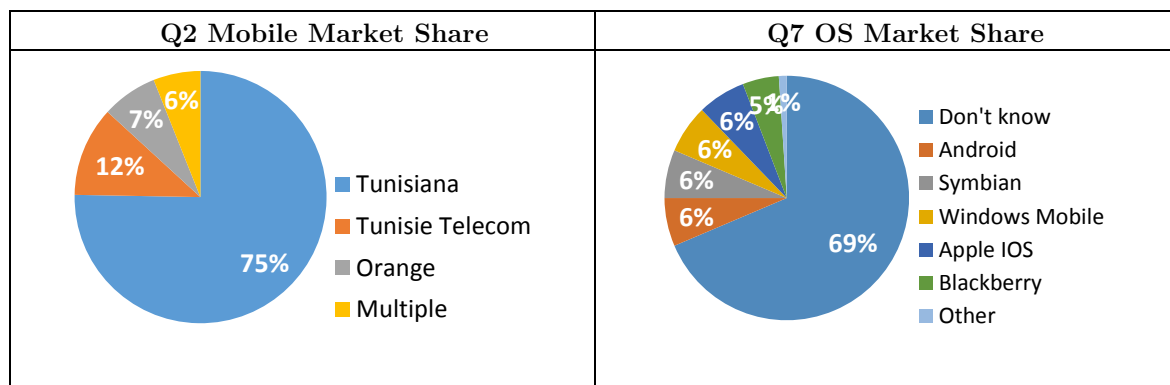


Chart 4.8: Market Indicators for Tunisia from user survey.

4.4.9 Republic of Uzbekistan

The population of the Republic of Uzbekistan exceeded 29 million. The telecommunications market of the Republic of Uzbekistan was in the process of saturation and was one of the fastest growing sectors of the economy. Uzbekistan had the highest rate of growth in the number of mobile subscribers in the Commonwealth of Independent States (CIS). The growth rate of revenues from mobile services lagged behind the pace of growth in the number of mobile subscribers. There were 24.3m mobile subscribers to the end of 2011.

The Uzbek Agency of Communication and Information acts as the main control center in the telecommunication field. All information about any internet or mobile user can be obtained as there was only one Tier-1 ISP which is the Uzbek telecom.

News websites and online newspapers are blocked. In some cases a partial or a temporary ban on the provision of services can happen as was the case with 1st of August (national university examinations).

BeeLine had 44% market share with MTS having 34% and Ucell having 11%. Android had 33% market share with 25% Symbian and 6% each for Apple IOS and Windows Mobile. Of particular interest is that more than 25% of respondents did not know what OS is installed on their phone and over 10% had services from multiple operators (Chart 4.9).

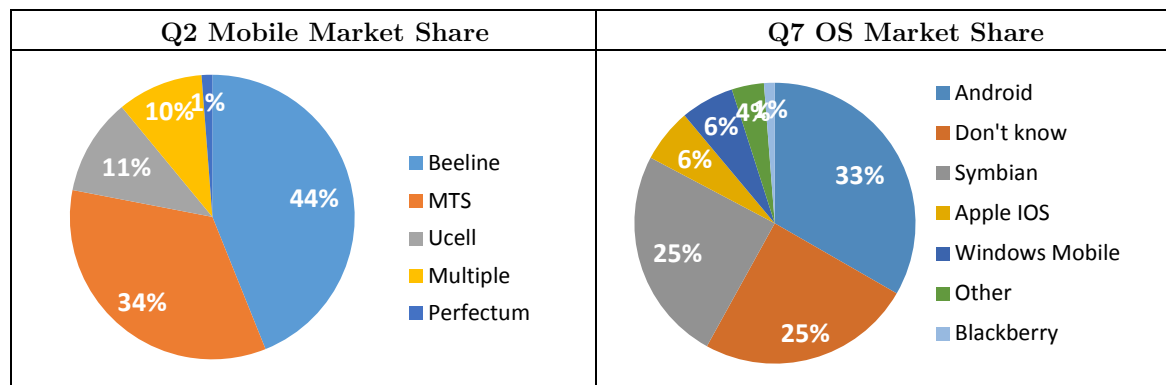


Chart 4.9: Market Indicators for Uzbekistan from user survey.

4.4.10 Socialist Republic of Vietnam

The population of the Socialist Republic of Vietnam exceeded 87.1 million. The mobile market in the Socialist Republic of Vietnam had been growing very fast. The mobile penetration had reached 137% of population over 9 years. Currently there were over 119 million subscribers.

It was one of the few countries that is making significant progress in the transition to IPv6 internet addressing technologies on mobile networks. A significant amount of Vietnamese mobile-broadband users access and download video content on their mobile phone.

As the ownership of the mobile networks was state based not much is known about blocking and monitoring. However, firewalls were used for preventing access to some web sites and call tracing was used for users indicated as “activist”. 18 bloggers and internet users had been arrested in previous years. Some social networks websites were also placed on the “black list” used for blocking.

Mobifone has 57% market share with Vinaphone having 21% and Viettel having 20%. Android has 23% market share with 16% Windows Mobile and 10% for Apple IOS and 8% for Symbian. Of particular interest was that more than 37% of respondents did not know what OS is installed on their phone and this country has the highest adoption rates for Windows Mobile at 16% (Chart 4.10).

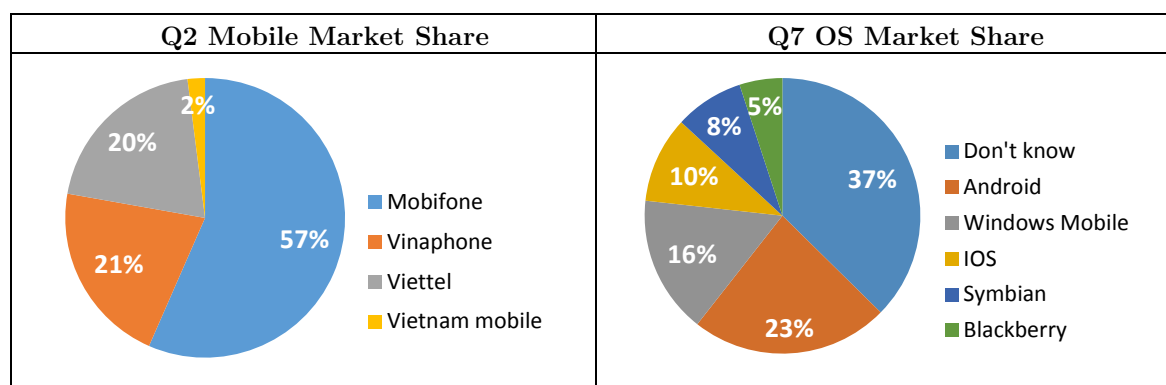


Chart 4.10: Market Indicators for Vietnam from user survey.

4.4.11 Summary

The mobile markets in these countries highlight a number of interesting characteristics. Some of them are listed below:

- Due to the nature of mobile communications where the radio spectrum is a scarce resource requiring direct regulation and management by the state, there are easy opportunities to increase mandatory requirements to include monitoring and surveillance capabilities.
- The size of the mobile markets in all the countries is large, with high levels of mobile penetration. The People's Republic of China is the largest, with 1,030 million subscriptions, while the Sultanate of Oman is the smallest, with 4.9 million subscriptions.
- The penetration of mobile subscriptions in the population of every country is high. The Syrian Arabic Republic has the lowest penetration, with almost 58%. The Kingdom of Saudi Arabia has the highest penetration, with 198%.
- The revenues from the mobile market are significant for both the mobile operator and the government. These revenues take the form of taxes and license fees.
- The investments in the fixed-line infrastructure are low in most of the countries in the survey.
- In several countries, such as the Republic of Belarus and the Socialist Republic of Vietnam, there is a vibrant black market for handsets. Of course, handsets can still be identified and logged by the mobile operator, but it is encouraging that such handsets were not installed with specific software configured by the state or mobile operator. In several countries, such as Sultanate of Oman, a handset-labelling requirement for authorized handsets has been implemented and spot audits have been performed on retail outlets selling handsets to ensure compliance.

4.5 Overall Results of the User Survey

The following information about basic services was recorded:

- 61% of users used a prepaid phone and 37% used a postpaid service. (Q3 Chart 4.11).
- It was found that 81% of the mobile users surveyed have access to the Internet using their mobile phone (Q4 Chart 4.12).
- 33% of users accessed the Internet with a mobile handset using a Wi-Fi connection, 33% of them access the network using a limited Internet bundle or by using a pay-as-you-go service (17%) (Q5 Chart 4.13).
- Over 71% of the users paid for their own phone services while in 23% of the cases the bill was paid by the user's family. This shows who could access user's billing information and usage data. A large number of employers with paid usage bills would suggest possibilities for third-party access to, and control of, detailed billing information together with the information about the call data (Q6 Chart 4.14).
- Over 69% of all respondents indicated that they have their own smartphone leaving a significant minority of 24% who did not have a smartphone and a small group of 7% who did not know what a smartphone was (Q15 Chart 4.15).

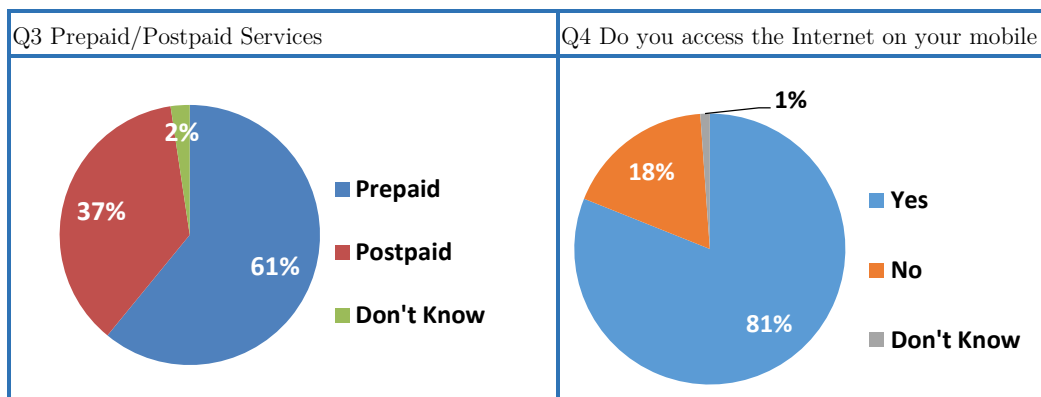


Chart 4.11: Q3 PrePaid/PostPaid

Chart 4.12: Q4 Mobile Internet

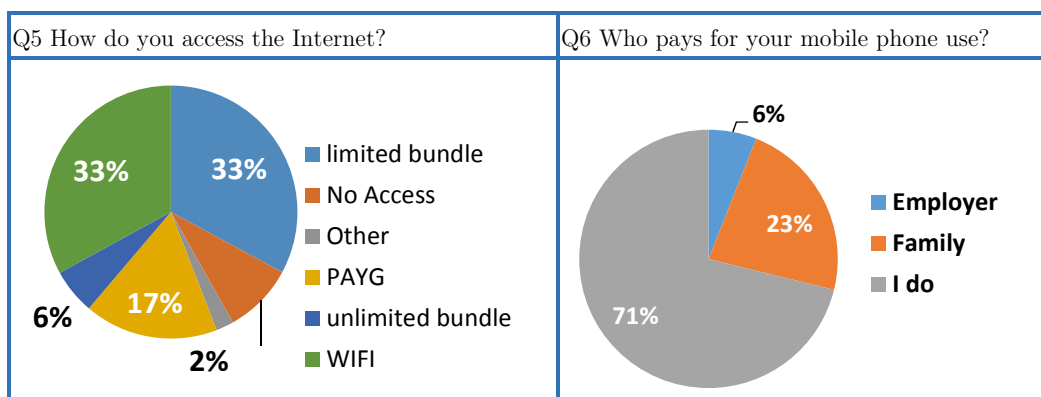


Chart 4.13: Q5 Internet access

Chart 4.14: Q16 Who Pays?

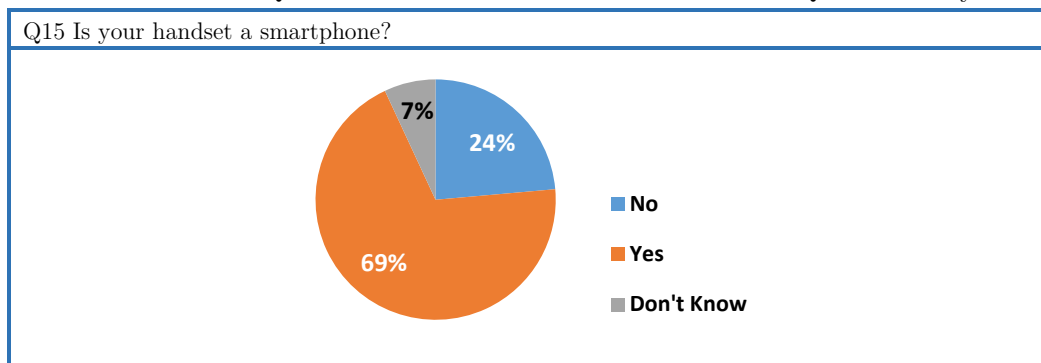


Chart 4.15: Q15 Smartphone?

The following information was recorded:

- In the survey respondents, over 31% users owned handsets manufactured by Nokia, 20% were made by Samsung and 19% were by Apple and 9% were made by Blackberry (Q7 Chart 4.16).
- In the survey respondents, over 27% users did not know what operating system was installed on their handsets and 24% owned handsets running the Google Android operating system, 17% had Apple IOS, 13% had Nokia Symbian and 8% had Blackberry (Q8 Chart 4.17).
- Over 57% of the users 'Rarely' or 'Never' share content using Bluetooth. This information is important since sharing content using personal area networks (short distance) is more secure and difficult to detect by malicious investigators unless the Bluetooth network ID (unique to each handset) is pre-stored by the handset retailer (Q10 Chart 4.20).
- Over 66% of the users did not 'jail-break' their phone – install software from a source other than the manufacturer leaving 21% who confirmed that they had. This information is important since there are more secure software versions available which can detect monitoring or promote awareness of monitoring possibilities (Q11 Chart 4.18).
- Over 46% had updated the firmware on their handset and 47% had not updated the firmware on their handset. This information is important since there are software updates which improve security or increase awareness of security risks or monitoring possibilities (Q12 Chart 4.19).
- 31% of users considered themselves as having basic skills, 60% considered themselves having intermediate skills and 9% self-assessed as having advanced skills (Q13 Chart 4.21).

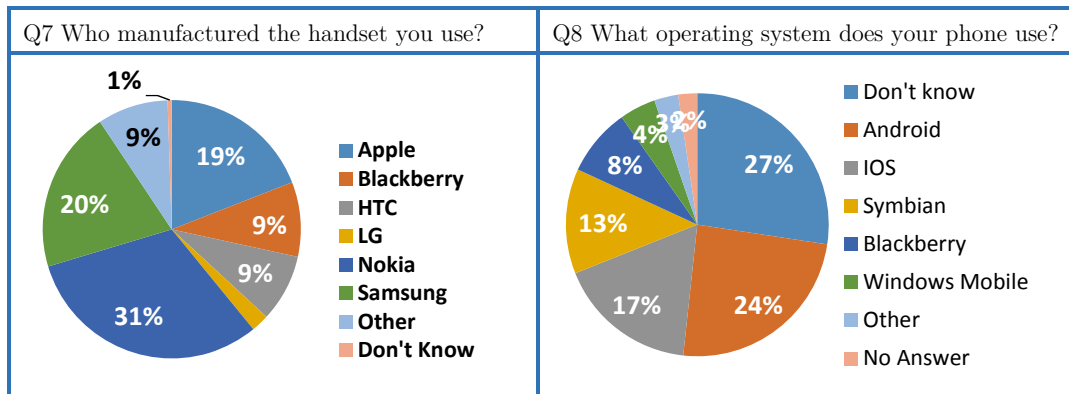


Chart 4.16: Q7 Handset Manufacturer

Chart 4.17: Q8 Phone OS

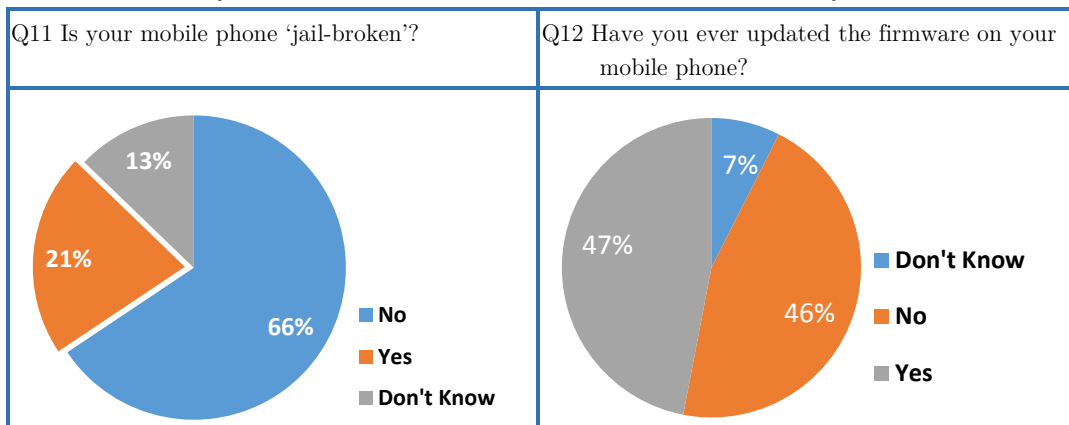


Chart 4.18: Q11 'Jail-broken'?

Chart 4.19: Q12 Firmware Upgraded

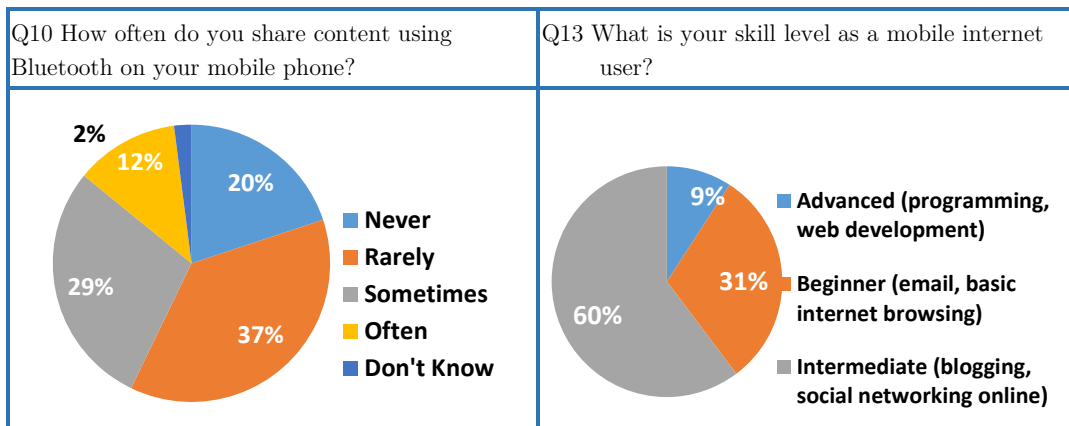


Chart 4.20: Q10 Share with Bluetooth

Chart 4.21: Q13 Skill Level

The following information was recorded:

- They use the internet 28% of their time to keep in touch with and communicate with others. 17% of time is allocated to social networking services as the second online activity and for work related activities respectively, 16% indicated that they access the internet for entertainment purposes, 13% time is spent on online news (Q18 Chart 4.22).
- 54% of users do not receive online bills and 46% do. This is important since it clearly records the cost of online services and it highlights to users the range of data that can be collected about usage over long periods of time (Q21 Chart 4.23).
- 45% of users use the internet to communicate with others, 29% access public information online and 13% time is allocated to accessing protected information and sharing sensitive information respectively. This could include political activism and personal information related to banking, relationships, etc. (Q19 Chart 4.24).
- 27% of content accessed relates to accessing text content on websites and emails. 22% of online activity is transmitting text content (emails, social networking, etc) and 21% is accessing content with many images and 17% is used on audio and visual multimedia content (Q20 Chart 4.25).

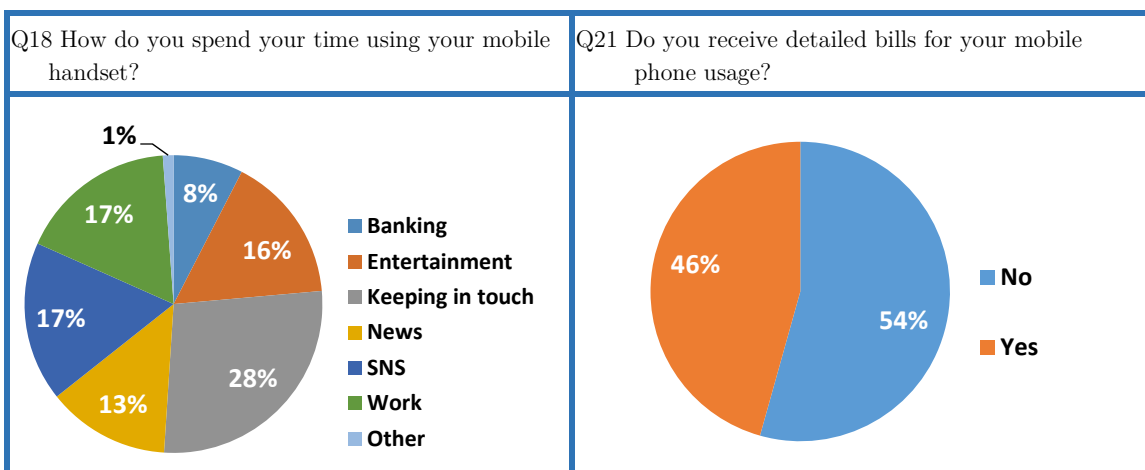


Chart 4.22: Q18 Mobile Usage

Chart 4.23: Q21 Detailed Billing

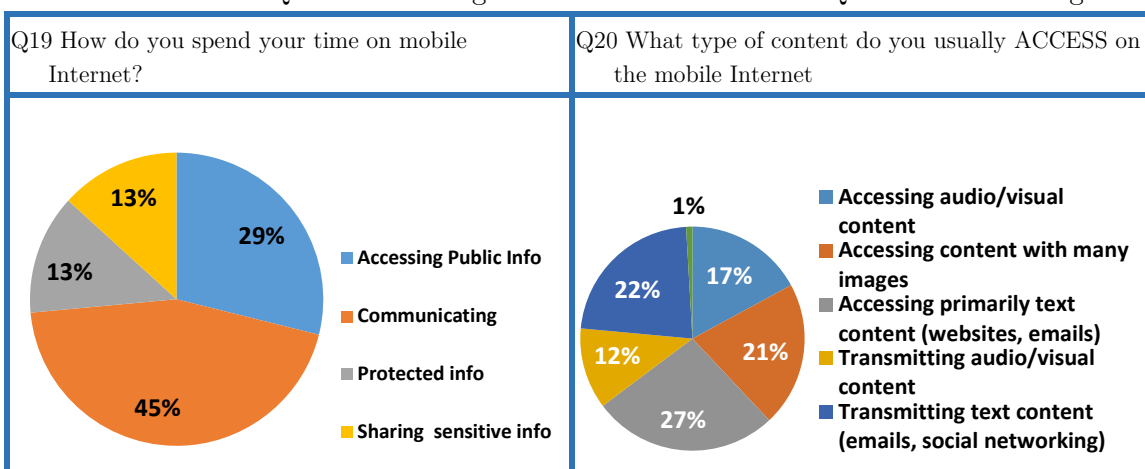


Chart 4.24: Q19 Mobile Internet Time

Chart 4.25: Q20 Mobile Content

In general, it is clear that there is a growing supply of handsets and an increasing number of new mobile packages offered in the target markets. This was considered an indicator of the greater availability of mobile technology. These findings suggest vibrant, competitive, and profitable markets with a strong demand for future mobile services. A wide variety of handsets presents itself, with important new challenges for the state security agencies and operators, who want to implement hardware-monitoring options specifically designed for a complex range of market-available handsets enabling Internet access.

The research in Chapters 2 and 3 confirmed the existence of a range of state strategies for ensuring effective state control of mobile operators—both in terms of selecting which market operators are licensed and in terms of the business activities of those licensed market operators. One motivation for state oversight of the Internet is to support and encourage extensive investment and sector growth, while a second, equally important aim, is to ensure suitable levels of state control over mobile operators.

4.6 Mitigating Filtering and Blocking and User Trust

The research in this Chapter and in Chapters 2 and 3 provided information about users’ abilities to understand the threats that they are exposed to and their awareness about the possibilities for upgrading their devices to help them mitigate the identified threats and risks. The information sought in the survey included the type of access to, and the use of, a mobile service; the operating system and the mobile handset used; the level of skills with respect to accessing the Internet via a mobile connection; the type of applications downloaded and used; and attitudes about privacy, content filtering/blocking and traffic monitoring.

51% indicate that they often or sometimes encounter blocking when using the internet (Q14 Chart 4.26)

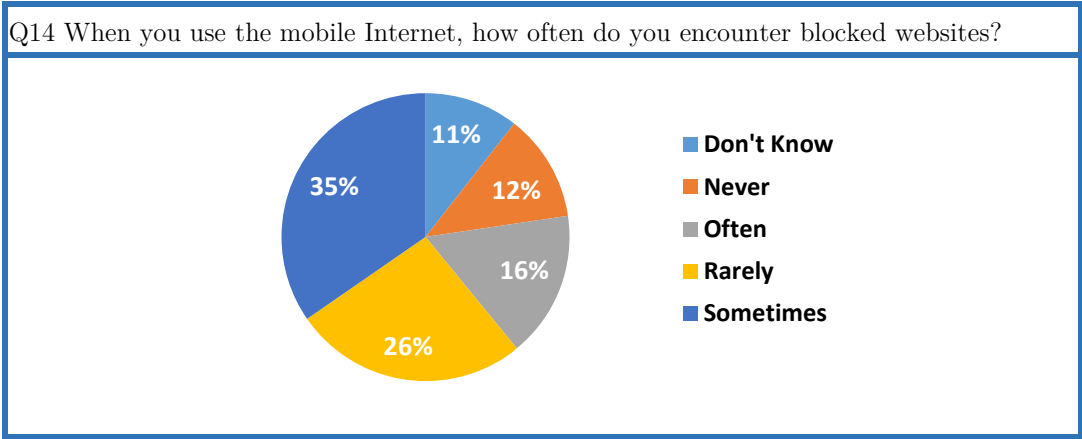


Chart 4.26: Q14 Encounter blocked websites

25% stated that mobile monitoring or blocking is performed by a specialised state agency responsible for communications supervision/ regulation and 18% indicate that this is supported by legislation requiring blocking / monitoring with limited supervision (Q22 Chart 4.27).

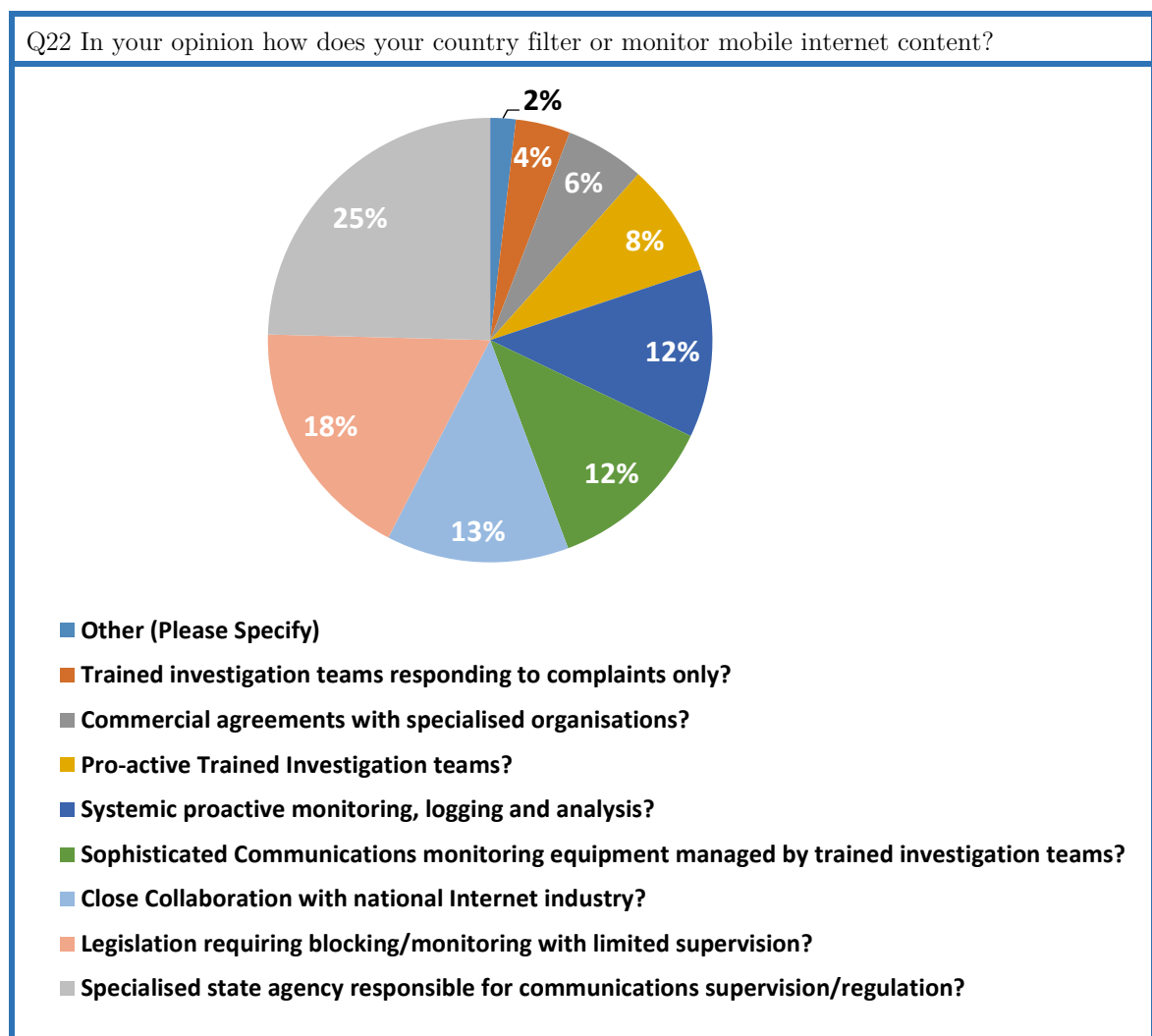


Chart 4.27: Q22 Who monitors?

As a result of the research completed in Chapter 3, the circumvention of content blocking or monitoring is still largely reliant on VPN technologies, which must be available in the network and in the smartphone as well.

From the five OS platforms studied, Android had the most complete landscape for “circumvention” and “voice/text” data protection. This is mainly due to the fact that access to the TOR application (The ToR Project, 2012) is available only to users of the Android OS.

The study results also confirmed that general platform security has a higher priority for manufacturers than the provision of circumvention capabilities for the smartphone users. From the perspective of an OS designed to prevent or minimize threats, recent and future developments are still required, and this demand should not be ignored by most of the participants in the market, especially by the niche manufacturers that dominate the area of circumvention tools.

From analysis of a range of responses collected from the user communities we can conclude that there is still a need for users to better understand the safety and security implications in order that they become more capable in terms of managing their privacy. While generic security checks would be helpful, many threats can only be mitigated through proper device management by the user and by the use of more advanced security

mechanisms that should be downloaded and installed. This means that raising awareness and sharing knowledge should be activities that continue in the future.

In the survey data differences were noticed among the user communities regarding the level of skill of the user (Q13 Chart 4.28).

In the three countries (Kingdom of Saudi Arabia, Sultanate of Oman and People's Republic of China) the skill level appeared to be very high, 89% of interviewed users in People's Republic of China consider them as high or intermediate level skilled users. The percentage of this type of users in the Kingdom of Saudi Arabia is 91% and in Sultanate of Oman this number is 90% (Q13 Chart 4.28).

They are also not very active in firmware updating (between 61% and 71%) (Q12 Chart 4.29).

In other studied countries the user skillfulness appeared to be rather low. In the Socialist Republic of Vietnam 63% users considered themselves as beginners, in the Syrian Arab Republic and in the Islamic Republic of Iran this amount was 53% and 73% respectively (Q13 Chart 4.28).

Q13 What is your skill level as a mobile internet user (excludes no answer)?

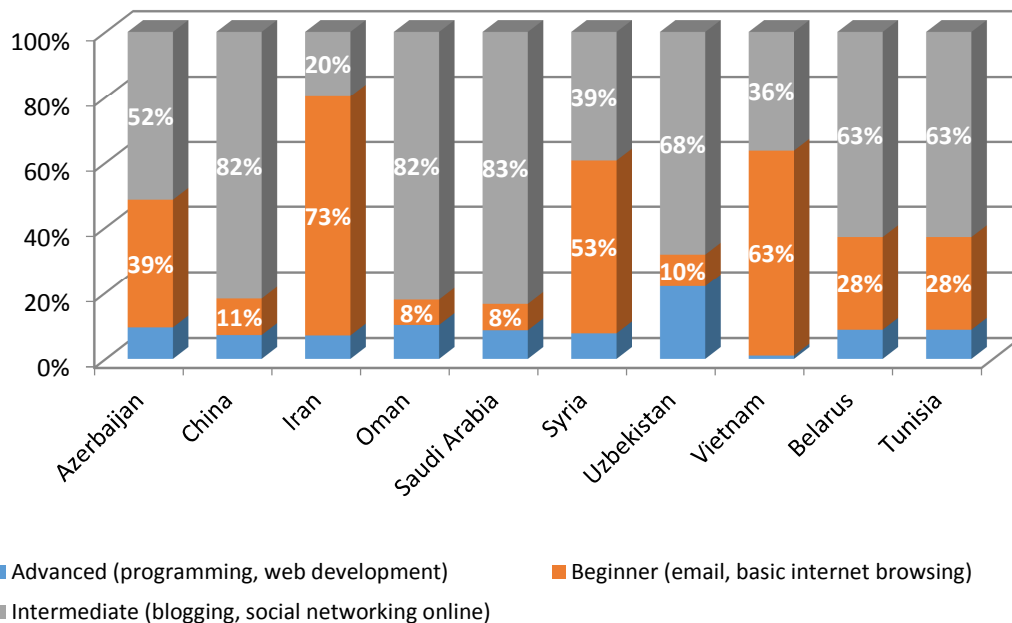


Chart 4.28: Q13 What is your skill level as a mobile internet user?

The Republic of Belarus, the Islamic Republic of Iran, the Syrian Arab Republic, Republic of Azerbaijan and the Republic of Uzbekistan have also majority of their users that do not upgrade their firmware (the amount of these is from 42% to 64%) (Q12 Chart 4.29).

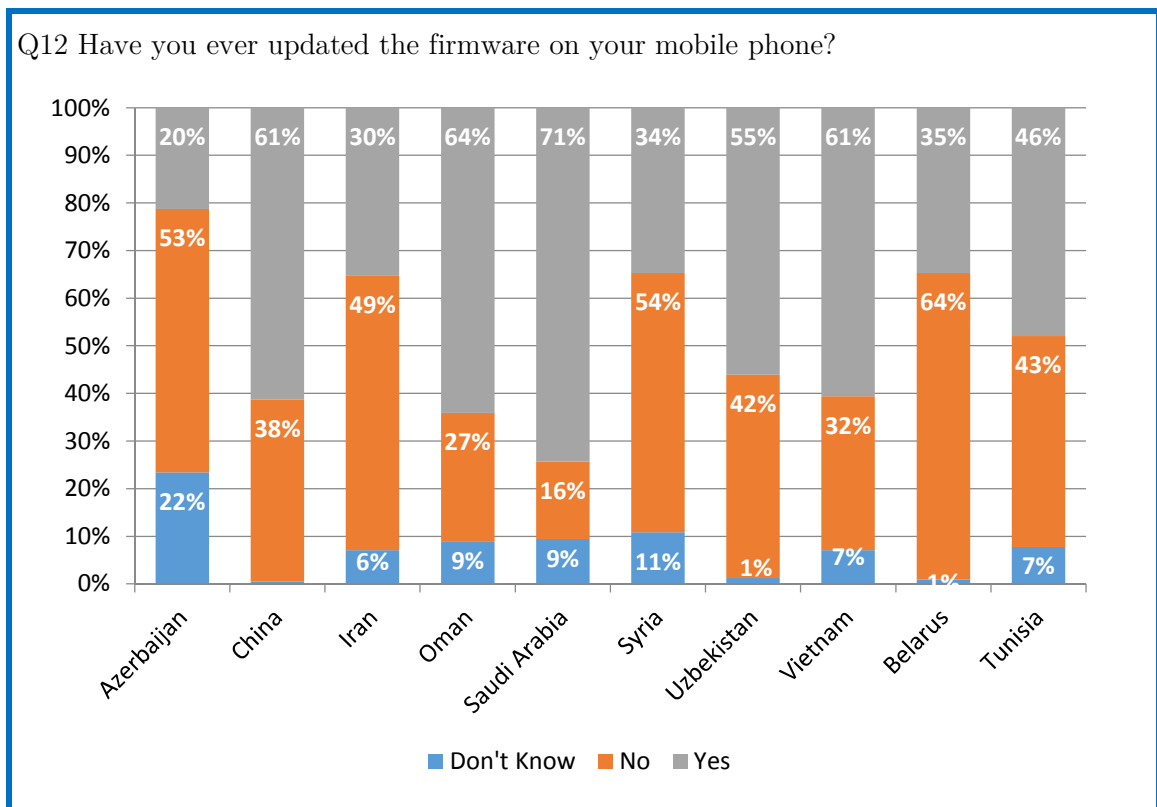


Chart 4.29: Q12 Have you ever updated the firmware on your mobile phone?

Users downloaded Apps in different frequencies, from a variety of online stores (1=rarely, 4 = often) (Q9 Chart 4.30).

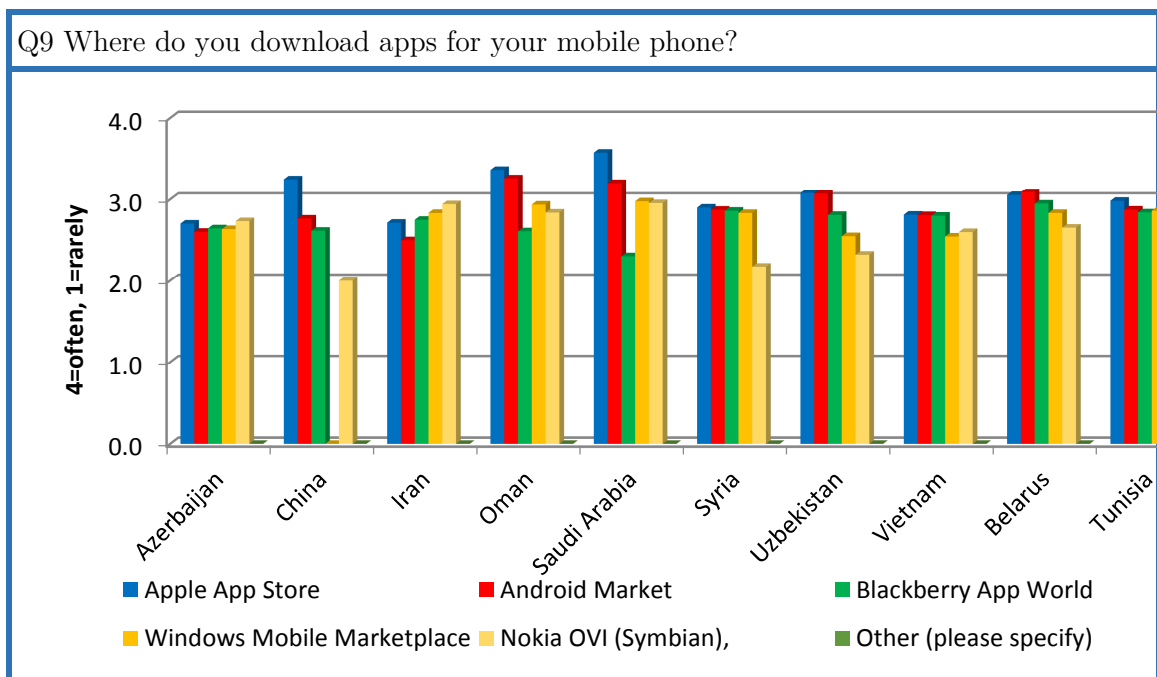


Chart 4.30: Q9 Where do you download apps for your mobile phone?

The analysis of the data showed that some user communities are neither very attentive nor knowledgeable with regards to the presence of monitoring and blocking in the network

In three countries (Kingdom of Saudi Arabia, Sultanate of Oman and People's Republic of China) users showed significant differences in how often they notice blocking compared to the other countries. For example, in Saudi Arabia, 44% of users notice blocking 'sometimes' and 34% of users rarely notice blocking. However, the responders from China differ slightly as they declared that they often encounter blocked content (35% of them) but no concern about that was expressed. These values are shown in Q14 Chart 4.31.

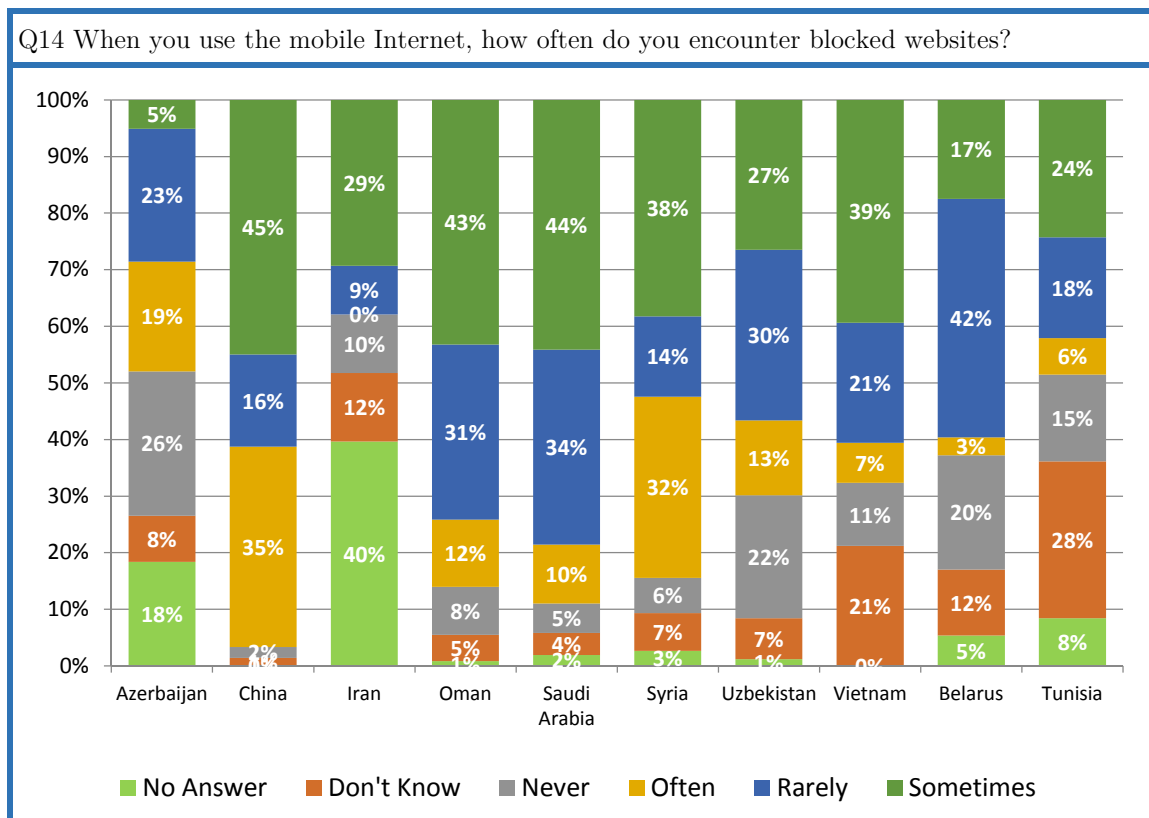


Chart 4.31: Q14 How often blocked websites are encountered on mobile Internet.

The differences noticed in the perception of blocking were reflected in the answers dealing with the identification of entities responsible for these activities (Q22 Chart 4.32). Most of the users from the studied countries answered that the blocking is performed by a specialized governmental agency and that this is due to adopted legislation. Some 35% to 45% of users answered that this is done by a specialized state-owned agency and 15% that this happens due to national legislation.

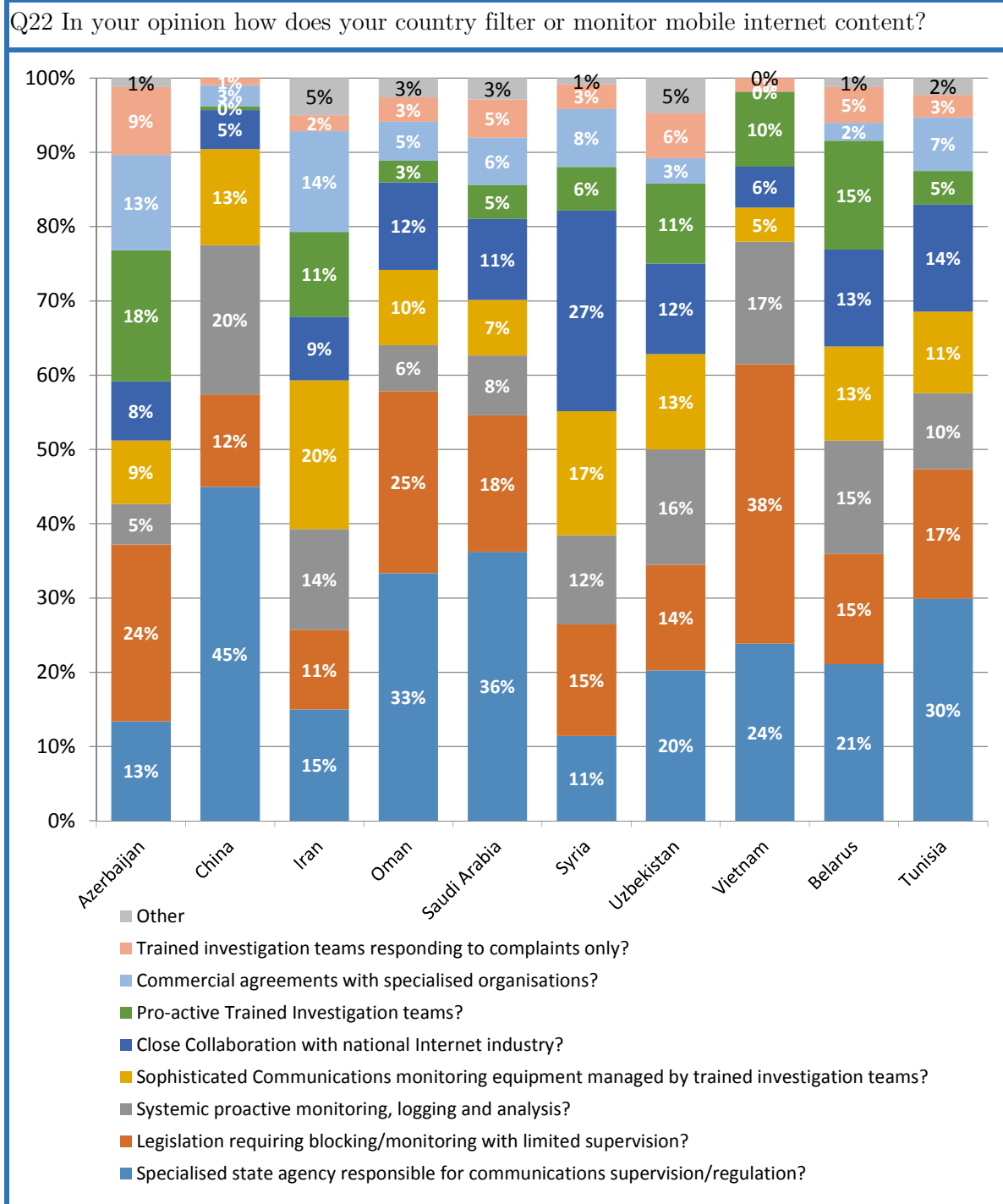


Chart 4.32: Q22 Respondents view on who filters or monitors mobile internet.

However, the answers regarding trust in entities that restrict content or monitor traffic among the studied communities appeared to differ significantly (Table 5.11 and Table 5.12). In the Sultanate of Oman and the Kingdom of Saudi Arabia the users trust the government, the state agencies and the ISPs inside their country. The ranking of these entities provided by these citizens filled the top three places on the scale of trust. In the People's Republic of China responses about whom to trust in mobile communications ranked the state agencies and government in 3rd and 5th positions, with and higher rankings of 1st and 2nd positions being given to commercial organizations

inside and outside the People’s Republic of China. The users of the Republic of Azerbaijan also indicated rather moderate trust than distrust towards government agencies. In the Republic of Azerbaijan, the Socialist Republic of Vietnam, the Syrian Arab Republic and the Republic of Uzbekistan the users trust, regarding their privacy, only ISPs that are outside the country, and in The Islamic Republic of Iran, to persons inside the country. The government and governmental agencies are not trusted at all. They received the lowest possible ranking on the trust scale.

With a high of 2.36 out of a score of 5 (where 1 = never and 5 = always) responses indicated very clearly that among the users there is low trust with respect to the majority of the stakeholders in this complex area (Q23 Chart 4.33). In most of the studied countries the governments and state organizations came among the lowest on the list.

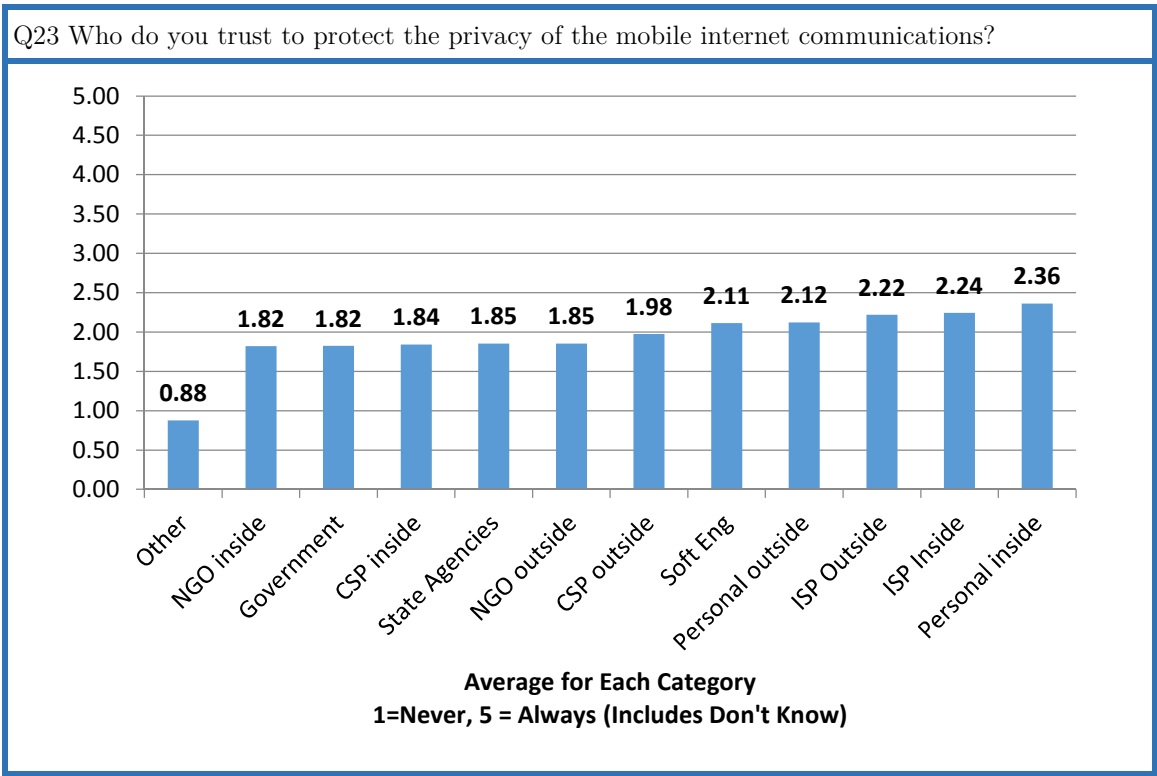


Chart 4.33: Q23 Who do you trust to protect the privacy of the mobile internet communications?

Issues about blocking, monitoring, and trust are analyzed in greater depth in the next chapter.

Chapter 5

Data Analysis

This chapter describes the additional analysis performed on the data collected in the user survey in order to confirm six hypotheses which are defined based on the research questions. The analysis considers factors associated with awareness of monitoring and blocking as well as factors associated with trust people put in different agents to protect their privacy during mobile internet communication. The association between the level of skill of mobile internet users and their ability to protect themselves against monitoring is also considered. The research investigates the level of individual user capabilities such as user-skillfulness or the characteristics of the environment such as the accessibility of technology or country characteristics such as broadband affordability, market development and religion associated with user awareness of monitoring and blocking of the internet content. It further investigates if these same characteristics are associated with trust users put in different sources to protect their privacy during mobile internet communication. It also gives insight on whether user-skillfulness influences the user capability to download additional tools to their smartphone to increase data protection and security. The analysis enables conclusions to be drawn regarding the factors that influence user attitudes towards mobile services privacy threats and their trust in the studied countries that have more restrictive regime and strongly controlled mobile market. This provides input on the most effective and high impact approaches to raise awareness about security risks and to develop processes to encourage and stimulate increased safer use of mobile devices.

The results of the user survey were analysed and compared with the GNI indices and with the affordability of the mobile technology measured by the service prices of the studied countries which is measured by ITU (ITU, 2012) as a percentage of GNI per capita for each country. The analysis enabled the development of a structural model which can provide input for future research initiatives in the specialist area of user security and privacy in an increasingly mobile dependent world.

5.1 Research Hypotheses

The research questions identified in the first chapter were reformulated into hypotheses, which will be proven or rejected by the data analysis. These are:

- H.1: Greater user awareness of Internet content restrictions is associated with higher level of information society development.
- H.2: User level of skill positively correlates with user capability to recognize traffic monitoring and content blocking.

- H.3: Higher level of information society development contributes to greater user awareness that content blocking and monitoring is performed by state owned agencies.
- H.4: 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.
- H.5: Skilled users are more likely to have jail-broken phones and to have updated the firmware on their phones which enables them to improve their privacy protection.
- H.6: User tolerance of content blocking and the user trust in state-owned agencies as entities that care about their privacy are correlated with the high level of information society development, the availability of technology, and the wealth of the country.

The structural model was designed after evaluation of the survey data and was built based on the confirmation or rejection of the six hypotheses. The methodology used to design the structural model is described in the next section. It is a model which can be used by future researchers for monitoring the changing landscape of mobile risks associated with mobile services and support focused risk-mitigation strategies.

5.2 Methodology

Regression models were built using variables obtained from two sources of information;

- feedback from the user survey respondents
- country statistics obtained from public sources

5.2.1 Factor Analysis

A factor analysis was performed using the collected 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), the mobile Internet usage and to eliminate unrelated variables.

Positive and significant correlations exist between the GNI and mobile market penetration ($r = 0.78$; $p = 0.005$) (Table 5.1)

Table 5.1: Correlation between GNI and Mobile Market penetration and IDI.

Country	GNI 2012	Mobile Market Penetration 2012 (%)	MISC IDI 2012
Republic of Azerbaijan	10365	99.0	5.01
Republic of Belarus	14950	108.9	6.11
People's Republic of China	9040	75.6	4.18
Islamic Republic of Iran (I.R.)	12895	72.3	3.79
Sultanate of Oman	25320	177.6	5.36
Kingdom of Saudi Arabia	30160	198.0	5.69
Syrian Arab Republic	5100	57.7	3.22
Tunisian Republic	9650	116.6	3.7
Republic of Uzbekistan	3670	84.0	3.12

Socialist Republic of Vietnam	3620	136.9	3.8
Correlation with GNI	1	0.78	0.77
p-value 2-df		0.005	0.007

Factor Analysis identifies the independent and dependent variables in the survey questions by analysing the correlation between the questions and by grouping questions with high correlation into common factors and then determining how influential each factor relates to the final analysis – this latter value is presented as a percentage of the final score.

The factor analysis using the Principal Axis Factoring method (PAF) gave a single-factor solution, as the GNI variability and mobile market penetration were explained with one factor of 86%. This is the “Mobile-Market-Development” factor score.

A moderately high and positive correlation was also found between the price of prepaid and post-paid mobile services as a percentage of GNI ($r = 0.64$; $p = 0.04$) and 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. This is the “Affordability of Technology” factor score.

The factor scores were saved as independent variables:

- one variable was used to represent the level of the **information society development**
- one variable was used to represent the **affordability and accessibility of technology**.

To understand the influence of user skillfulness, the user level-of-skill (user-skillfulness) was used as the third variable.

Table 5.2: Country Level Independent Variables.

Independent Variables	Value
Mobile Market Development	GNI variability and mobile market penetration were explained with one factor of 86%. (higher score, higher market development)
Affordability of Technology	Expressed as factor score obtained by factor analysis on pre-paid and post-paid mobile broadband prices of countries in the sample; higher score = higher affordability).
User Skillfulness	Skill level as mobile internet user Frequency of Apps Download

These variables were used as the country-level variables for the subsequent analysis and are listed in Table 5.2 and in Figure 5.1.

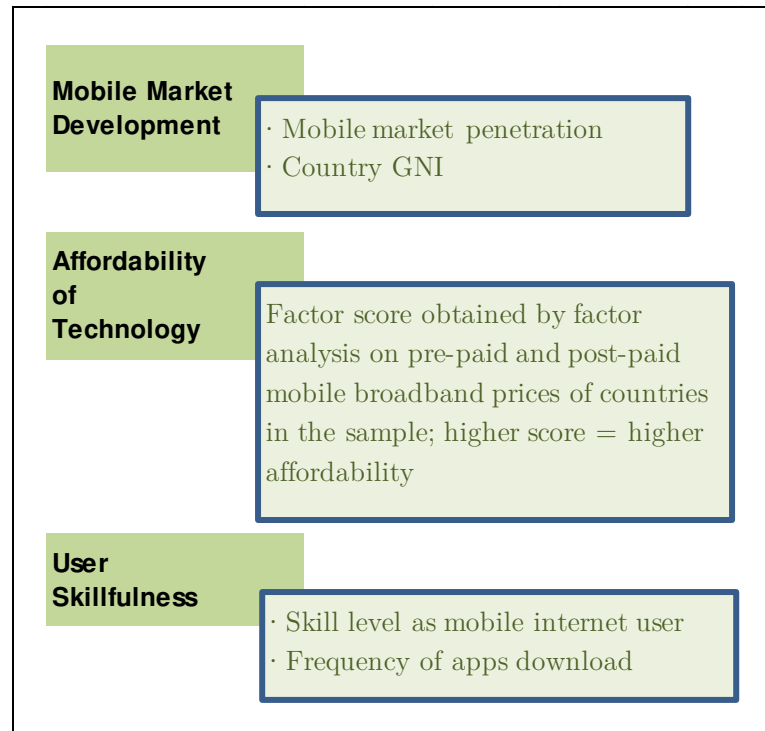


Figure 5.1: Independent Variables

Figure 5.1 lists the independent variables and how they are measured. The boxes on the left-hand-side indicate the variable titles and the text in the right-hand-box indicates how these variables are calculated or measured.

5.2.2 Regression Analysis

To test the hypotheses deriving from these variables, a multilevel, multivariate, logistic regression analysis was used. This analysis was performed simultaneously on two levels.

- First level, all respondents were included in the sample, and
- Second level, all countries were included in the sample³¹.

Several predictors were provided by the regression analysis. The hypotheses were tested with $\alpha = 0.05$ and $p < 0.05$, which were treated as statistically significant. By using this method of analysis it was possible to include state variables in the prediction model. At the same time a grouping effect (similarity between individuals inside each group – country) was taken into account when testing given hypotheses. Several predictors were included in the regression model at the same time to obtain more valid results regarding explanation power of each included predictor.

Four regression models were built to answer the research questions and to check the validity of the hypotheses.

The first regression model includes market-development variables used for measuring the level of information society development (mobile market penetration data, GNI).

The second regression model uses affordability of the mobile broadband technology as described previously in Table 5.2.

The independent user-level variables are: the level of user skills (based on self-assessment - beginner, intermediate, or advanced), the frequency of application

³¹ Since the second level sample size was rather low, only a computationally less demanding random intercept model was investigated.

downloads (at most sometimes or often), mobile 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). (Table 5.3)

Table 5.3: Independent User-level Variables from user survey.

Independent User Survey Variable	Possible Values
Level of User Skills (User Skillfulness)	Beginner, Intermediate or Advanced (based on self-assessment)
Frequency of Application Downloads	At Most Sometimes / Often
Mobile Internet access	Yes / No
Mobile services	Pre- / Post-Paid
Mobile Brand	Apple, Blackberry, HTC, LG, Nokia, , Samsung, or other

The dependent variables are: the frequency of encountering blocked web sites (rarely/never, sometimes, or often), 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 jail-broken phone, which enables the installation of applications from other manufacturers (Table 5.4). Rarely and Never were combined since the value for "never" variable is quite low and by grouping the "never" with "rarely" we have a variable which has more influence on the correlation.

Table 5.4: Dependent variables from user survey.

Dependent Variables (User Survey)	Values
Frequency of Encountering Blocked content	(Often, Sometimes) / (Never, Rarely)
Phone Firmware updates	Yes / No
Users' Opinion about who is Responsible for Monitoring and Internet Content Blocking	State / Non-state
Who is Perceived as Trustworthy Provider of Mobile Privacy Protection	Answers grouped into three categories: • State and state-owned agencies • Non-state agencies • Private sources • No One
Jail-broken Phone, (which enables the installation of applications from other sources)	Yes / No

To develop the structural model further the level of significance between the independent variables and the dependent variables was investigated. These variables are available from the user survey. The Affordability of Technology and Mobile Market Development were added from the ITU Report about the development of the Information

Society in each of the studied countries and they determine the independent variable called Information Society Development.

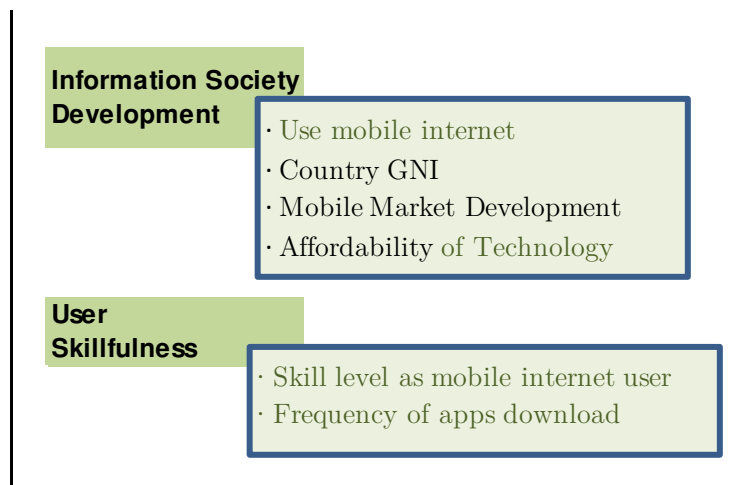


Figure 5.2: Combined Independent Variables

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 greater 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 less 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.

All the variables for the studied data are identified in Table 5.5.

Table 5.5: Overview of Independent and Dependent Variables.

Independent User-Level Variables				Dependent Variables			
Accessibility of technology		Skilfulness		Protection		Monitor & trust	
f (%)		f (%)		f (%)		f (%)	
Handset Brand		As download		Jail-broken phone		Trusted agents	
Apple	297 (18.8)	At most	577 (36.6)	Yes	327 (25)	No One	520 (34.0)
Blackberry	149 (9.4)	sometimes		No	979 (75)	State	320 (20.9)
HTC	134 (8.5)	Often	999 (63.4)	Updated phone		Non-state	292 (19.1)
LG	30 (1.9)	Skill level		Yes	720 (49.9)	Private	399 (26.1)
Nokia	519 (32.8)	Beginner	474 (30.9)	No	723 (50.1)	Monitor	
Samsung	322 (20.3)	Intermediate	917 (59.8)			State	748 (70.2)
Other	133 (8.4)	Advanced	143 (9.3)			Non-state	318 (29.8)
Mobile internet		Blocked Content					
Yes	1274 (81.9)	Never /					
No	281 (18.1)	Rarely 565 (41.5)					
Mobile service		Sometimes 509 (37.3)					
Post-paid	573 (37)	Often 289 (21.2)					
Pre-paid	975 (63)						

* f = frequency

The statistical significance of the calculated odds ratio is expressed with p-values. Correlations with p-values lower than or equal to 0.05 are treated as statistically significant.

5.3 Results and Findings

5.3.1 Hypotheses H1 and H2

The first regression model was used to test the H1 and H2 claims, which identify the factors that have influence on 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 filters/blocks mobile Internet usage.

In this section, we shall analyse the first aspect, i.e. the frequency of occurrence of the blocked content events. The results of the multivariable regression analysis using the frequency-of-occurrence-of-blocked-content are presented in Table 5.6.

H1 states that greater user awareness of Internet content restrictions is associated with higher level of information society development.

The information society level of development measured as the mobile market development and wealth of the citizens (GNI) are also associated with the frequency of encountering blocked content. From Table 5.6 users from the more developed markets

detect more blocked content events (OR 2.92 (1.08; 7.93) $p = 0.04$) (Table 5.6 last row). Skilled users and users from developed and wealthy markets are more aware of blocking than the less skilled users and users from the less developed and less wealthy markets.

This confirms the first hypothesis H1. The analysis confirms that greater user awareness of Internet content restrictions is associated with higher level of information society development.

Table 5.6: Factors associated with frequency of encountering blocked content (results of multilevel multinomial logistic regression; reference category = often).

Frequency Blocked Content => Predictors (reference category)	Never/Rarely			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
Mobile Brand						
Apple (other)	0.53	(0.24; 1.20)	0.13	0.66	(0.30; 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; 0.70)	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; 1.40)	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)	2.60	(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	0.70	(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

H2 states that the user level-of-skill positively correlates with user capability to recognize traffic monitoring and content blocking.

As is evident from Table 5.6, Mobile-Internet-skills correlate with the frequency-of-occurrence-of-blocked-content. Compared to the skills of advanced users, beginners have higher odds of never encountering a blocked website (OR³²: 2.6 [1.4; 4.9], $p < 0.001$); they also have higher odds to encounter blocked websites sometimes, rather than often (OR³³: 1.9 [1.04; 3.5]; $p = 0.04$).

This confirms the second hypothesis H2. The analysis confirms that the user level-of-skill positively correlates with user capability to recognize traffic monitoring and content blocking.

However, if the affordability of technology is measured on the basis of market diversity, it becomes clear that the users of some smartphone brands are more likely to

³² The odds ratio when holding other predictors in the model constant.

³³ idem

come across a blocked site than others; e.g. Blackberry users have higher odds of encountering blocked content than users of smartphones from other (non-listed) phone manufacturers (OR: 0.37 [0.15; 0.92]; $p < 0.03$) and (OR: 0.34 [0.14; 0.85] $p < 0.02$). It is not possible to simply 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).

Blackberry is widely adopted by commercial organizations which are aware of its enhanced security capabilities since it offers stronger and broader security controls to IT departments and the higher odds of encountering blocked content could therefore indicate that these controls are more commonly applied against users of Blackberry devices by their organizations.

5.3.2 Hypothesis H3

Hypothesis H3 states that a higher level of information society development contributes to greater user awareness that content blocking and monitoring is performed by state-owned agencies.

The level of significance between the independent variables on information society development and awareness of blocking/monitoring by state agencies is investigated. The awareness of monitoring by state agencies is measured through the variables listed in the sub-box on the right-hand-side outlined by a dotted line. This variable is available from the user survey.

The **dependent variable** for the second regression model was user-awareness-of-the-content-blocking-and-traffic-monitoring-implemented-by-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 user awareness of the state-imposed filtering of Internet content. The more developed the market, the higher the probability that users are aware of 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 state-imposed monitoring than those from the less developed markets.

Highlighted data from Table 5.7 (OR = 2.13 (CI = (1.38; 3.27)) and $p = 0.001$) led to the conclusion that the more developed the market, the greater the chances of an increased awareness of state-initiated filtering and monitoring.

This confirms the third hypothesis (H3). The analysis confirms that a higher level of information society development is associated with greater user awareness that content blocking and monitoring is performed by state-owned agencies.

Table 5.7: Factors associated with opinion on state role for filtering Internet content (results of multilevel binary logistic regression; reference category = non-state).

Monitoring/Blocking=>	by State		
Predictors (Reference Category)	OR	(95% CI)	p
Post-paid (pre-paid)	1.20	(0.86; 1.66)	0.285
Mobile internet yes (no)	0.70	(0.44; 1.14)	0.153
Mobile Brand			
Apple (other)	0.91	(0.46; 1.80)	0.776
Blackberry (other)	0.96	(0.42; 2.19)	0.921
HTC (other)	0.63	(0.30; 1.30)	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; 2.40)	0.535
Download at most sometimes (often)	1.22	(0.88; 1.70)	0.230
Skill level beginner (advanced)	0.76	(0.43; 1.37)	0.368
Skill level intermediate (advanced)	0.86	(0.50; 1.47)	0.572
Religion: Islam	0.97	(0.57; 1.64)	0.899
Broadband affordability	0.83	(0.56; 1.22)	0.340
Market development	2.13	(1.38; 3.27)	0.001

* OR: odds ratio; p: p-value; CI: Confidence Interval

5.3.3 Hypothesis H4

Hypothesis H4 states that users with advanced skills and those who often download content via mobile Internet trust the state-owned stakeholders less than other market players.

The second regression model is designed to provide information about the predictors associated with the **dependent** variable of the users' trust in different telecommunications market players (state-owned tele-operators (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 mobile Internet users' trust.

Data from Table 5.8 led to the conclusion that trust correlates with user skillfulness levels.

The mobile phone users who download content via mobile Internet at-most-sometimes, trust the state-owned operators more than anyone else on the list (OR: 1.58 [1.10; 2.27] $p < 0.01$).

In comparison to beginners and intermediate users, advanced mobile Internet users trust private owned organisations more than state-owned organisations (OR: 0.46 [0.21; 0.98] $p < 0.04$) and (OR: 0.52 [0.28; 1.00] $p < 0.05$) and (OR: 0.45 [0.22; 0.89] $p < 0.02$).

This analysis confirms the fourth hypothesis (H4). The analysis confirms that 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.

Table 5.8: Factors associated with opinion to whom user trust (results of multilevel multinomial logistic regression; reference category = state).

Trusted Entity => Predictors (reference category)	Nobody		Non-state		Private	
	OR (95% CI)	p	OR (95% CI)	p	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
Mobile Brand						
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; 0.80)	0.02
HTC (other)	0.97 (0.37; 2.59)	0.96	1.35 (0.48; 3.80)	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 (0.20; 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 (1.10; 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; 1.00)	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 (0.40; 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

Some differences can be observed between different smartphone brand users: e.g. Blackberry, Samsung and Nokia users trust the state-owned agencies more than other entities on the list.

5.3.3.1 State Supported Religion as a Predictor

This regression model included a variable for state-supported religion. The correlation between state religion (measured by the proportion of Muslims in the population) and user trust did not yield statistically significant results (OR: 3.05 [0.44; 20.86] $p < 0.26$) and (OR: 1.66 [0.40; 6.87] $p < 0.49$) and (OR: 2.33 [0.26; 20.61] $p < .45$). However, it is important to note 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 Muslims in the population seems to lower the odds for the state (referent category) which contributes to higher trust in the protective role of state entities. If more predominantly Muslim countries could be included the explanatory power of the results regarding the role of the religion could yield results in favour of this presumption. The third last row in Table 5.8 is highlighted and shows the results for this analysis.

5.3.4 Hypothesis H5

Hypothesis H5 states that skilled users are more likely to have jail-broken phones and to have updated the firmware on their phones on which enables them to improve their privacy protection.

The third regression model was designed to investigate the correlation between user level of skill ('user skillfulness') and users' capability to protect their privacy by uploading important security additions to the OS.

Research from Chapter 3 (Section 3.7) shows that users' with jail-broken phones, who frequently download applications and who perform firmware upgrades are expected to have the necessary skills for the installation of additional security applications, and to care more for protection of their privacy from monitoring and blocking.

Table 5.9 clearly shows that users with basic or intermediate skills are more likely to not have a jail-broken phone (OR: 2.41 [1.65; 3.54] $p < 0.001$) and (OR: 1.84 [1.41; 2.4] $p < 0.001$) and to have an un-updated firmware on their phone (OR: 3.54 [1.96; 6.39] $p < 0.001$) and (OR: 1.71 [1.001; 2.93] $p < 0.049$). We can conclude that users with advanced skills are more likely to have a jail-broken phone and to have updated the firmware on their phone. In summary less skilled users are less likely to have a jail-broken phone and are less likely to update their phone firmware, as they download applications less frequently (OR: 2.55 [1.88; 3.47] $p < 0.001$) and (OR: 2.83 [2.37; 3.37] $p < 0.001$). Therefore the skillfulness of smartphone users *positively* correlates to their ability to protect themselves against monitoring and blocking. Therefore, there is a correlation between users' skillfulness and their ability to download additional tools to improve their security.

This confirms the fifth hypothesis (H5). The analysis confirms that skilled users are more likely to have updated firmware and jail-broken phones which enables them to improve their privacy protection.

Table 5.9: Factors associated with "jail-broken" phone and updating phone firmware (results of multilevel binomial logistic regression; reference category = yes).

	Not "jail-broken" phone		Un-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

5.3.5 Hypothesis H6

Hypothesis H6 states that user tolerance of content blocking and the user trust in state-owned agencies as entities that care about their privacy are correlated with the high level of information society development, the availability of technology, and the wealth of a country. These are the independent variables determined from factor analysis.

It was possible to further explore user tolerance of state-implemented Internet content blocking and monitoring.

The descriptive charts suggested that the tolerance and acceptance levels of state censorship differ from one country to another. For this reason, a more detailed analysis of the answers to question no. 23 for each country was performed.

Question no. 23 listed 12 entities, and respondents were asked to choose from values on a Likert scale where 1= never-trust and 5= always-trust and the choices could then be ranked on a scale of trustworthiness from 1 to 12. The values were generated using the sub-of-products of the value of the Likert scale and then ranked in value. The top of the scale position (position no. 1) was reserved for the most trusted entity, while the least trusted was to be ranked twelfth. Based on users' responses, two groups of countries were identified.

The rankings of the listed entities in the question no. 23 are presented in Table 5.12 (for Azerbaijan, Belarus, Iran, Syria, Tunisia, Uzbekistan and Vietnam), Table 5.11 (for China, Oman and Saudi Arabia), and Table 5.10 (for all countries).

Table 5.10: The ranking of the entities who user's trust (all countries).

Trusted entity/User ranking in the country	Rank 1=Most trust, 12 = lowest trust
Government	12
Other	11
State Agency	10
ISP inside country	9
NGO inside	8
CSP inside	7
NGO outside	6
CSP outside	5
Personal contact outside	4
Personal contact inside	3
Software engineers	2
ISP from outside	1

The overall ranking (all countries together) is presented in Table 5.10 and further investigation suggested the highest impact was caused by users from seven countries forming the first group, who do not trust state-owned entities at all.

Group 1 includes Azerbaijan, Belarus, Iran, Syria, Tunisia, Uzbekistan and Vietnam. Their rankings are presented in Table 5.11. This table shows that Government and State Agencies were ranked very low (at 11 or 12 for Belarus, Iran, Syria, Tunisia Uzbekistan and Vietnam) and 5 and 9 for Azerbaijan.

Table 5.11: Ranking of entities whom users trust in group of seven countries.

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

Group 2 consists of three countries represented in Table 5.12. This group includes China, Oman and Saudi Arabia. It was surprising to find that although users in this group were well aware (close to 60%) of the specialized state agencies, and of Internet blocking and monitoring imposed by the national legislation and the state entities (Q22 Chart 4.32), their user communities trust their governments and believe the state-owned agencies protect their privacy and protect them from harmful content. Table 5.12 shows that China, Oman and Saudi Arabia ranked their trust in Government (at 3, 2 and 3 respectively) and state agencies (3 and 2 for Oman and Saudi Arabia respectively).

Table 5.12: Ranking of entities whom users trust in the group of three countries.

Trusted entity/User ranking (per 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
CSP 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

From the tables on GNI and mobile penetration presented in Chapter 4 we know that 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.

However, China has a much lower GNI compared to these two countries (Table 4.3). Despite this its mobile communications market is highly developed, users are skilled (Q13 Chart 4.28) and much of the technology on the market is produced at home (China has its own mobile technology manufacturers and network providers as described in Chapter 2).

The situation in Group 1 is different. Of the seven countries, the GNI in some countries (e.g., Belarus) is over twice that of the poorest states (e.g., Vietnam). The seven user communities scored lower for their trust in their governments, ranking their governments higher than 10 (except Azerbaijan), and scored lower for State Agencies, ranking them higher than 9 (except in Uzbekistan and Vietnam).

These findings confirm the sixth hypothesis (H6). The analysis confirms that user tolerance of content blocking and the user trust in state-owned agencies as entities that care about their privacy are correlated with the high level of information society development, the availability of technology, and the wealth of a country.

Findings from the regression analysis presented above were used to complete the structural model presented in Figure 5.3.

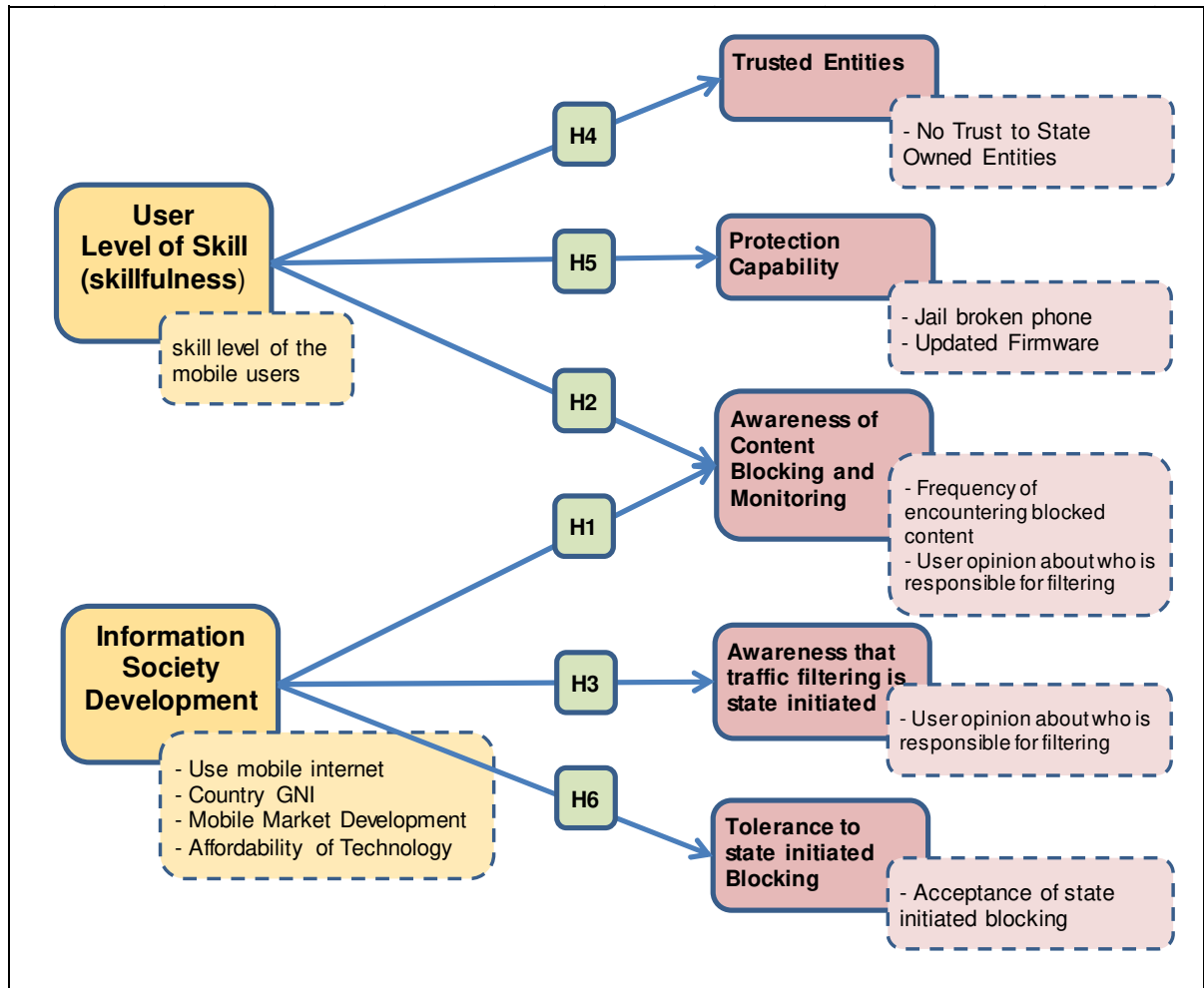


Figure 5.3: Final completed conceptual model.

Figure 5.3 shows the final structural model and all the relationships which are considered significant between the independent variables relating to User Skill and Information Society Development and the dependent variables about user awareness and tolerance of content blocking and their ability to enhance their mobile security.

The structural model shows the link between the independent variable identified as User Skill Level (User Skillfulness) with hypotheses H2, H4 and H5 to the dependent variables Trusted Entities, Protection Capability and Awareness of Content blocking and monitoring respectively.

The structural model also shows a direct link between the independent variable of Information Society Development with hypotheses H1, H3 and H6 to dependent variables Awareness of Content Blocking, Awareness that traffic filtering is state initiated and the tolerance to state initiated blocking respectively.

5.4 Discussion

5.4.1 Tolerance towards Internet Content Blocking

The general findings underline the fact that users in the 10 studied countries are aware that a wide variety of Internet content is blocked. Users often adopt circumvention solutions which are widely available to re-gain access to blocked content.

Some types of blocked content such as child abuse material (CAM) (often defined in legislation as child pornography) and hate speech are considered criminally illegal in most countries around the world. Identifying such content is complex since the definition and interpretation of what is considered hate speech or terrorist content is much broader or differently classified in different countries. However blocking other content such as religious content, foreign news channels or national news sources, as well as politically-sensitive content is less common, is problematic and is often in conflict with fundamental human rights.

The experts participating in the expert survey reported that the types of content which are filtered is not the same in all countries. Phishing and gambling are less prohibited (filtered only in three countries according to (FreedomHouse, 2013)) than the leading political, religious or adult-only content, which is filtered in all the surveyed 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 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 a low freedom score according to the Freedom House scale (FreedomHouse, 2013) but with a high level of information society development, **state control seems acceptable**.

5.4.1.1 Trust and Privacy

Some theories about the trust relationships in the electronic world point to the evident mitigation of the expected risks by the users. (Ibbott & O'Keefe, 2004) who based their theory on the work of (Gallivan & Depledge, 2003) 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 relational risk, it can be seen as an alternative to control mechanisms; i.e. partners trust the actions of each other as an alternative to specifying detailed protocols for each other's behaviour.

Studies implemented in communities in developed parts of the world where the technology is affordable, e.g. in California and Greece (Ackerman, Cranor, & Reagle, 1999; Consolvo, et al., 2005; Buchanan, Paine, Joinson, & Reips, 2007; Felt, et al., 2012b; Mylonas, Dritsas, Tsoumas, & Gritzalis, 2011) with high country scores for freedom show that user feelings about privacy are very complicated, and sometimes contradictory. Studies have shown that users are neither very attentive nor knowledgeable with regards to the presence of traffic monitoring or content blocking. When asked directly about their privacy preferences, users present themselves as very protective regarding their personal data, which is often in contradiction to their everyday actions which they practice on the telecommunications networks. This does not correspond to the user preferences found in studies of social networks (Ažderska & Blažič, 2012), which most notably point to user negligence and their lack of knowledge or understanding of privacy threats, as well as the trust between the communication parties, including the relaying party.

An additional explanation of user actions that breach their expressed preferences can be found in the user trust evidenced in our study. Users trust the regulatory agencies and state-owned telecommunications operators. The survey results from the two different groups of countries show that the more developed markets offer more affordable technology, the countries are wealthier and trust in state-related entities on the mobile networking market is higher.

5.4.1.2 Increasing Awareness of Privacy and Security Failures

Any public disclosures or revelations about traffic- or content-monitoring activities by government agencies have triggered significant negative reaction by the public in the countries with highly developed democracy. It should be noted, however, that the 2007 disclosure of the activities of the PRISM electronic surveillance of the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) (Franceschi-Bicchierai, 2014) had significant impact on users from the developed regions, and have shaken their trust in online services. According to leaked documents obtained by the Guardian newspaper, the National Security Agency PRISM programme tapped into the systems of Apple, Google, Facebook, Skype, Yahoo and other US internet giants. In June 2013, details about its existence were leaked to The Washington Post (Lee, 2013) and The Guardian (theGuardian, 2013) by Edward Snowden who was an NSA contractor. These disclosures have an influence on user privacy awareness.

The Global Report on Privacy (AVG, 2013) revealed that almost 80% of respondents were concerned about their privacy online. (GSMA, 2014) The Enjoy Safer Technology Survey (Schrott, 2012) revealed that 83% of those polled changed their social media account privacy settings over the last 6 months. (Tanner, 2013) Furthermore, the Trust Privacy Index for 2013 (Bachman, 2013; Big Brother Watch, 2013) also pointed out that 74% of Internet users voiced concerns about their privacy, and 76% were saying that they were more likely to check websites and applications for privacy certification or seals.

Users increasingly petition for reviews of existing monitoring and blocking programmes and request stricter public control over such activities.

5.4.2 Privacy Views Different Between User Communities

From the study results it is clear that the user communities in the countries with vibrant, competitive, profitable, and very developed mobile markets with strong demand for services are not significantly concerned 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 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 Saudi Arabia and the Sultanate of Oman, where users trust their governments, state agencies and the country's own ISPs. In China, the government and state agencies ranked high on the trustworthiness scale, when excluding the "Don't know" responses. When the "Don't know" responses are included, the ranking changes and commercial organizations inside and outside China are preferred rather than the government-related organizations.

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 government agencies are not trusted at all.

It follows from this analysis 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., Islam in Oman and Saudi Arabia), are not perceived as a great evil by users, and are sometimes completely unnoticed. The Kingdom of Saudi Arabia, the Sultanate of Oman and the People's Republic of China are examples of countries where users perceive content blocking as an attempt by the state to protect its people from adverse religious content or other content not aligned with their culture and the state regime. This is also what makes them different from users in the developed part of the world.

In contrast, 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.

It should be noted that the level of skill of a user that was found to differ among the user communities of the studied countries is also an important factor that influence a user's capabilities to understand the privacy threats and the need to download the necessary security tools. Skilled users from well-developed mobile markets are more capable to protect their privacy to some level and avoid monitoring and blocking by regularly updating their handsets (Mylonas, Kastania, & Gritzalis, 2013).

5.4.3 The Wealth of a Country

The wealth of the country and its citizens is a factor that influences the level of the market development, the availability and the affordability of the advanced technology. Where advanced mobile technology is present and is freely offered to citizens who can reasonably afford it, the restrictions and regulations imposed by the government, if they are aligned with the prevailing state-supported religion or type of regime, are not seen as a great evil by the users and are sometimes not even registered by the users.

The Kingdom of Saudi Arabia, The Sultanate of Oman and People's Republic of China are examples for that as the user communities in these countries understand the content blocking as a state action being done for their benefit in protecting themselves from adversary religious content or other content not aligned with their culture and the state regime. The GNI of the Sultanate of Oman and the Kingdom of Saudi Arabia are three times higher or more compared to the GNI of the other studied countries (\$25,320 for Oman and \$30,160 for Saudi Arabia), while the people of the Republic of China have a lower GNI (\$9040). However, China has one of the leading emerging markets for mobile technology, with the largest number of subscribers and national valued manufacturers. The pre-paid packets for mobile service measured as a percentage of GNI for these three countries are categorised as very affordable.

In contrast to this, when the developmental level of the mobile market is lower, and when the country and the citizens are poor (e.g., the case of Uzbekistan with \$3670 GNI, Syria with \$5120 and Vietnam with \$3620 of GNI), the market is strongly controlled and the regime is more oppressive, then the restrictions and content blocking are not accepted by the user community and distrust with respect to the government or state-owned entities is high.

From the responses to the global disclosures on widespread monitoring of internet and mobile activities by democratic governments in addition to data retention regimes in Europe, it is important to note that the wealth of a country and the affordability of technology were also found to have similar impact in nations which also have a long tradition of high protection of human rights. The level of trust was not evaluated in the current user survey but should be a focus of further research.

5.5 Findings and Conclusion

The experimental study of the most popular handsets has shown that security and privacy protection are not adequate by default and that the level of security standards applied are not appropriate.

From the study results it is clear that the user communities in the countries with vibrant, competitive, profitable, and very developed mobile markets with strong demand for services are often aware of and not significantly concerned about strong governmental regulation.

The research identified that characteristics such as user-skillfulness and country characteristics such as GNI per capita, broadband affordability and market development were associated with awareness of monitoring and blocking of the internet content. It confirmed that the same characteristics are associated with trust users put in different stakeholders to protect their privacy during mobile internet communications. It confirmed that user-skillfulness influences the user's capability to download additional tools to their smartphone to increase data protection and security.

The analysis identified the factors that influence user attitudes towards mobile privacy threats. Some countries in the 10 countries which were studied, exhibit high levels of trust in their state agencies and some are more willing to trust a wide range of alternative stakeholders. Raising the levels of skill for all users is an important strategy to enhance user support and understanding towards appropriately sanctioned, proportional mobile network monitoring and filtering by governments and state agencies.

The detailed analysis completed in this chapter provided the verification for the six hypotheses. This research is distinctive since no previous survey with subsequence detailed analysis has been conducted for these specific 10 countries. Chapter 4 provides the results of the individual national surveys and descriptive comparisons on the selected countries. Chapter 5 identified the shared trends and the differentiating factors between the selected countries. The analysis permitted detailed rigorous comparison between a unique range of selected countries across the world where modern mobile communications networks are substantially adopted by their citizens – as demonstrated by the market penetration statistics.

A structural model has been presented where all the significant relationships between the independent variables relating to user skillfulness and information society development and the dependent variables measuring user awareness and user tolerance of content blocking and their ability to enhance their mobile security. This model shows the link between the independent variable identified as user skill level (user skillfulness) with hypotheses H2, H4 and H5 to the dependent variables trusted-entities, protection-capability and awareness-of-content-blocking-and-monitoring respectively. It also shows the direct link between the independent variable of information-society-development with hypotheses H1, H3 and H6 to dependent variables awareness-of-content-blocking, awareness-that-traffic-filtering is state initiated and the tolerance to state initiated blocking respectively. The structural model provides a simple diagram to remember these links.

There is a significant role for government and state agencies in regulating and monitoring mobile operators and networks. The selected countries experience ongoing political and social change and this dissertation has provided an important baseline review of the attitude of users and stakeholders in those countries towards safety and protection in mobile networks. The mobile device ecosystem continues to evolve at a phenomenal pace and further future research will support citizenship and good governance with accountability and transparency.

The selected countries have dynamic mobile markets with increasing adoption of mobile technologies. From ITU Measuring the Information Society Report in 2017 we can see that Azerbaijan grew to 111.3% mobile market penetration in 2015. China achieved 93.2% penetration and Iran 93.4% and even countries affected by recent troubles such as Syria have grown to 62.4% penetration. However, Saudi Arabia has dropped to 129.9% penetration. The reasons behind all these changes and how they have impacted society need further research.

It is clear from this dissertation that a vibrant mobile market is supported by, and encourages, Information Society Development and citizen engagement in society. In some countries governments will need to improve the level of trust from their citizens. This can often be achieved through increased government transparency.

There is much that can be done by telecom operators and handset designers to improve security. This can include more secure access-protocols to improve:

- ongoing protections against malware infections
- increased support for two-factor identification
- increased security on stored data using on-device encryption
- network security by providing stronger and more reliable and robust implementations of virtual private network tools.

All these features should be provided in a simple-to-use interface with consistent clear graphical user interfaces which highlight risks and system failures.

Ultimately, the mobile device owner must perform a personal risk assessment and consider all aspects of daily handset use to reflect on how his/her activities can be monitored and recorded by persons with a non-beneficial interest in their activities. Awareness of potential threats and knowledge about existing tools can help in self-protection of a user's privacy and are important for mobile networking evolution in the future.

In conclusion, states and citizens have a demanding challenge facing them to achieve the complex balance needed between fundamental human rights and freedoms and the need to empower and adequately resource trusted state agencies to investigate crimes committed using mobile technologies which have significant negative impact on citizens.

Chapter 6

Conclusions

6.1 Findings

Based on the study it was possible to conclude that developing security and safety strategies for the users of mobile handsets in countries with strong regulations covering the mobile market is very complicated and is influenced by several factors. The dominating factors are the wealth of the country, the level of market development, affordability of the technology and the user skill level. With the impact of the disclosed activities of NSA PRISM program, these issues also apply to the less-restrictive regimes belonging to developed democracies. These disclosures have shown that the challenge of privacy and personal data protection for mobile handset users is relevant for all countries and not only the selected countries in the presented study.

The level of telecommunications market development, and consequently also the level of information society development, is one of the most influential indicators regarding user acceptance or rejection of state-initiated Internet content blocking and monitoring.

Performing a comprehensive risk assessment in this area in different parts of the world is a very complex task. The purpose of a risk assessment is to identify accurately and comprehensively, the potentially dangerous uses of mobile technologies. However, the present study carried out in the dissertation research has revealed that the current situation regarding the level of awareness of privacy abuse and the use of appropriate security technology tools for better privacy protection should be 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.

A single player acting in isolation on this market cannot change the current situation, since both platform-security development at the OS level, as well as circumvention application development stakeholders, have so far left some user communities outside the mainstream development goals. The collected data have shown also that the mobile OS developed by the leading global manufacturers focus largely on security features and platform security models that rely on the amount of trust placed by users in the network operators, which is the case in the most developed economies or wealthy countries with vibrant and developed markets.

There are serious concerns by IT security officers to the adoption of the BYOD paradigm relating to data security and access to corporate databases. This is now evolving into the area of BYOS (Bring Your Own Software) where the benefits are similar to the BYOD model where employees select software which they are knowledgeable about and compatible with other devices owned by the employee.

Corporate IT controls are now completely based on the development of API interfaces to corporate data which offers more opportunities for employees to select not only their preferred device but their preferred software solution. (Van Leeuwen, 2014)

The disclosure of wide-spread surveillance by the US Agency for National Security (NSA) in 2007 has shown that users from developed parts of the world are not as well protected regarding their privacy and personal data as they thought they were. Users and large companies across the world are moving their data from US service providers to service providers that assure safe email and web-hosting in countries like Norway. The Norwegian-based Runbox Company reported in June 2013 a jump in customers of 34% (Greene, Kehl, Morgua, & Bankston, 2014). Citizens have requested legal restrictions on government surveillance (European Court of Human Rights, 2015; European Commission, 2000) and for the development of hardware and services with new encryption techniques that will provide adequate user protection all over the world.

In 2014, the E.U. Commissioner for Justice, stated that “*Data Protection is made in Europe. Strong data protection rules must be Europe's trade mark. Following the U.S. data spying scandals, data protection is more than ever a competitive advantage.*” (European Commission, 2014). Strong data protection should also be a recommendation for the governments of the studied countries. (European Parliament and the Council of the European Union, 1995; Council of Europe, 1981; OECD, 1980; Ambrose & Ausloos, 2013; Hallinan, Friedewald, & McCarthy, 2012; Birnhack, 2008) Economic prosperity is strongly related to the use of ICT technology and the innovative online services connecting the world, but the positive effect of ICT is conditional on user trust. According to the economist Joseph Stiglitz “*Trust is what makes contracts, plans and everyday transaction possible, it facilitates the democratic process, from voting to law creation, and is necessary for social stability*” (Stiglitz, 2013).

The current world turmoil caused by the revelation of massive surveillance by the NSA is an opportunity for the governments of the studied countries to understand the importance of trust and to join the international efforts for the adoption of a new agreement about Internet governance that will ensure access, safety and security. According to the CEO of the Internet Corporation for Assigned Names and Numbers (ICANN), Dr. Chedade, “*We are at a time when the Internet plays a key role in economics, politics, social stability, and world peace. Unlike the early Internet period, there's heightened interest on who manages the Internet and how it is managed*” (ICANN, 2016; Chedade, 2014). A new agreement may give more sovereignty to the national management of Internet services; however, at the same time national governments should guarantee security as a part of the technological sovereignty acquired. (Rosenzweig, 2014)

A conclusion that follows from this study is that the complex environments in which mobile operators operate create challenges for government, industry and mobile users to strike the appropriate balance between sharing significant amounts of data online and protecting that data from misuse. However, in a tightly regulated market, such as the mobile market, with a limited number of operators and with a highly regulated telecommunications infrastructure, user protection is difficult to achieve.

Simultaneously with a prosperous society with well-developed services, user skills, proficiency and ICT knowledge are also very important for the development of the information society and the national economy. Smartphones and other modern mobile devices are complex computers with an increasing range of sensors and functionalities. As a consequence, users clearly need more knowledge and information to enhance their proficiency on these devices for efficient use and self-protection. In that context, an information campaign focusing on risk assessment and risk mitigation is to be welcomed by all stakeholders. Users' attention must be gained in all the studied countries for them

to understand their high-risk environments, especially when the risks and the resulting consequences cannot be completely eliminated. Further research and capacity building is required.

6.2 Research Completed

This dissertation:

1. Completed an external review of mobile operational environments in 10 selected countries which have a history of lower levels of human rights protection
2. Developed repeatable test criteria for an assessment of mobile devices in real-world scenarios
3. Implemented a laboratory based testing environment for mobile handsets to determine their strengths and weaknesses in protecting personal data and personal communications and identify known risks.
4. Developed and implemented a comprehensive survey of user attitudes to privacy and to determine a gap assessment about the level of knowledge about known risks and the level of user skills to implement risk mitigation strategies in these 10 countries
5. Developed a structural model to identify the key independent variables and the dependent variables which can provide useful correlations about the level of information society development and the user skill level relationship to the awareness of content blocking and monitoring, the tolerance to state initiated blocking and the ability of users to protect themselves

6.3 Dissertation Contributions

This dissertation investigated the area of mobile privacy and data protection for users in 10 selected countries of the world where access to the internet is important for the exercise of everyday rights such as business, entertainment and politics.

The selected countries had the necessary characteristics that enable deep analysis and evaluation of the components that influence the level of user trust to particular stakeholders in the mobile communication market. A common aspect in all the geographically dispersed countries is a regime with strong regulation of the mobile telecommunications market and a history of lower levels of human rights protection but exhibit significantly high levels of usage of mobile devices and networks. Many of these countries are active in the areas of mobile network supervision and in blocking internet content.

The scientific contributions of the dissertation are important and are part of the ICT mobile security area. The security and personal data protection risks faced by end users of mobile devices and mobile networks are clearly identified. This dissertation accurately and comprehensively identifies the potential threats of mobile technologies which are used in regions with different levels of mobile market developments and different telecommunication market regulation.

1. The research includes detailed analysis and findings about the capabilities of modern mobile devices regarding security applications that provide data and privacy protection. It also considers the availability of ease-to-use tools for circumvention of blocking systems in order to access blocked content and upload sensitive information to online services. The work of the dissertation identifies necessary system capabilities required in order to protect the personal data of mobile data users and the conflicts this causes with government national security.

The completed research provides a better understanding of the current situation, as a precursor to the adoption of new, advanced and affordable security ICT applications in the developing world. Significant difficulties were overcome to obtain information about the emerging and developing countries' perception of security and their fears about personal data privacy abuse. This is important for the development of 'off-the-shelf' protection tools. The research findings also contribute to the provision of secure network services, which are a prerequisite for the growth of the information society globally. Researchers gain a baseline analysis of inherent privacy and personal data threats and risks associated with the use of mobile technologies. It becomes clear how such issues are a design feature of the mobile ecosystem and difficult to mitigate.

2. The research includes good analysis and findings about the level of user understanding of mobile device technology, awareness about internet blocking and filtering and skill level of the approached user communities regarding protection of personal data. It identifies the challenges users are faced with state actors.

The challenges they face depend critically on the design of the hardware, the design and implementation of the operating system and the range of applications which are installed, and the regulatory environment where the mobile network operates. These properties are evaluated in semi-real and experimental environments.

The level of security provision in mobile networks depends on the skill level of the user in addition to capabilities of the hardware and software of the mobile device. This required onsite studies in different environments especially in those that were not studied and evaluated previously due to some restrictions. The dissertation determined the best tools available today to be applied by the end users for their own privacy protection in areas where end users fail to do so due to factors beyond their control. Knowledge about user attitudes and understanding of self-protection capabilities regarding privacy will be included as this provides important knowledge and research regarding future technology and market development.

3. A structural model was developed that defines the influence and the dependencies between the level of information society development, the affordability of ICT technology, user skills and the level of user protection capacity, awareness of internet blocking and filtering, awareness that these activities are initiated by the state & government and the differences regarding the tolerance toward this type of monitoring and blocking. The wealth of countries and their user communities show similar attributes as western developed countries such as the USA and Europe.

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

6.4 Future Work

Mobile markets and technologies are rapidly evolving. There is increased dependence and use of mobile data networks for mobile broadband access along with increased reliability and speed.

The survey developed should be repeated on a regular basis to determine how the markets have developed in these countries over time.

The structural model can be used to compare the results achieved in this report with the current situation and can be used to develop training strategies to improve awareness of private and data protection risks for users.

Bring-your-own-device is a very successful corporate paradigm which has turned traditional approaches to corporate IT solutions upside-down. The impact of user innovation drives the organisation to a new understanding of user-centric services and motivates the organisation to focus on data and information security whilst offering complex IT services to both employees and customers. However, the data privacy risks move to impact on users and their employers in ways outlined but only briefly explored in this dissertation. Intelligent devices including smart home thermostats, cars or home network routers are targets of malware attacks and these devices are often controlled by smartphones. The Internet of Things will bring enormous challenges to this space.

The effect of the new European Union General Data Protection Regulations on mobile data privacy issues needs further investigation since the GDPR will be the most significant change in European data privacy rules which will have global impact since companies trading with the EU must comply with these rules regardless of where they are located in the world (Heimes, 2016a; Maldoff, 2016; Heimes, 2016b).

Appendix A

User Survey

The User Survey was implemented either online using SurveyMonkey with the survey translated into the national language or directly performed by a single individual in the country. The responses were translated back into English for analysis. The data for the survey answers included in this dissertation is available on request for academic research by contacting ijis@aconite.com.

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?

PrePaid		Postpaid		Don't Know	
---------	--	----------	--	------------	--

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

Yes		No		Don't Know	
-----	--	----	--	------------	--

5. How do you access the internet on your mobile phone

Wi-Fi	
A limited bundle with my subscription	
An unlimited data bundle with my subscription	
I pay per MB/Kb of data usage	
I have no access	
Other (please specify)	

6. Who pays for your mobile phone use?

I do	
Another member of my family	
My employer	

7. Who manufactured the handset you use?

Nokia	
HTC	
Apple	
Samsung	
Blackberry	
Other (please specify)	

8. What operating system does your phone use?

Android	
---------	--

IOS	
Symbian	
Blackberry	
Windows Mobile	
Don't know	
Other (please specify)	

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

	Often	Not Very Often	Sometimes	Rarely	Never	Don't Know How
Apple App store						
Android Market						
Blackberry App World						
Windows Mobile Marketplace						
Nokia OVI (Symbian)						
Other (please specify)						

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

Often	
Sometimes	
Rarely	
Never	
Don't Know how	

11. Is your mobile phone 'jail-broken'?

Yes		No		Don't Know	
-----	--	----	--	------------	--

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

Yes		No		Don't Know	
-----	--	----	--	------------	--

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

Beginner	(email basic internet browsing)	
Intermediate	(blogging social networking online)	
Advanced	(programming web development)	

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

Often	
Sometimes	
Rarely	
Never	
Don't Know how	

15. Is your handset a smartphone?

Yes		No		Don't Know	
-----	--	----	--	------------	--

16. What do you download to your mobile handset?

	Often	Sometimes	Rarely	Never	Don't Know how

Free Apps					
Paid Apps					
Free Content					
Paid Content					
Other (please specify)					

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

	Often	Sometimes	Rarely	Never	Don't Know how
Music					
Videos					
Games					
News and Affairs					
Other (please specify)					

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

(Categorize in percentages)

Work use	
Keeping in touch with family and Friends	
Entertainment (Music, Videos, Games)	
Banking	
Other (please specify)	

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

(Categorize in percentages)

Accessing Public Information	
Communicating with Colleagues and Friends	
Accessing protected information	
Sharing potentially sensitive information regarding my country	

20. What type of content do you usually access on the Internet

(Categorize your use in percentages)

Accessing primarily text content (websites, emails)	
Accessing content with many images	
Accessing audio/visual content	
Transmitting text content (emails, social networking)	
Transmitting audio/visual content	

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

Yes		No	
-----	--	----	--

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

Legislation requiring blocking/monitoring with limited supervision?	
Specialized state agency responsible for communications supervision/regulation?	
Trained investigation teams responding to complaints only?	

Pro-active Trained Investigation teams?	
Sophisticated Communications monitoring equipment managed by trained investigation teams?	
Close Collaboration with national Internet industry?	
Commercial agreements with specialized organisations?	
Systemic pro-active monitoring, logging and analysis?	
Other (please specify)	

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

	Never	Rarely	Sometimes	Most of the Time	Always	Don't Know
Government						
State Agencies						
Communications Service Providers located inside your country? (ISP, Mobile, Telecommunications company)						
Communications Services Providers located outside your country? (ISP, Mobile, Telecommunications company)						
Non-Governmental Organisations located inside your country?						
Non-Governmental Organisations located outside your country?						
Commercial countries located inside your country?						
Commercial organisations located outside your country?						
Personal friends/contacts located in your country?						
Personal friends/contacts located outside your country?						
Software and application developers						
Other						

References

- 3GPP. (2007, Jun). *Universal Mobile Telecommunications System (UMTS): Specification of the 3GPP confidentiality and integrity algorithms Document 1: f8 and f9 specification (3GPP TS 35.201 version 7.0.0 release 7)*. Retrieved July 2017, from 3GPP: http://www.etsi.org/images/files/3GPPAlgorithms/ts_135201v070000p.pdf
- 3GPP. (2009). *International Mobile station Equipment Identities (IMEI) (Release 9)*. Retrieved May 2013, from 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects: http://www.3gpp.org/ftp/Specs/archive/22_series/22.016/22016-900.zip
- 3GPP. (2012). *Confidentiality Algorithms*. Retrieved from 3GPP: <http://www.3gpp.org/specifications/60-confidentiality-algorithms>
- 3GPP. (2015). *Generic Authentication Architecture (GAA); System description*. Retrieved from 3GPP: <http://www.3gpp.org/ftp/Specs/html-info/33919.htm>
- Ackerman, M., Cranor, L., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. *Proceedings of ACM Conference on Electronic Commerce* (pp. 1-8). ACM.
- ACPO. (2013, Feb). *Guidelines on the Safe use of the Internet and Social Media by Police Officers and Police Staff*. Retrieved Dec 13, 2015, from Association of Chief Police Officers: <http://library.college.police.uk/docs/ACPO/safe-use-of-the-Internet-Feb-2013.pdf>
- Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. *International Conference on Information Systems (ICIS)* (p. Paper 94). AIS Electronic Library (AISeL).
- Adams, A., & Sasse, M. (1999). Taming the wolf in sheep's clothing: privacy in multimedia communications. *Proceedings of the seventh ACM international conference on Multimedia (Part 1)* (pp. 101-107). ACM.
- Akuity. (2014, Mar 7). *Seven Stats About The Future of BYOD*. Retrieved Nov 30, 2015, from Akuity: <http://www.akuity.com/2014/03/17/seven-stats-about-the-future-of-byod/>
- Alexander, S., & Droms, R. (1997). *RFC2132: DHCP options and BOOTP Vendor Extensions*. USA.
- Ambrose, M., & Ausloos, J. (2013). The right to be forgotten across the pond. *Journal of Information Policy*, 3, 1-23.
- AnalogBit. (2012). *AnalogBit tcp-over-dns*. Retrieved from AnalogBit: <http://analogbit.com/software/tcp-over-dns/>
- Anderson, N. (2011, February 21). *Black ops: how HBGary wrote backdoors for the government*. Retrieved from arsTechnica: <https://arstechnica.com/tech-policy/2011/02/black-ops-how-hbgary-wrote-backdoors-and-rootkits-for-the-government/>
- Appelbaum, J. (2012). Technical analysis of the Ultrasurf proxying software. The ToR Project.

- arsTechnica UK. (2015, Dec 10). *How the smartphone changed everything; or, the rise of BYOD in the workplace*. Retrieved Dec 13, 2015, from arsTechnica UK: <http://arstechnica.co.uk/information-technology/2015/12/how-the-smartphone-changed-everything-or-the-rise-of-byod-in-the-workplace/>
- AVG. (2013, February 21). *MEF Global Privacy Report 2013*. Retrieved July 11, 2017, from AVG Press Release: <http://now.avg.com/mef-global-privacy-report-2013-highlights-consumer-need-for-transparency-in-mobile-apps/>
- Ažderska, T., & Blažič, B. (2012). Trust as an organismic trait of e-commerce systems. *Multidisciplinary Research and Practice for Information Systems*, 161-175.
- Ažderska, T., & Jerman Blažič, B. (2011). A novel systemic taxonomy of trust in the online environment. *Towards a Service-Based Internet*, 122-133.
- Ažderska, T., & Jerman-Blažič, B. (2013). A holistic approach for designing human-centric trust systems. *Systemic Practice and Action Research*, 26(5), 417-450.
- Bachman, K. (2013, November 20). *Government Report Calls For Comprehensive Privacy Law*. Retrieved July 10, 2017, from Adweek: <http://www.adweek.com/digital/government-report-calls-comprehensive-privacy-law-153996/>
- Baliga, A., Killian, J., & Iftode, L. (2007). A web based covert file system. *Proceedings of the 11th USENIX workshop on Hot topics in Operating Systems (HOTOS)* (pp. 14-21). San Diego, USA: ACM.
- Banuri, H., Alam, M., Khan, S., Manzoor, J., Ali, B., Khan, Y., . . . Zhang, X. (2012). An Android runtime security policy enforcement framework. *Personal and Ubiquitous Computing*, 16(6), 631-641.
- Bauer, M. (2005). Paranoid penguin: Linux vpn technologies. *Linux Journal*, 130, 13.
- BBC News. (2015, October 21). *Sony pays up to \$8m over employees' hacked data*. Retrieved from BBC News: <http://www.bbc.com/news/business-34589710>
- Beckett, P. (2014). BYOD - popular and problematic. *Network Security*(9), 7-9.
- Bellens, R., Vlassenroot, S., Verstraeten, D., & Guatama, S. (2011). Collecting and Processing of Crowd Behaviour Data by the use of Cell Phone Data. *18th World congress on Intelligent Transport Systems (ITS World 2011) Keeping the economy moving*. Ghent, Belgium. Retrieved from <https://biblio.ugent.be/publication/2049934/file/2049935.pdf>
- Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. *Proceedings of the Third European Conference on Computer-Supported Cooperative Work (ECSCW'93) 13-17 September 1993* (pp. 77-92). Milan, Italy: Springer Netherlands. doi:10.1007/978-94-011-2094-4_6
- Bencie, L. (2013). *Among Enemies: Counter-Espionage for the Business Traveler*. United States: D. Street Books, Mountain Lake Press.
- Big Brother Watch. (2013, June 24). *New research: Global attitudes to privacy online*. Retrieved July 11, 2017, from Big Brother Watch Blog: <https://bigbrotherwatch.org.uk/2013/06/new-research-global-attitudes-to-privacy-online/>
- Birnhack, M. (2008). The EU data protection directive: an engine of a global regime. *Computer Law & Security Review*, 24 (6), 508-520.
- Born, K., & Gustafson, D. (2010). Detecting dns tunnels using character frequency analysis. *Proceedings of the 9th Annual Security Conference*. Las Vegas, Nevada USA: arXiv preprint arXiv:1004.4358.
- Bose, A., & Shin, K. (2006). On mobile viruses exploiting messaging and bluetooth services. *Securecomm and Workshops, 2006* (pp. 1-10). IEEE.

- BT. (2017, Oct). *Child sexual abuse images*. Retrieved Oct 2017, from BT: <http://www.btplc.com/Thegroup/Ourcompany/Ourvalues/Privacyandfreeexpression/Freeexpressiononline/Childimages/index.htm>
- Buchanan, T., Paine, C., Joinson, A., & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the Association for Information Science and Technology*, 58(2), 157-165.
- Burnett, S., Feamster, N., & Vempala, S. (2010). Chipping Away at Censorship Firewalls with User-Generated Content. *USENIX Security Symposium* (pp. 463-468). Washington DC: The USENIX Association.
- Bury, S., Ishmael, J., Race, N. J., & Smith, P. (2010). Designing for social interaction with mundane technologies: issues of security and trust. *Personal and Ubiquitous Computing*, 14(3), 227-236.
- BusinessWire. (2015, Jun 23). *IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020*. Retrieved Nov 2017, from BusinessWire: <http://www.businesswire.com/news/home/20150623005073/en#.VYmhfEZB58m>
- Callanan, C., & Dries-Ziekenheiner, H. (2012). *Safety on the Line*. Retrieved July 10, 2017, from Broadcasting Board of Governors/Freedom House: <https://www.bbg.gov/wp-content/media/2012/07/Safety-on-the-Line.pdf>
- Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A., & Guerra, R. (2011). *Leaping over the firewall: A review of censorship circumvention tools*. Washington DC USA: Freedom House.
- Callanan, C., Gercke, M., De Marco, E., & Dries-Ziekenheimer, H. (2009). *Internet blocking - Balancing Cybercrime Responses in Democratic Societies*. Retrieved July 10, 2017, from Aconite Internet Solutions: http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf
- Case of Copland v. The United Kingdom, 62617/00 (ECHR April 3, 2007). Retrieved from <http://hudoc.echr.coe.int/eng?i=001-79996>
- Cellebrite. (2012). *Mobile Forensics*. Retrieved May 5, 2012, from Cellebrite: <http://www.cellebrite.com/Mobile-Forensics>
- Chehade, F. (2014). *Internet Governance*. Retrieved 07 10, 2017, from Business Korea: <http://www.businesskorea.co.kr/english/news/ict/1582-internet-governance-icann-ceo-fadi-chehade-points-korea-role-model-internet-governance>
- Cisco. (2014a, January). *Cisco 2014 Annual Security Report*. Retrieved July 10, 2017, from Cisco: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
- Cisco. (2014b, July 7). *Lawful Interception for 3GPP: Cisco Service Independent Intercept in the GGSN*. Retrieved July 10, 2017, from Cisco: <http://www.cisco.com/c/en/us/about/security-center/lawful-interception-3gpp.html>
- Clayton, R. (2006). Failures in a hybrid content blocking system. *Lecture Notes in Computer Science* 3856, 78-92.
- Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: why, when, & what people want to share. *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 81-90). Portland OR: ACM.
- Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg: Council of Europe. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/convention_en.asp

- Data Protection Commissioner. (2011). Personal Data Security Breach Code of Practice. Dublin. Retrieved from https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm
- Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314.
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 386-408.
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Washington DC: Naval Research Lab.
- Disterer, G., & Kliener, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, 9, 43-53.
- Dusi, M., Gringoli, F., & Salgarelli, L. (2008). A preliminary look at the privacy of ssh tunnels. *17th International Conference on Computer Communications and Networks, ICCCN'08* (pp. 1-7). IEEE.
- Dynamic Internet Technology. (2016). *Freigate Software Application and Technical Support*. Retrieved July 10, 2017, from Dynamic Internet Technology: <http://dit-inc.us/>
- Egyptian Chronicles. (2011, March 8). *The night the capital of Hell fell down !!*. Retrieved from Egyptian Chronicles: <http://egyptianchronicles.blogspot.si/2011/03/night-capital-of-hell-fell-down.html>
- Enck, W., Ongtang, M., & McDaniel, P. (2009). On lightweight mobile phone application certification. *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 235-245). Chicago, IL: ACM.
- ETSI. (2012). *Using cellular algorithms*. Retrieved from ETSI: <http://www.etsi.org/about/what-we-do/security-algorithms-and-codes/cellular-algorithm-licences>
- EUR-Lex. (2016, Apr 6). *General Data Protection Regulations*. Retrieved Nov 20, 2017, from EUR-Lex: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679>
- European Commission. (2000). 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued b. Brussels. Retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>
- European Commission. (2014, March 12). *Progress on EU data protection reform now irreversible following European Parliament vote*. Retrieved from European Commission: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm
- European Commission. (2016, Nov). *Article 29 Working Party*. Retrieved Nov 20, 2017, from Justice and Consumers: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- European Court of Human Rights. (2015). Reference for a preliminary ruling from High Court of Ireland (Ireland) made on 25 July 2014 – Maximillian Schrems v Data Protection Commissioner. Strasbourg. Retrieved from <http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=244813>
- European Parliament. (2008, April 10). *European Parliament resolution on cultural industries in Europe (2007/2153(INI))*. Retrieved July 12, 2017, from European

- Parliament: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN>
- European Parliament and the Council of the European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels: EUR-Lex. Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046>
- Fabian, B., Goertz, F., Kunz, S., Muller, S., & Nitzsche, M. (2010). Privately waiting—a usability analysis of the tor anonymity network. *Sustainable e-Business Management: 16th Americas Conference on Information Systems, AMCIS 2010, SIGeBIZ track*. 58, pp. 63-75. Lima, Peru: Springer-Verlag Berlin.
- Feamster, N., Balazinska, M., Harfst, G., Balakrishnan, H., & Karger, D. (2002). Infranet: Circumventing Web Censorship and Surveillance. *USENIX Security Symposium*, (pp. 247-262).
- Feamster, N., Balazinska, M., Wang, W., Balakrishnan, H., & Karger, D. (2003). Thwarting web censorship with untrusted messenger discovery. *Privacy Enhancing Technologies*, 2760, pp. 125-140.
- Feilner, M. (2006). *OpenVPN: Building and integrating virtual private networks*. Packt Publishing Ltd.
- Felt, A., Egelman, S., & Wager, D. (2012a). I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 33-44). Raleigh, North Carolina, USA: ACM.
- Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012b). Android permissions: User Attention, Comprehension, and Behavior. *Proceedings of the eighth Symposium On Usable Privacy and Security (SOUPS)* (p. 3). Washington DC USA: ACM.
- Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G., & Mehes, A. (2007). Can you infect me now?: malware propagation in mobile phone networks. *Proceedings of the 2007 ACM Workshop On Recurring Malcode (WORM'07)* (pp. 61-68). Alexandria, Virginia, USA: ACM.
- Forbes Magazine. (2012, Feb 16). *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*. Retrieved from Forbes Technology: <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>
- Franceschi-Bicchierai, L. (2014, April 23). *NSA Finally Reveals How PRISM Works, But It's Nothing New*. Retrieved from Mashable: <http://mashable.com/2014/04/22/nsa-prism-report>
- FreedomHouse. (2013). *Freedom on the Net 2013*. Washington DC USA: FreedomHouse. Retrieved from FreedomHouse.
- F-Secure. (2004). *Bluetooth-Worm:SymbOS/Cabir*. Retrieved July 12, 2017, from F-Secure: <https://www.f-secure.com/v-descs/cabir.shtml>
- F-Secure. (2005a, January). *Trojan:SymbOS/Skulls.A Threat Description*. Retrieved July 11, 2017, from F-Secure: <https://www.f-secure.com/v-descs/skulls.shtml>
- F-Secure. (2005b, April). *Worm:SymbOS/Mabir.A Threat Description*. Retrieved July 11, 2017, from F-Secure: <https://www.f-secure.com/v-descs/mabir.shtml>
- F-Secure Labs. (2011, March 8). *Egypt, FinFisher Intrusion Tools and Ethics*. Retrieved from F-Secure Labs: <https://www.f-secure.com/weblog/archives/00002114.html>
- Gallivan, M., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, 13(2), 159-190.

- Gartner. (2013). *Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes*. Retrieved Nov 30, 2015, from Gartner: <http://www.gartner.com/newsroom/id/2466615>
- Gartner. (2016, Nov 29). *Gartner Survey Shows That Mobile Device Adoption in the Workplace Is Not Yet Mature*. Retrieved Nov 20, 2017, from Gartner: <https://www.gartner.com/newsroom/id/3528217>
- Gasser, U., Heacock Jones, R., Faris, R., Roberts, H., & Zuckerman, E. (2011). *Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge and Practice*. Cambridge MA USA: Berkman Center.
- G-Data. (2015, Jul 1). *G DATA Releases Mobile Malware Report for the First Quarter of 2015*. Retrieved Dec 13, 2015, from G Data Software AG: <https://secure.gd/dl-us-mmwr201501>
- Gebauer, J., & Shaw, M. (2004). Success Factors and impacts of mobile business applications: results from a mobile e-procurement study. *International Journal of Electronic Commerce*, 8(3), 19-42.
- Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 27(1), 51-90.
- Gold, S. (2011). Cracking GSM. *Network Security*, 2011(4), 12-15.
- Grace, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). Riskranker: scalable and accurate zero-day android malware detection. *Proceedings of the 10th international conference on Mobile Systems, Applications, and Services (MobiSys'12)* (pp. 281-294). Low Wood Bay, Lake District, UK.: ACM.
- Greene, R., Kehl, D., Morgua, R., & Bankston, K. (2014, July 29). *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*. Retrieved July 11, 2017, from Open technology Institute: <https://www.newamerica.org/oti/policy-papers/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/>
- GSMA. (2000). *GSM Association Specification for A5/3 - Technical Specification*. Retrieved May 2013, from 3GPP: http://www.3gpp.org/ftp/tsg_sa/wg3_security/tsgs3_13_yokohama/docs/pdf/s3-000362.pdf
- GSMA. (2011, Jul 27). *IMEI Allocation and Approval Guidelines*. Retrieved May 2013, from GSMA: <http://www.gsma.com/newsroom/wp-content/uploads/2012/03/ts0660tacallocationprocessapproved.pdf>
- GSMA. (2014, Feb). *Mobile Privacy: Consumer Research insights and considerations for policymakers*. Retrieved July 11, 2017, from GSMA: https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf
- Guardian Project. (2012). *Guardian Project*. Retrieved July 11, 2017, from The Guardian Project: <https://guardianproject.info/>
- Guardster. (2012). *Welcome to Guardster - Your Privacy Headquarters*. Retrieved July 11, 2017, from Welcome to Guardster: <http://www.guardster.com/>
- Guo, C., Wang, H., & Zhu, W. (2004). Smart-phone attacks and defenses. *Third Workshop on Hot topics in Networks (HotNets III)*. San Diego, CA USA: ACM.
- Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, 28, 263-272.

- Hansen, F. (1972). Consumer choice behavior: a cognitive theory. In F. Hansen, *Consumer choice behavior: a cognitive theory* (pp. 493-538.). New York: Free Press.
- Heimes, R. (2016a). *Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification*. Retrieved Dec 2, 2016, from The International Association of Privacy Professionals: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/>
- Heimes, R. (2016b). *Top 10 operational impacts of the GDPR: Part 5 - Profiling*. Retrieved Dec 2, 2016, from The International Association of Privacy Professionals: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling/>
- Hone, T., & Creutzburg, R. (2011). iPhone forensics: A practical overview with certain commercial software. *SPIE Defense, Security, and Sensing, 80630M-80630M*.
- Houses of the Oireachtas. (1988). Data Protection Act, 1988. Dublin. Retrieved from <http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/html>
- Houses of the Oireachtas. (2003). Data Protection (Amendment) Act 2003. Dublin. Retrieved from <http://www.irishstatutebook.ie/2003/en/act/pub/0006/>
- Howarth, P., Cameron, J., & Gillham, M. (2012). *Poptop - The PPTP Server for Linux*. Retrieved July 11, 2017, from Sourceforge: <http://poptop.sourceforge.net/>
- HP. (2015). *HP Touchpoint Manager*. Retrieved Dec 13, 2015, from HP: <http://www8.hp.com/us/en/solutions/touchpoint-manager/overview.html>
- Huawei. (2017). <http://www.huawei.com/worldwide/index.htm>. Retrieved July 2017, from Huawei: <http://www.huawei.com/en/about-huawei>
- Hypponen, M. (2006). Malware goes mobile. *Scientific American*, 295(5), pp. 70-77.
- Ibbott, C., & O'Keefe, R. (2004). Trust, planning and benefits in a global interorganizational system. *Information Systems Journal*, 14(2), 131-152.
- IBM. (2016, Apr 5). *IBM MaaS360 (SaaS)*. Retrieved Jul 14, 2017, from IBM: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=897/ENUS216-152&infotype=AN&subtype=CA>
- ICANN. (2016, January 5). *ICANN CEO Fadi Chehade on Internet governance & balancing security, innovation, and privacy*. Retrieved July 10, 2017, from The Prospect Group: <http://www.theprospectgroup.com/icann-ceo-fadi-chehade-internet-governance-balancing-security-innovation-privacy-82299/>
- Internet Society. (2013, December 15). *Internet Society 2013 Annual Report*. Retrieved July 11, 2017, from Internet Society: <https://www.internetsociety.org/publications/internet-society-2013-annual-report>
- Internet Society. (2015). *Global Internet Report 2015*. Retrieved Nov 20, 2017, from Internet Society: <https://www.internetsociety.org/globalinternetreport/2015/>
- Internet Society. (2016, 2017). *Global Internet Report 2016*. Retrieved Nov 20, 2017, from Internet Society: <https://www.internetsociety.org/globalinternetreport/>
- Internet Systems Consortium. (2012, June). *ISC DHCP*. Retrieved July 11, 2017, from Internet Systems Consortium: <https://www.isc.org/downloads/dhcp/>
- INTERPOL. (2017, Oct). *Access blocking*. Retrieved Oct 2017, from INTERPOL: <https://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking>
- ITU. (2005). *Structure of the land mobile global title for the signalling connection control part (SCCP)*. Retrieved May 2013, from ITU-T Recommendations: <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=7433&lang=en>
- ITU. (2008). *Study Group 2 E.212 - International Identification Plan for Mobile Terminals and Mobile Users*. Retrieved May 2013, from ITU: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9300&lang=en>

- ITU. (2012). *Measuring the Information Society 2012*. Retrieved July 12, 2017, from ITU: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf
- ITU. (2013, October 7). *Measuring the Information Society Report 2013*. Retrieved July 11, 2017, from ITU: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx>
- ITU Broadband Commission for Digital Development. (2013a, July). *Why National Broadband Plans Matter - Broadband Commission*. Retrieved July 10, 2017, from ITU Broadband Commission for Digital Development: www.broadbandcommission.org/documents/reportNBP2013.pdf
- ITU Broadband Commission for Digital Development. (2013b, September). *A 2013 report - Broadband Commission*. Retrieved July 10, 2017, from ITU Broadband Commission for Digital Development: www.broadbandcommission.org/documents/bb-annualreport2013.pdf
- Jamaluddin, J., Zotou, N., Edwards R., & Coulton, P. (2004). Mobile phone vulnerabilities: a new generation of malware. *Consumer Electronics 2004 IEEE International Symposium* (pp. 199-202). IEEE.
- JISC. (2015a, October 9). *Your staff, mobile devices, law and liability*. Retrieved December 12, 2015, from JISC: <https://www.jisc.ac.uk/guides/your-staff-mobile-devices-law-and-liability>
- JISC. (2015b, October 9). *Risk, liability and mobile devices*. Retrieved December 12, 2015, from JISC: <https://www.jisc.ac.uk/guides/risk-liability-and-mobile-devices>
- Joinson, A., Reips, U., Buchanan, T., & Schofield, C. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25(1), 1-24.
- Kargl, F., Lawrence, E., Fischer, M., & Lim, Y. Y. (2008). Security, privacy and legal issues in pervasive ehealth monitoring systems. *7th International Conference on Mobile Business*, (pp. 296-304).
- Karlin, J., Ellard, D., Jackson, A., Jones, C., Lauer, G., Mankins, D., & Strayer, W. (2011). Decoy Routing: Toward Unblockable Internet Communication. *FOCI'11 - Proceedings of the USENIX Workshop on Free and Open Communications on the Internet*. San Francisco, CA, USA.
- Kelley, S. (2008). Dnsmasq. Retrieved May 5, 2012, from <http://www.dd-wrt.com>
- Kingpin, K., & Mudge, M. (2001). Security analysis of the palm operating system and its weaknesses against malicious code threats. *Proceedings of the 10th conference on USENIX Security Symposium*. 10, pp. 1-18. Washington, D.C., USA: USENIX Association.
- Kravets, D. (2011, June 3). *U.N. Report Declares Internet Access a Human Right*. Retrieved July 11, 2017, from Wired: <https://www.wired.com/2011/06/internet-a-human-right/>
- Lee, T. (2013, June 12). *Here's everything we know about PRISM to date*. Retrieved from The Washington Post: <https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/>
- Levine, B., & Shields, C. (2002). Hordes: a multicast based protocol for anonymity. *Journal of Computer Security*, 10(3), 213-240.
- Liang, T., & Yeh, Y. (2011). Effect of use contexts on the continuous use of mobile services: the case of mobile games. *Personal and Ubiquitous Computing*, 15(2), 187-196.
- Lo, C., & Chen, Y. (1999). Secure communication mechanisms for GSM networks. *IEEE Transactions on Consumer Electronics*, 45(4), 1074-1080.

- Maitland, C., Thomas, H., & Tchouakeu, L. (2012). Internet censorship circumvention technology use in human rights organizations: an exploratory analysis. *Journal of Information Technology*, 27(4), 285-300.
- Maldoff, G. (2016). *Top 10 operational impacts of the GDPR: Part 3 – consent*. Retrieved Dec 2, 2016, from The International Association of Privacy Professionals: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/>
- Manning, M., Gomes, A., & Rahimi, A. (2014, Aug 22). *Psiphon Security Assessment*. Retrieved July 11, 2017, from Psiphon Inc: <https://psiphon.ca/assets/Psiphon-3-iSEC-Partners-v1.1-08-2014.pdf>
- Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the ‘right to be forgotten’. *Computer Law & Security Review*, 29(3), 229-235.
- MarketsandMarkets. (2014, April). *Global Advancements, Market Forecast and Analysis (2014 – 2019)*. Retrieved Nov 11, 2015, from MarketsandMarkets: <http://marketsandmarkets.com/Market-Reports/enterprise-mobility-334.html>
- McAfee. (2016, Mar 1). *Mobile Threats Report: What’s on the Horizon for 2016*. Retrieved Nov 20, 2017, from McAfee: <https://securingtomorrow.mcafee.com/consumer/mobile-security/mobile-threats-report-whats-on-the-horizon-for-2016/>
- McIntyre, T. (2011). *Child abuse images and cleanfeeds: Assessing internet blocking systems*. Cheltenham, UK: Ian Brown, ed., Research Handbook on Governance of the Internet. Retrieved from http://researchrepository.ucd.ie/bitstream/handle/10197/7594/Child_abuse_images_and_Cleanfeeds.pdf?sequence=1
- Membrey, P., Verhoeven, T., Angenendt, R., de Bruijn, B., & Singh, K. (2009). *The definitive guide to Centos*. Apress.
- Microsoft. (2015, Jul 15). *Microsoft’s PhotoDNA: Protecting children and businesses in the cloud*. Retrieved Oct 2017, from Microsoft Digital Cybercrime Center: <https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/>
- Mirkovic, J., Benzel, T., Faber, T., Braden, R., Wroclawski, J., & Schwab, S. (2010). The DETER project: Advancing the science of cyber security experimentation and test. *2010 IEEE International Conference Technologies for Homeland Security (HST)* (pp. 1-7). Boston Waltham, MA, USA: IEEE.
- MobileIron. (2017, Oct). *MobileIron – The Leader in Enterprise Mobility Management*. Retrieved Oct 2017, from MobileIron: MobileIron
- Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*, 5-8.
- Mylonas, A., Dritsas, S., Tsoumas, B., & Gritzalis, D. (2011). Smartphone security evaluation The malware attack case. *2011 Proceedings of the International Conference Security and Cryptography (SECRYPT)* (pp. 25-36). Seville, Spain: IEEE.
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47-66.
- Mylonas, A., Meletiadiis, V., Mitrou, L., & Gritzalis, D. (2013). Smartphone sensor data as digital evidence. *Computers & Security*, 38, 51-75.
- Mylonas, A., Theoharidou, M., & Gritzalis, D. (2013). Assessing privacy risks in android: A user-centric approach. *International Workshop on Risk Assessment and Risk-driven Testing* (pp. 21-37). Istanbul, Turkey: Springer.

- National Criminal Justice Reference Service (NCJRS). (2012, July). *Cellebrite UFED, Version 1.1.7.6 Evaluation Report*. Retrieved July 11, 2017, from National Criminal Justice Reference Service (NCJRS): <https://www.ncjrs.gov/App/AbstractDB/AbstractDBDetails.aspx?id=261660>
- O'Connor, B. (2006). *Vulnerabilities in Not-So Embedded Systems*. Retrieved December 12, 2015, from Black Hat Conference: <http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-OConnor.pdf>
- OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD. Retrieved from <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>
- OpenNet Initiative (ONI). (2012, June). *Research*. Retrieved July 11, 2017, from OpenNet Initiative (ONI): <https://opennet.net/research>
- Openswan. (2012, April). *Welcome to Openswan*. Retrieved July 11, 2017, from Openswan: <https://www.openswan.org/>
- OpenVPN Technologies. (2012, May). *OpenVPN*. Retrieved July 11, 2017, from OpenVPN Technologies, Inc: <https://openvpn.net/>
- OpenWrt. (2012, May). *OpenWrt*. Retrieved July 11, 2017, from OpenWrt: <https://openwrt.org/>
- Oxygen Forensics. (2012). *Oxygen Forensics*. Retrieved July 11, 2017, from Oxygen Forensics: <https://www.oxygen-forensic.com/en/download/documentation>
- Price, B., Adam, K., & Nuseibeh, B. (2005). Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies*, 63(1), 228-253.
- Ramsay, M. (2000). PoPToP, a Secure and Free VPN Solution. *Linux Journal*, 74es, 7.
- Research in Motion (RIM). (2012). *Company History*. Retrieved July 11, 2017, from Research in Motion (RIM): https://www.blackberry.com/select/get_the_facts/pdfs/rim/rim_history.pdf
- Reuters. (2015, Oct 20). *Sony to pay up to \$8 million in 'Interview' hacking lawsuit*. Retrieved from Reuters: <http://www.reuters.com/article/2015/10/20/us-sony-cyberattack-lawsuit-idUSKCN0SE2JI20151020>
- Romer, H. (2014). Best Practices for BYOD security. *Computer Fraud and Security*, 13-15.
- Rosenzweig, P. (2014, Jan 13). The Continuing Struggle for Control of Cyberspace - and The Deterioration of Western Influence. *LAWFARE*. Retrieved from <https://www.lawfareblog.com/continuing-struggle-control-cyberspace-and-deterioration-western-influence>
- Roskowski, S., Kolm, D., Ruf, M., Jaquet, J., & Othmer, K. (2009, October 27). *Patent No. 7609650 B2*. US. Retrieved from <https://www.google.com/patents/US7609650>
- Saltaformaggio, B., Choi, H., Johnson, K., Kwon, Y., Zhang, Q., Zhang, X., . . . Qian, J. (2016). Eavesdropping on Fine-Grained User Activities Within Smartphone Apps Over Encrypted Network Traffic. *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. USENIX Association.
- Samsung. (2015, Feb 10). *Samsung Smart TVs Do Not Monitor Living Room Conversations*. Retrieved Dec 13, 2015, from Samsung: <http://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations>
- Schmidt, A., Schmidt, H., Batyuk, L., Clausen, J., Camtepe, S., Albayrak, S., & Yildizli, C. (2009). Smartphone malware evolution revisited: Android next target?. *4th*

- International Conference on Malicious and Unwanted Software (MALWARE)* (pp. 1-7). Montreal, Quebec, Canada: IEEE.
- Schrott, U. (2012, December 11). *Trends for 2013: Astounding growth of mobile malware*. Retrieved July 10, 2017, from ESET Ireland: <https://blog.eset.ie/2012/12/11/trends-for-2013-astounding-growth-of-mobile-malware/>
- SELinux Project. (2013, May 12). *SELinux Project Wiki*. Retrieved July 11, 2017, from SELinux Project: https://selinuxproject.org/page/Main_Page
- Serpanos, D., & Lipton, R. (2001). Defense against man-in-the-middle attack in client-server systems. *Proceedings of Sixth IEEE Symposium on Computers and Communications* (pp. 9-14). Hammamet, Tunisia: IEEE.
- Smart, J., Tedeschi, K., Meakins, D., Hannay, P., & Bolan, C. (2008). Subverting national internet censorship-an investigation into existing tools and techniques. *Proceedings of the 6th Australian Digital Forensics Conference* (p. 52). Perth, Western Australia: Edith Cowan University.
- Sophos. (2015, Oct 30). *"Hell No Barbie" social media campaign targets Mattel's talking toy*. Retrieved Dec 13, 2015, from Naked Security by Sophos: <https://nakedsecurity.sophos.com/2015/10/30/hell-no-barbie-social-media-campaign-targets-mattels-talking-toy/>
- StatCounter. (2012). *StatCounter GlobalStats*. Retrieved July 11, 2017, from StatCounter: <http://gs.statcounter.com/>
- Stiglitz, J. (2013, December 12). *In No One We Trust*. Retrieved from New York Times: <https://opinionator.blogs.nytimes.com/author/joseph-e-stiglitz/>
- Straub, D., & Nance, W. (1988). Uncovering and disciplining computer abuse: organizational responses and options. *Information Age*, 10(3), 151-156.
- Straub, D., & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.
- Syntonic. (2016, Jun). *Syntonic 2016 Employer Report: BYOD Usage in the Enterprise*. Retrieved Nov 20, 2017, from Syntonic: <https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf>
- Tanner, A. (2013, November 13). *Users More Savvy About Social Media Privacy Than Thought, Poll Finds*. Retrieved July 11, 2017, from Forber Tech: <https://www.forbes.com/sites/adamtanner/2013/11/13/users-more-savvy-about-social-media-privacy-than-thought-poll-finds/>
- TCPDump & LibPCap. (2012). *TCPDump & LibPCap*. Retrieved July 11, 2017, from TCPDump & LibPCap: <http://www.tcpdump.org/>
- The New York Times. (2012, Feb 16). *How Companies Learn Your Secrets*. Retrieved from The New York Times Magazine: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp
- the Register. (2015, Feb 19). *Hello Barbie: Hang on, this Wi-Fi doll records your child's voice?* Retrieved Dec 13, 2015, from the Reigster: http://www.theregister.co.uk/2015/02/19/hello_barbie/
- The Telegraph. (2015, Feb 9). *Samsung SmartTV customers warned personal conversations may be recorded*. Retrieved Dec 13, 2015, from The Telegraph: <http://www.telegraph.co.uk/news/shopping-and-consumer-news/11399677/Samsung-SmartTV-customers-warned-personal-conversations-may-be-recorded.html>

- The ToR Project. (2012). *Orbot: Proxy with Tor*. Retrieved July 11, 2017, from Google Play:
<https://play.google.com/store/apps/details?id=org.torproject.android&hl=en>
- theGuardian. (2013, November 1). *NSA Prism program slides*. Retrieved from theGuardian:
<https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>
- theGuardian. (2015, Feb 27). *Samsung's voice-recording smart TVs breach privacy law, campaigners claim*. Retrieved Dec 13, 2015, from theGuardian:
<http://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim>
- Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A risk assessment method for smartphones. *Information security and privacy research*, 443-456.
- Thielens, J. (2013, Aug). Why APIs are central to a BYOD security strategy. *Network Security, 2013*(8), 5-6.
- Toyssy, S., & Helenius, M. (2006). About malicious software in smartphones. *Journal in Computer Virology*, 2(2), 109-119.
- UltraReach Internet Corp. (2012, May). *Ultrasurf - Privacy, Security, Freedom*. Retrieved July 11, 2017, from UltraSurf: <https://ultrasurf.us/>
- United Nations Humans Rights Council. (2011, May 16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. Retrieved July 11, 2017, from United Nations :
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- United States Government Accountability Office. (2013, September). *Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*. Retrieved July 10, 2017, from United States Government Accountability Office:
<http://www.gao.gov/assets/660/658151.pdf>
- UpsideOut. (2012). *Protect yourself online with our anonymous proxy service*. Retrieved July 11, 2017, from Proxify: <https://proxify.com/>
- US Federal Bureau of Investigation. (2017, July 11). *Safety and Security for the Business Professional Traveling Abroad*. Retrieved July 11, 2017, from US Federal Bureau of Investigation:
<https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view>
- Van Leeuwen, D. (2014). Bring your own software. *Network Security*(3), 12-13.
- Variety. (2015, March 3). *Sony Ex-Employees File Amended Class Action Suit Over Hacking Attack*. Retrieved from Variety: <http://variety.com/2015/biz/news/sony-hack-scandal-lawsuit-1201445372/>
- Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)*. 50, pp. 511-516. Elsevier.
- Vlassenroot, S., Gillis, D., Bellens, R., & Gautama, S. (2015). The use of smartphone applications in the collection of travel behaviour data. *International Journal of Intelligent Transportation Systems Research*, 13(1), 17-27.
- VMware. (2017, Sep). *VMware Airwatch*. Retrieved Oct 14, 2017, from VMware:
<https://www.air-watch.com/solutions/mobile-device-management/>
- Wang, Y., Streff, K., & Raman, S. (2012a). Security threats and analysis of security challenges in smartphones. *Computer*, 45(12), 52-58. doi:10.1109/MC.2012.288
- Wang, Y., Streff, K., & Raman, S. (2012b). Smartphone security challenges. *Computer*, 45(12), 0052-58.

- West, D. (2012). How mobile devices are transforming healthcare. *Issues in technology innovation*, 18(1), 1-11.
- Wired Magazine. (2014, March 12). *Sony Got Hacked Hard: What We Know and Don't Know So Far*. Retrieved from Wired: <http://www.wired.com/2014/12/sony-hack-what-we-know/#slide-1>
- Wireshark Foundation. (2012, June). *Wireshark - network protocol analyzer*. Retrieved July 11, 2017, from Wireshark: <https://www.wireshark.org/>
- Wong, R. (2011). Data protection: The future of privacy. *Computer law & security review*, 27(1), 53-57.
- Wouters, P., & Bantoft, K. (2006). *Building and Integrating Virtual Private Networks with Openswan: Learn from the Developers of Openswan how to Building Industry-standard, Military-grade VPNs and Connect Them with Windows, Mac OS X, and Other VPN Vendors*. Packt Publishing Ltd.
- Wustrow, E., Wolchok, S., Goldberg, I., & Halderman, J. (2011). Telex: Anticensorship in the Network Infrastructure. *20th USENIX Security Symposium* (pp. 459-474). San Francisco CA USA: The USENIX Association.
- Yan, Z., Liu, C., Niemi, V., & Yu, G. (2013). Exploring the impact of trust information visualization on mobile application usage. *Personal and Ubiquitous Computing*, 17(6), 1295-1313. doi:DOI 10.1007/s00779-013-0636-4
- Zafar, H., & Clark, J. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, 24(1), 34.
- Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. (Elsevier, Ed.) *Computers & Security*, 55, 81-99.
- Zhou, Y., & Jiang, X. (2012). Dissecting android malware: Characterization and evolution. *2012 IEEE Symposium on Security and Privacy (SP)* (pp. 95-109). San Francisco CA USA: IEEE.
- Zhou, Y., Wang, Z., Zhou, W., & Jiang, X. (2012). Hey, you, get off of my market: detecting malicious apps in official and alternative android markets. *19th Annual Network & Distributed System Security Symposium*. 25, pp. 2017-2023. San Diego CA USA: ISOC.
- Zittrain, J., & Edelman, B. (2002). *Documentation of internet filtering in Saudi Arabia* Harvard Law School. Retrieved from <http://cyber.law.harvard.edu/filtering/saudiarabia/>
- ZTE. (2017). *ZTE*. Retrieved July 2017, from ZTE: <http://www.zte.com.cn/global/>

Bibliography

Publications Related to the Thesis

Journal Articles

- Callanan, C., & Jerman-Blažič, B. (2014). User understanding of privacy in emerging mobile markets. *IEEE technology & society magazine*, 33(4), 48-56.
- Callanan, C., Jerman-Blažič, B., & Jerman-Blažič, A. (2016). User awareness and tolerance of privacy abuse on mobile internet : an exploratory study. *Telematics and informatics : an international journal on telecommunications & information*, 33(1), 109-128.
- Callanan, C., Jerman-Blažič, B., & Jerman-Blažič, A. (2016). User tolerance of privacy abuse on mobile Internet and the country level of development. *Information development : the international journal for librarians, archivists and information*, 32(3), 728-750.

Conference Paper

- Callanan, C., Dries-Ziekenheiner, H., & Jerman-Blažič, B. (2013). Empirical assessment of data protection and circumvention tools availability. *The Second International Conference on Cyber Security, Cyber Peace Fare and Digital Forensic, CyberSec*, (pp. 206-220). Kuala Lumpur, Malaysia.

Published Books

- Callanan, C., & Jerman-Blažič, B. (2016). *User tolerance for privacy abuse on mobile internet*. LAP Lambert. ISBN-13: 978-3-330-01757-3 EAN: 9783330017573.

Reports

- Callanan, C., & Dries-Ziekenheiner, H. (2012). *Safety on the Line*. Washington DC: FreedomHouse. url: <https://freedomhouse.org/sites/default/files/Safety%20on%20the%20Line.pdf>
- Callanan, C., DeMarco, E., Dries-Ziekenheiner, H., & Gercke, M. (2009). *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies*. London: Open Society Institute.
- Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A., & Guerra, R. (2011). *Leaping over the firewall: A review of censorship circumvention tools*. Washington DC: FreedomHouse.

Other Publications

- Callanan, C., & Gercke, M. (2008, June 25). *Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines*. Retrieved July 17, 2017, from Council of Europe Project on Cybercrime: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-wgSTUDY_25June2008.pdf
- Jerman-Blažič, B., Klobučar, T., Vermeersch, E., Bosco, F., Wells, D., Brewster, B., et al. (2015). Research Agenda Items for Fight against cybercrime and cyberterrorism. COBISS.SI-ID: 29004327 IJS delovno poročilo
- Tropina, T., & Callanan, C. (2015). *Self-and Co-regulation in Cybercrime, Cybersecurity*. Heidelberg: Springer International Publishing.

Biography

The author of this dissertation Cormac Callanan holds a B.A. (Mod) in Computer Science and MSc (Computer Design) from the University of Dublin, Ireland and an MSc from Edinburgh Napier University in Advanced Security and Digital Forensics. He has provided training at Interpol and Europol and to law enforcement agencies around the world on the subject of emerging and developing technologies, cybercrime and the role of internet industry in combating cybercrime. He is a member of the Irish Internet Safety Advisory Committee to the Irish Department of Justice.

He owns/operates an independent consultancy company from Dublin, Ireland called Aconite Internet Solutions (www.aconite.com) which provides expertise in policy development in the specialty area of international cybercrime and Internet security & safety.

He has over 30 years working experience on international computer networks and 25 years' experience in the policy area of illegal content and cybercrime activities on the Internet. He was co-author of the Council of Europe Guidelines on Cooperation between Law Enforcement and Internet Service Providers quoted by the European Court of Human Rights as achieving the appropriate balance between sharing data and data protection.

He has presented 150+ seminars on data sharing and industry cooperation at international events in over 50 countries on behalf of COE, OSCE, EC, ERA and UNODC targeting Government, Law Enforcement, Industry, Judiciary, Prosecutors and NGO.

Cormac Callanan was past-president and CEO of INHOPE – the International Association of Internet Hotlines (www.inhope.org) dealing with illegal internet content. INHOPE facilitates and co-ordinates the work of Internet hotlines responding to illegal use and content on the Internet.

Cormac was founding Chairman of the Internet Service Provider Association of Ireland (www.ispai.ie) in 1997 which he led for 5 years and served as Secretary General of the European Service Provider Association (www.euroispa.org). He was founding Director of the Irish www.hotline.ie service responding to reports about illegal child pornography and hate speech on the Internet.

