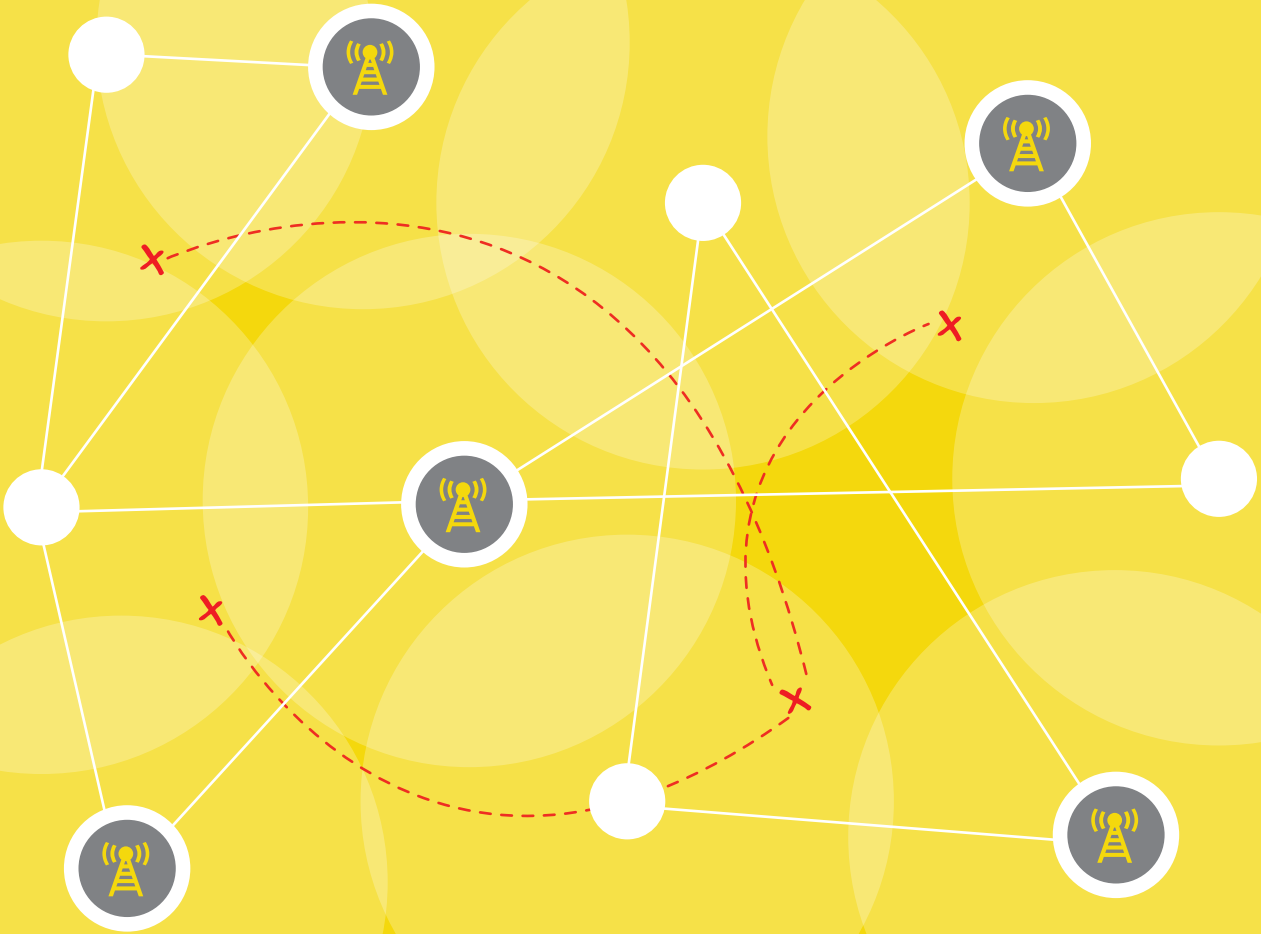
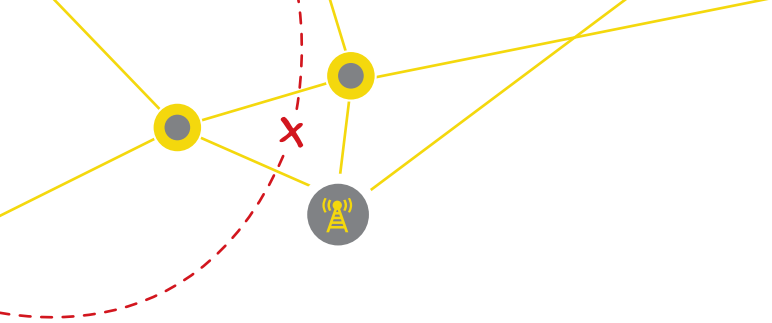
Safety on the Line

Exposing the myth of mobile communication security

Prepared by:
Cormac Callanan
Hein Dries-Ziekenheiner

Supported by:
Freedom House and
Broadcasting Board of Governors





This report has been prepared within the framework of Freedom House/Broadcasting Board of Governors funding. The views expressed in this document do not necessarily reflect those of Freedom House nor those of the Broadcasting Board of Governors.

July 2012

Contacts

FOR FURTHER INFORMATION PLEASE CONTACT:

Mr. Cormac Callanan
Email: safetyontheline@aconite.com

Mr. Hein Dries-Ziekenheiner
Email: safetyontheline@vigilo.nl

Authors

CORMAC CALLANAN
IRELAND

Cormac Callanan is director of Aconite Internet Solutions (www.aconite.com), which provides expertise in policy development in the area of cybercrime and internet security and safety.

Holding an MSc in Computer Science, he has over 25 years working experience on international computer networks and 10 years experience in the area of cybercrime. He has provided training at Interpol and Europol and to law enforcement agencies around the world. He has worked on policy development with the Council of Europe and the UNODC.

In 2008 he completed a study of best practice guidelines for the cooperation between service providers and law enforcement against cybercrime (www.coe.int/cybercrime). In 2009 he produced the 2Centre (Cybercrime Centres of Excellence Network for Training Research and Education) study profiling international best practices for IT forensics training to law enforcement (www.2centre.eu).

Cormac was president and CEO of INHOPE – the International Association of internet Hotlines (www.inhope.org) – co-ordinating the work of internet hotlines responding to illegal use/content on the internet. He co-authored the first INHOPE Global Internet Trend report in 2007, a landmark publication on internet child pornography. He also served president of the board of the European Internet Service Providers Association (EuroISPA).

HEIN DRIES-ZIEKENHEINER
THE NETHERLANDS

Hein Dries-Ziekenheiner LL.M is the CEO of VIGILO consult, a Netherlands based consultancy specializing in internet enforcement, cybercrime and IT law. Hein holds a Master's degree in Dutch civil law from Leiden University and has more than 10 years of legal and technical experience in forensic IT and law enforcement on the internet.

Hein was technical advisor to the acclaimed Netherlands anti-spam team at OPTA, the Netherlands Independent Post and Telecommunications Authority, and frequently advises on both technical and legal issues related to cybercrime. He was responsible for the first fine ever to be issued to a spammer under the EU anti-spam legislation while at OPTA and as lead investigator, he was involved in many cybercrime related enforcement actions and takedowns; including several malware cases and high profile international spam cases.

Hein served as legal and regulatory counsel and representative of the Netherlands ISP Industry Association (NLIP) and delegate to the board of the European Internet Service Providers Association (EuroISPA).

He regularly presents and moderates technical training sessions at international conferences on cybercrime and security and delivers training at both government and industry events. Hein regularly publishes and speaks on issues relating to law enforcement and cybercrime.

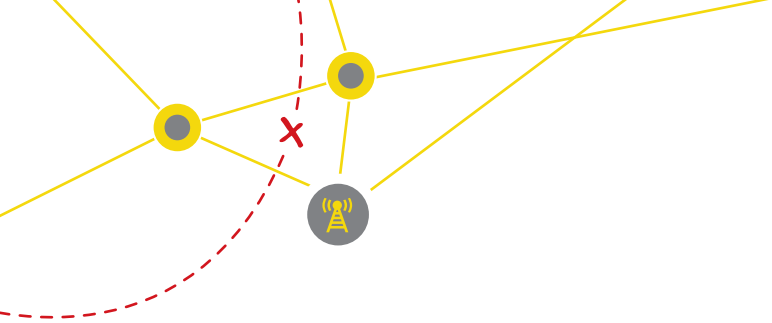


Table of Contents

Authors 3
Table of Contents 4

Executive Summary 6
Introduction 7
Background 8
Technical Testing 10
Threat Assessment 11
Country Profiles 15
Conclusions 19
Recommendations 19

Introduction 23
Freedom House 24
Broadcasting Board of Governors 24
Structure of This Report 25
Evolution of Mobile Markets 26
Market Actors 27
Blocking and Monitoring 29
Mobile Threats and Risk 31
Conclusion 37

Background 39
Smartphones 40
Hardware and OS layers 40
APIs and Security 41
Operating Systems: Differences in Architecture and Security 41
Mobile Networks 46
Conclusions 57

Technical Testing 58
Introduction 59
Selecting Applications 59
Testing 60
Set Up 60
Testing Criteria 61
Forensic Data Extraction 63
Selected Results 63
Results of Forensic Extraction 67
Conclusion 68

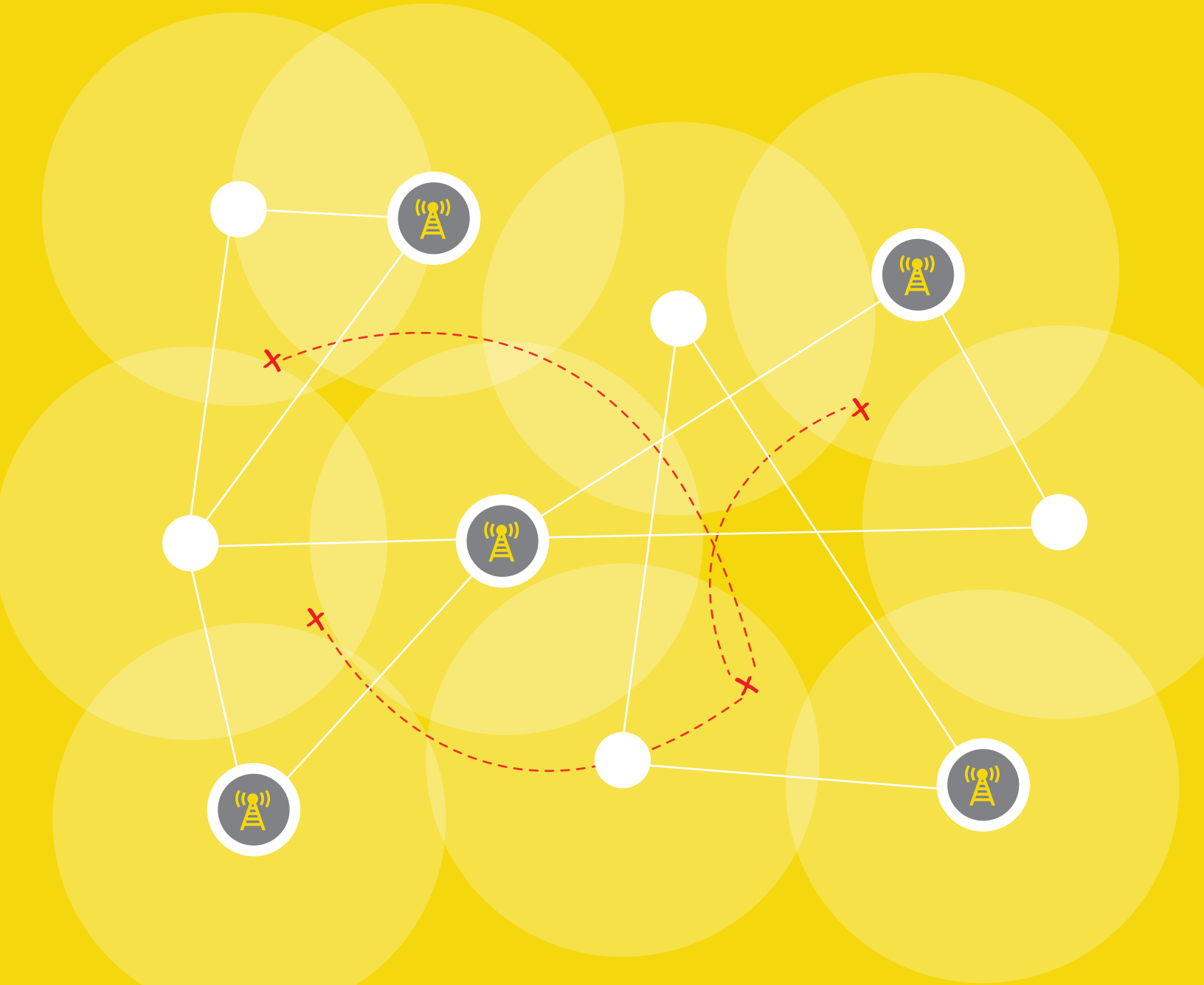
Threat Assessment 69
Introduction 70
Modeling the Mobile Environment 71
Types of Applications 71
Target Audience and Target Use Case 73
Phases of Mobile Phone Usage/Threats 74
Mitigating Threats 78
Countermeasures 79
Interim Conclusions 83
Developments 89
Conclusions 90

Country Profiles 91
Country Overview 93
In-Country Mobile Users 97
Republic of Azerbaijan 104
Republic of Belarus 109
People's Republic of China 113
Arab Republic of Egypt 116
Islamic Republic of Iran 120
Libya 125
Sultanate of Oman 127
Kingdom of Saudi Arabia 132
Syrian Arab Republic 136
Tunisian Republic 141
Republic of Uzbekistan 144
Socialist Republic of Vietnam 148
Findings 154

Conclusions 155
Recommendations 157

Appendix I Methodology 162
Appendix II Broadcasting Board of Governors Broadcasting Principles 167
Glossary of Terms 168
Information Sources 170
Developers 172

Chapter 1:
Executive Summary



Executive Summary

This report evaluates the risks and vulnerabilities of mobile phone services and apps in 12 specified countries: the Republic of Azerbaijan, the Republic of Belarus, the People's Republic of China, the Arab Republic of Egypt, the Islamic Republic of Iran, Libya, the Sultanate of Oman, the Kingdom of Saudi Arabia, the Syrian Arab Republic, the Tunisian Republic, the Republic of Uzbekistan, and the Socialist Republic of Vietnam. Rather than focus on a single innovation, this study analyzes multiple mobile technologies – including operating systems, applications and mobile protocols – to determine their capacity to protect security and privacy and to combat censorship and surveillance. Throughout this study the protection of mobile phone users was of paramount importance.

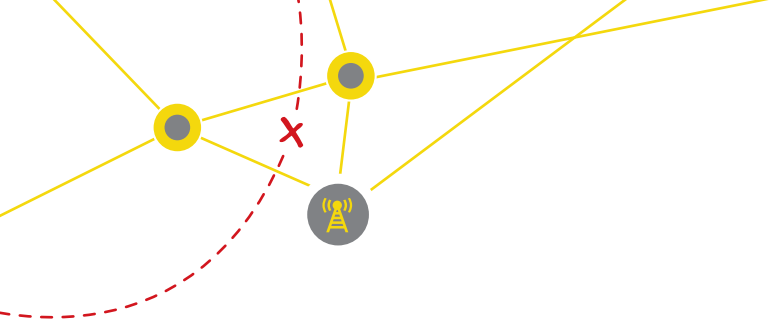
This project was managed by Freedom House and supported by the Broadcasting Board of Governors.

This study is divided into several sections. The **Introduction** outlines this research initiative and its methodology. It also justifies the need to focus attention on specific mobile phone environments. The **Background** section provides a comprehensive description of mobile phone technologies with particular emphasis on smartphones. **Technical Testing** outlines an analysis of the five primary platforms for smartphone usage: Apple iOS, Google Android, Nokia Symbian, Microsoft Windows Phone, and RIM BlackBerry OS. A **Threat Assessment** analyzes security and privacy challenges facing citizens who own and use a mobile phone, as well as obstacles confronting mobile internet users. The assessment confirms that various platforms can be used to overcome some threats particularly when blocking and circumvention technology is used. The **Country Profiles** evaluate 12 countries predetermined by the BBG for investigation. Data points in the analysis include the most recent key performance indicators for each national mobile market, various mobile operators, the range of handsets in use and the scale of mobile penetration for each country. The report is completed with a short section of **Findings** and a list of **Recommendations** for the future.

INTRODUCTION

There are many stakeholders with different areas of responsibility in the mobile market. At the state level, a **government's department for information and communications technologies (ICT)** is responsible for implementing government policy as well as setting and developing telecom strategy. A separate **telecommunications regulator** is usually independent of direct political control and regulates the TV and radio sectors, fixed line telecoms, mobile telecoms, and the airwaves over which wireless devices operate. The telecommunications regulators in the countries appearing in this report are not sufficiently independent from political influence. Individual companies called telecom operators – or a **telecommunications service provider (TSP)** – 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 mobile standards. 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 OS developers** create the interface installed on mobile handsets. Smartphone operating systems combine many of the attributes of a personal computer operating system with touchscreen, radio cell communications, Bluetooth, WiFi, GPS mobile navigation, camera, video camera, speech recognition, voice recorder, music player, near-field communication, personal digital assistant (PDA), and other features. **Application (app) developers** design and craft software applications for mobile devices. These applications are either pre-installed on handsets during manufacture or can be downloaded by customers from various mobile software distribution platforms.

This report analyzes mobile technologies – including operating systems, applications, and mobile protocols – to determine how they may work to combat censorship and surveillance. The report also provides an overview of the security and privacy challenges posed by mobile technologies.



The global adoption of mobile technologies has dramatically increased the privacy challenges and security risks for both businesses and citizens. The capability of states to monitor and track owners of mobile phones, and to block access to mobile and internet content, has significantly increased. Mobile phones are sophisticated devices that include all the elements of an excellent covert monitoring tool. They are personal devices and tend to spend most of their existence physically close to their owner, fully charged and connected to a mobile network. They are small and portable. They include microphones, cameras, speakers and storage capacity for SMS text messages, recordings, lists of contacts, calendar entries, activity logs, and copies of personal documents. Every hour of the day, each day of the year, mobile phones are connected to a radio data network that is managed and controlled by a network operator. This operator can manage the network and the handsets remotely with little to no oversight by the end user.

Since mobile technologies are in widespread global use, there are numerous manufacturers designing, developing, and selling equipment that can monitor and intercept mobile communication for use by mobile operators, states, companies, and end users. There is a vibrant competitive landscape for the manufacture and sale of these interception systems. A byproduct of mobile network design is easy access to a large volume of profiling data on every handset in use on the network.

Manifold users often fail to realize that combining all the log data from network towers and individual handsets enables both the complex analysis of phone records and the creation of crowd profiles. Applying crowd analysis and crowd modeling theories to the data available from mobile networks with a high penetration of smartphones is a dangerous tool in the hands of restrictive regimes.

Developing security and safety strategies for users of mobile handsets in countries with poor human rights records is complicated, and performing a comprehensive risk assessment is equally complex.

The purpose of risk evaluation is to accurately identify the potentially dangerous uses of mobile technologies. The assessment must address significant concerns of the affected users and make this risk information understandable and accessible. In the end, the handset owner must consider all aspects of daily handset use and reflect on how his/her use can be seen and recorded by persons with a non-beneficial interest in their activities.

BACKGROUND

Globally, access to the internet through mobile networks typically involves the use of smartphones or tablets. These devices can connect to a variety of communications networks (most notably WiFi and mobile networks) and provide internet access to applications running on them. The primary characteristic that defines a smartphone is its ability to run applications that enhance its functionality above and beyond the common features of voice calling and text messaging. In short, a smartphone is truly a pocket computer rather than a traditional telephone. Despite a wide variety of hardware manufacturers, the basic functions and design of mobile phones differ only slightly.

Each mobile handset runs on a hardware platform that is capable of various types of digital transmission. The most common technology for this is Global System for Mobile Communication (GSM). It evolved over time to support the transmission of data according to clearly defined protocols (such as GPRS, EDGE, HSDPA, and LTE). In addition, smartphones typically support communication and networking through WiFi and Bluetooth, as well as through cable-bound protocols such as USB and/or proprietary data exchange mechanisms.

Modern mobile operating systems usually provide ways to enhance the security of data through encryption. The OS also takes care of basic system protection (such as requiring a password and phone locking/unlocking mechanisms), data entry, and

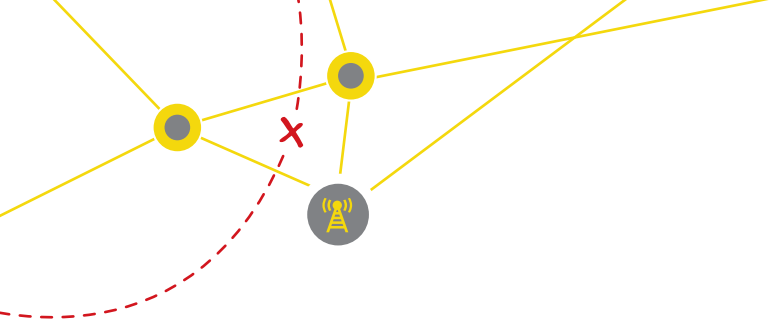
display functionality. Advanced programming interfaces (APIs) are commonly used to allow applications on the device to utilize the functionality available in the hardware. The use of APIs prevents applications from requiring direct communication with the underlying hardware. This enables the OS to implement security elements related to applications using specific features.

Android is an operating system for smartphones developed by Google. It is 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. However, a recent report showed that a majority of phones were not receiving the latest major version update within a year after its release. The Google application store is called Google Play and is universally installed on Android phones. Google has been criticized for not sufficiently monitoring Google Play to root out malicious applications. Consequently, the company has introduced automated tests with the intention of preventing the spread of malicious applications. Applications installed through Google Play can be uninstalled (revoked) centrally. 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 bypass certain security features of Android OS, and the phone hardware, the user sometimes needs to gain "root" access, a practice known as "rooting." This allows the user to install applications that access the phone's functionality that is only available to the core operating system and unavailable through APIs.

iOS is the operating system that drives Apple's iPhone, iPad, iPod touch, and Apple TV products. Although the version released in June 2012 was iOS 5.1.1, it is not uncommon for Apple users to maintain older iOS versions on their devices. Permissions management for iOS is less focused around the installation process than it is in Android. Instead, 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 versions 3.0 onward support the Apple App Store, an online repository containing many applications that can be downloaded and run on iOS devices. Applications in the App Store are tested by Apple and only accepted under strict conditions. Among these is the requirement that a developer submit his/her photo ID before being permitted to post there. However, the BootROM of most iOS versions can be hacked, enabling customizations to the operating system that would otherwise be impossible. In Apple-speak this is called "Jailbreaking" and is, in effect similar to "rooting" the phone as is done on Android devices.

Symbian is a mobile OS series developed by Nokia and was based on earlier operating systems (the EPOC series) from the mobile device manufacturer Psion. It has a much longer track record than both Android and iOS, and is still in use by many devices today. Despite Nokia's recent decision to favor Windows Phone 7 as its flagship operating system, Symbian is by far the most common OS for Nokia smartphones, and is still the most widely distributed smartphone OS in many markets. Symbian's base operating system runs in a slightly less protected environment as compared to Apple or Android, making it more susceptible to attack by mobile viruses. Its design is renowned for its efficient memory and resource usage, making Symbian a reference operating system in terms of true multitasking ability (the capacity to simultaneously run several applications in real time while sharing system resources). This functionality has long led to difficulties in early Android and iOS versions.

BlackBerry, the operating system that drives all RIM BlackBerry devices, was developed from the ground up with (corporate) security in mind. While adoption



of the technology was at first driven by larger corporate players, BlackBerry soon became the platform of choice for text-based communication for many ordinary users. RIM promoted the concept of secure communication between its services network and the BlackBerry hardware.

Windows Phone is the successor to Microsoft's Windows Mobile series of mobile phone and PDA operating systems. Similar to other modern smartphone operating systems, the Windows Phone uses the concept of sandboxed application execution. This means that applications 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, directly. Instead, Windows apps will have to use a strictly defined API for this, and are also restricted to their own data storage.

By far the largest contributor to the success of mobile telephony (and later, SMS and mobile internet access), was the relatively low cost of rolling out the required radio networks. Although the cost of handsets slightly offset this advantage, increased availability of ubiquitous, standardized (GSM) networks turned mobile networks into one of the major milestones of late 20th and early 21st century communication.

Blocking and monitoring occur across mobile networks. Blocking is the practice of stopping traffic from reaching an otherwise accessible destination. Monitoring, on the other hand, is the practice of listening in on (voice or data) conversations taking place on the network. The most important characteristic of blocking, as discussed in this report, is the level at which it occurs. There are significant differences in the blocking and monitoring schemes of the countries examined in this report. The fact, however, that governments want to control the characteristics of the blocking activities indicates that a central blocking list or set of criteria is usually present. Monitoring of voice traffic is often observed, whereas proactive blocking is a rather rare phenomenon for voice traffic.

With the advent of smartphones that feature significant processing power, there is more and more investment in device-based monitoring strategies. These take advantage of vulnerabilities in the various layers of mobile phone hardware in order to install malicious software, or functionalities that can be used to monitor both data and communications emanating from the device.

Circumvention technology aims to bypass the blocking mechanism that operates in many countries. As blocking is primarily implemented on data connections, the general technologies available for circumvention on mobile phones do not differ much from regular, desktop computer oriented tools. Primary circumvention techniques include using proxies, tunnels/VPN, DNS-bypassing, and onion routing.

Increasingly, nation states are known to use targeted attacks to monitor or infiltrate the social networks of individuals perceived as enemies of the state. This means authorities employ significant resources targeted against certain persons or organizations, and persistently try to infect or infiltrate their network and equipment. Due to the technical expertise required for such monitoring or infiltration, the number of such attacks is likely lower compared to network-based blocking and monitoring.

TECHNICAL TESTING

This section describes the technical testing performed for this study, which focused mainly on applications used for circumvention and monitoring or for replacing voice and text services provided by GSM networks.

Although the advent of these alternate voice and text applications may well be driven by the desire of western consumers to evade the cost of using these services through the GSM network, they could, if implemented securely, also serve to evade monitoring and blocking in oppressive regimes.

The testing was primarily on text and voice tools with security or circumvention characteristics, as well as general circumvention tools, which provide unrestricted internet access to users regardless of the application they use. Testing focused on a range of criteria, with each being scored from 1 to 5. An unweighted average of several factors was used to create a score for each tool on three criteria: security, usability, and resilience to blocking.

In order to test the performance of the various applications and operating systems, five different mobile phones were used in a controlled test environment (see the appendix on Methodology).

The overall aim of the testing, therefore, was to try to provide the most secure platform using the principles of security-by-design, cross platform interoperability and resilience to blocking and monitoring by the government.

The assessment confirmed that the circumvention and blocking ecosystem for mobile phones is not favorable. Only one purpose-built tool was deemed sufficiently mature to merit testing. Several tools are still under development. At the same time, users indicate using non-purpose-built tools, like VPNs, for circumvention. This raises several questions, since these tools will often provide no more anonymity or security than a regular internet connection, even if they allow the use of the "free" internet.

Technical testing of the available VPN solutions provided more insight into the practicalities of running a VPN on a day to day basis. The design of many VPN systems seems geared mainly toward western-world risks and uses rather than the needs of users in oppressive states. A number of issues illustrate this problem, including encryption and security not transparent to users.

Although IPv6 functionality was not rigorously tested in the course of this study's technical testing, one of the WiFi networks the phone hardware was exposed to during testing did have native IPv6 available. This traffic was not blocked by most tools, effectively creating a means to bypass any IPv4 based circumvention.

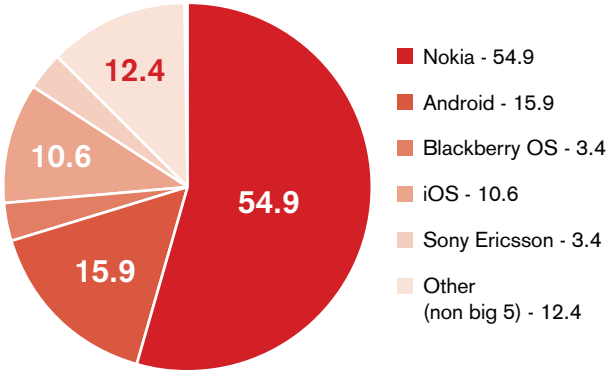
Many VPN and circumvention tools require rooting (Android) or jailbreaking (Apple). This creates an inherently unsafe situation, whereby, to make one application function, security for the entire platform has to be reduced. The technical testing did not involve a study into alternatives for this practice, though better APIs in this area may well make programming of robust circumvention tools more feasible and more secure.

Current VPN options are not great for circumvention. There is a clear need for a purpose-built VPN tool designed for circumventing blocking and avoiding monitoring. There is further requirement for more purpose-built tools. As well, greater attention to IPv6 issues is warranted. Developers need to either design for it or actively block it. Apps should be designed so as not to require jailbreaking or rooting of handsets, though current operating system designs may not make this easy. Finally, operating system designers and coders should configure APIs to allow their use for this purpose.

THREAT ASSESSMENT

Given internet usage patterns and the available hardware for mobile internet access, this study aimed at identifying where users are most vulnerable to blocking and monitoring by oppressive regimes. To further appreciate the risks people face, the study used a threat model to identify where usage patterns could lead to identifiable threats or opportunities for governments to block or monitor internet traffic. Applications and solutions were then identified that could allay these threats. Since these are, to some extent, based on software, mitigating measures per operating system were investigated.

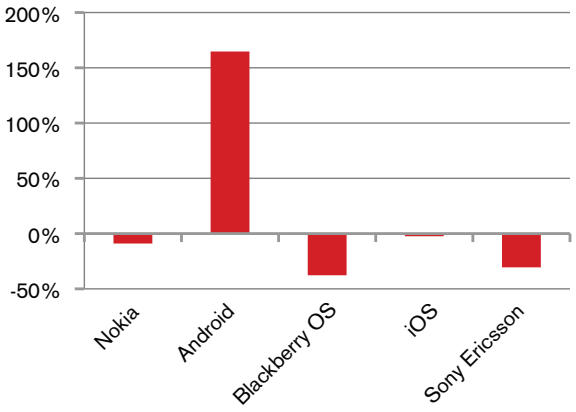
BIG 5 MARKET SHARE, MAY 2012

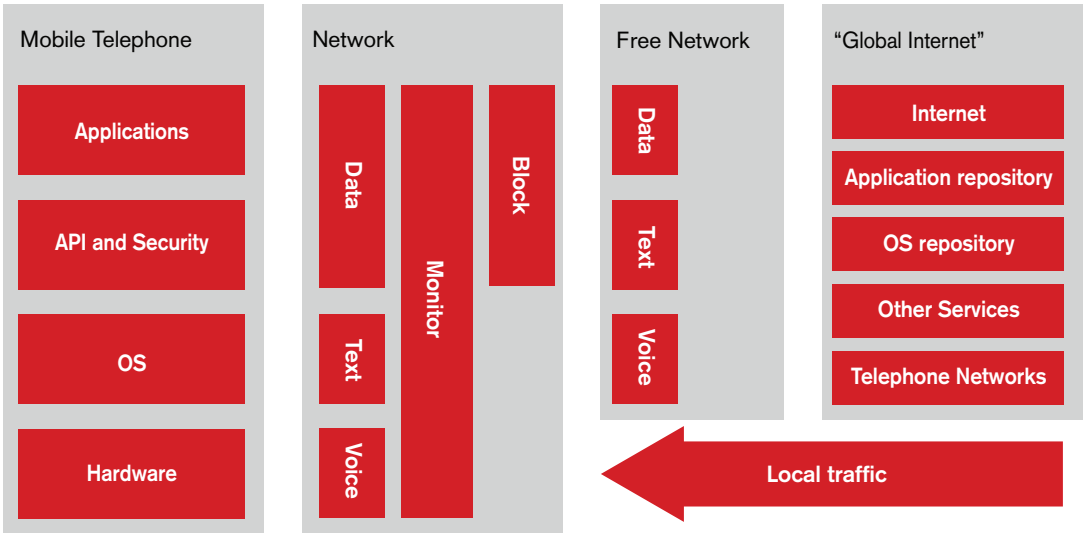


Source: www.statcounter.com (total for countries in survey)

The majority of users in the 12 countries investigated in the survey were using Nokia-based operating systems (predominantly Symbian variants) at the time that this report was written.

GROWTH RATE



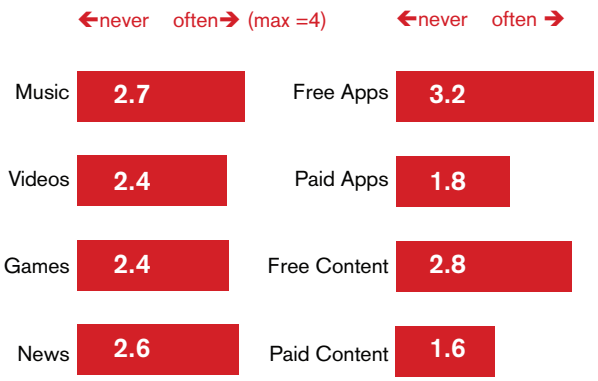


Technical testing focused on the assessment of circumvention and anti-monitoring tools that were currently available. In order to model the environment in which users exist, the researchers employed the following simplified model of the mobile environment (above). On the left is the mobile phone, with its various layers represented. This is the device that connects to the network to provide a voice, text, or data network access role.

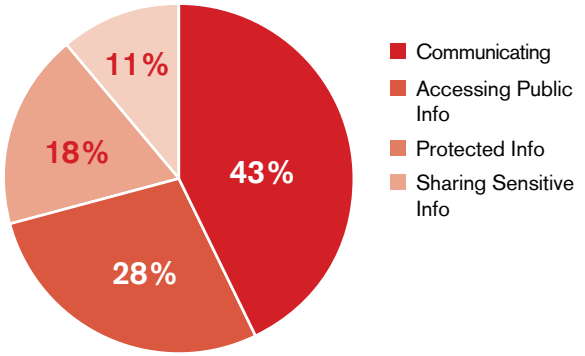
Once the mobile environment has been modeled, it is important to have some understanding of the type of activity users employ online and the type of risk these activities carry. Unfortunately, little information was available on this subject other than the in-country reports that were gathered in the user survey and expert survey.

It is clear, however, that mobile users favor free apps, and spend most of their time using these devices for direct one-to-one communication.

DOWNLOADS TO MOBILE HANDSET



TIME SPENT ON MOBILE INTERNET



It is important to note that the applications that were tested can be divided into five categories: regular applications, voice services, text services, circumvention tools, and security enhancements.

Given the weak security of GSM phone calls, there is a need for a more secure alternative to the voice service. Security of SMS text messaging is also weak, and even easier to monitor than voice service. A number of applications were identified that are capable of sending and receiving text messages through data channels. A number of apps that provide cryptography were also found.

To develop an appropriate threat model for mobile internet users in oppressive regimes, a generic user profile or use case is needed to limit the threats to the appropriate and most common risks. This report also focuses on applications that have either received, or have the potential for, mass deployment. This means the applications business model should potentially be able to sustain such growth.

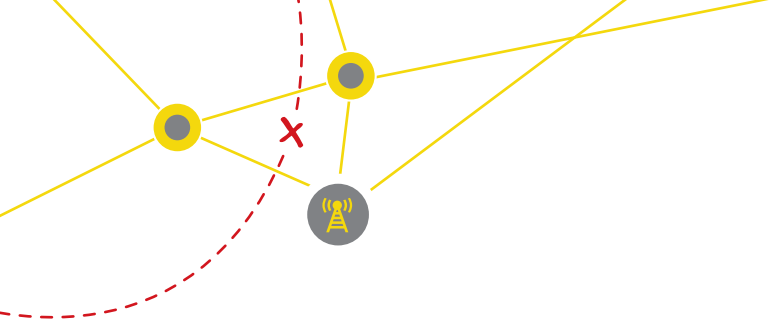
In order to analyze the situation of mobile phone users under repressive regimes, the researchers have developed a threat model based on the service life of a mobile phone and have categorized the related threats accordingly. The phases of this service life include purchasing a handset, using a mobile handset, installing applications, and access to the phone either physically or remotely.

Not every threat mentioned above can be overcome by technology alone. Some threats are nearly impossible to mitigate completely. For the purpose of this report, the researchers have focused on assuaging threats to a level more or less acceptable for the average user of mobile internet keeping in mind that a targeted effort by a regime, as well as the behavior of a user, may influence the safety of a person's internet usage.

In terms of countermeasures, possible (generic) measures have been identified including code signing, secure boot, anti-virus software, security enhancements, and file-system encryption.

While the researchers tested a number of security applications that allowed users to guard against blocking and monitoring, only a limited number of applications are available that enhance the operating systems' security level.

Tampering with rudimentary elements of the mobile phone (such as the bootloader and the radio firmware, often called baseband or the operating system) is detected as a matter of course by modern phone



operating systems. This, however, does not mean that these features cannot be disabled or circumvented. In case a user decides to install another operating system or aftermarket firmware on his device, these features are often disabled in the process of 'jailbreaking' or 'rooting' the phone. Similarly, states that want to spy on their citizens could easily pre-install such software or modify phones before marketing them.

Running applications and using the phone are by far the most important areas where users are exposed to threats. Not only are there various attack vectors in play, but the main interest of oppressive regimes will likely be in the real time data that is generated from mobile phone use. Not only text and voice, but also location data and other types of online communication form the main targets of many a monitoring operation.

Physical access to mobile phones is conceivably the most intrusive of all threats discussed here. By gaining physical access, an attacker exposes the phone's storage media, leading to possibilities for extraction of stored data and credentials. Close proximity access, such as near field communications, tethered connections, and Bluetooth, can yield similar results.

The next step is to perform a more detailed analysis of the blocking and circumvention options open to users of the main smartphone platforms.

The regular SMS text service is not very secure. The selected replacement text applications, therefore, usually run on the device's various data networks, bypassing the operator's infrastructure. In all cases they provide cryptography, and in many cases they provide more than just text messaging.

Similar to text messages, voice service on the average GSM network is also susceptible to snooping. Without special hardware, no options exist for encrypting GSM voice traffic. All use software-based encryption and the smartphone's internet connection in order to bypass government based monitoring.

Rather than bypassing the censor at a per-application level, it is also possible to capture and reroute a device's entire internet connection. This requires two layers of connectivity: one internet connection that is capable of reaching a third party service, and another overlay connection that is capable of carrying the actual data traffic that is being transported.

Detailed tables in this chapter list the score for a variety of applications and rate whether the outcome is insufficient, adequate, or good for an entire category of applications. Overall, iOS and Android scored best. However, this does not imply they are entirely safe to use.

From the perspective of a threat analysis, recent and expected future developments should not be ignored. In many countries, the deployment of LTE is in progress, and in some countries implementation is already in effect. Since current LTE standards plan for the implementation of IPv6, this may serve to underline the importance of raising awareness among both tool makers and OS manufacturers to approach technology in a secure and transparent fashion.

Furthermore, there is a trend for applications, and even operating systems, to be entirely web based. This is the expectation of a mobile OS such as Firefox OS (formerly known as Boot to Gecko), from the Mozilla Foundation. Firefox OS Applications are HTML5-based and can be run from an adapted mobile browser environment, rather than a fully specified OS.

The combination of the two (HTML5-enabled applications and a fast, IP-based mobile network) will enable a more IP-centered world which, on the one hand, may provide users with added independence from OS and handset manufacturers, but on the other, raises significant concerns for those users whose internet access is routinely blocked and monitored. Early attention to VPN or proxy access for such users would definitely be recommended.

Generally, all operating systems provide some level of circumvention and alternate voice and text messaging that can be considered secure for relatively low-risk communication. Circumvention on mobile devices appears to be largely reliant on VPN technologies. Using VPNs as a circumvention tool puts users at risk when switching connection type and where cryptographic implementation is concerned. Of all the platforms, Android scored as the most complete setup for "circumvention" and "voice/text." TOR is only available on Android, and was the first true circumvention tool available during the test period.

However, without further measures to enhance platform security, the level and maturity of circumvention tools is of little relevance to the mobile security debate. One could say that platform security is of higher priority than circumvention capability.

COUNTRY PROFILES

The 12 country profiles in this report were based on the analysis of publicly available data from inside and outside each country, as well as research conducted by in-country experts. In addition, the results of an in-country survey of mobile use were added to the profiles. The purpose of the survey was to supplement knowledge gained from the complex, comprehensive technical descriptions above with a richer understanding of the mobile usage patterns where these handsets are in use.

The mobile communication market is a fast changing and highly volatile area. In China alone, over 30 million additional subscribers were added to the country's mobile networks in the first three months of 2012.

In most markets analyzed, there are high levels of dependence on mobile communication, which is the preferred strategy for both voice and data communication. Due to the overwhelming success of mobile technology, fixed infrastructure is seeing very low investment and growth. For example, the Kingdom of Saudi Arabia is remarkable for having nearly achieved 200% penetration of mobile subscriptions in the mobile market – an average of two mobile subscriptions for every person in the country.

Globally, the top five mobile operators generate revenues of over $300 billion with 1.7 billion subscribers. The markets researched in this report represent almost 1.4 billion mobile service subscribers; 500 million of these are actively using mobile data services. Over 44 mobile operators were included in the research for this report and nine of these operators were fully owned by the state (the overall subscriber base for these operators is over 1.1 billion subscribers).

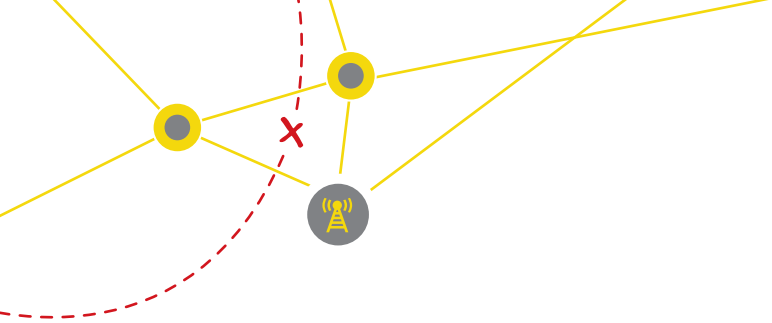
Many of the large operators are active in multiple countries. This provides a challenge for restricting the sale and deployment of dual-use technologies since operators will have access to the same equipment in separate markets, which allow operators to move and process user data to wherever their equipment is located.

From the expert research, the focus of mobile internet users in these countries is on access to news content. The second area of use is for entertainment. Thirdly, users are interested in accessing video content from sources such as YouTube or the national variants of YouTube. Due to the high reliance on mobile technologies, the need for access to an open and unfiltered internet is considered essential for all aspects of mobile internet use.

Analysis of the survey results for the markets selected shows a range of state strategies for ensuring effective control of mobile operators – both in terms of which market participants are licensed and the business activites of those licensed market operators.

One motivation of state oversight 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.

Based on the research, handset choice is increasing



in each market and new mobile packages are regularly made available. Mobile data usage is also increasing. All these suggest vibrant, competitive, profitable markets with strong demand for services into the future. Where there is a wide variety of handsets available, a significant technical challenge is created for state security agencies to develop hardware monitoring options specifically designed for a complex range of handsets.

A wide variety of content is blocked in the countries studied in this report. Much of this content, such as child pornography and hate speech, is considered illegal in countries across the world. However, blocking some types of content – such as religious content, foreign news, or national news sources – is problematic and is a direct challenge to freedom of speech. In addition, the interpretation of what constitutes hate speech or terrorist content can be much broader in some countries than in others.

The total number of respondents was 1,644 in all 12 countries surveyed. Over 60% of users surveyed chose pre-paid options for their mobile service and just over 36% have a post-paid contract in place. 79% of mobile users surveyed have access to the internet using their mobile phone, but almost 18% did not. Almost 33% of users accessed the internet with their mobile handsets using WiFi. Access via a limited internet bundle (32%) or a pay-as-you-go service (17%) are the next most popular methods of connecting to the internet from a mobile handset. Handsets from Nokia (32%) are still the most prevalent. Samsung (20%) comes second and Apple (19%) is third. These three manufacturers share about 72% of the total handset market, but market share changes rapidly.

Trusted Sources of Mobile Internet Communication

Includes Don't Knows

	Rank	Never (max = 5) Always
Government	11	1.1
State Agencies	10	1.2
ISP Inside	6	1.3
ISP Outside	1	1.5
NGO inside	7	1.3
NGO outside	9	1.3
CSP inside	8	1.3
CSP outside	5	1.3
Personal inside	2	1.5
Personal outside	3	1.4
Software Engineers	4	1.4
Other	12	0.7

The researchers surveyed mobile users, asking them who they would trust to protect the privacy on their mobile internet communications. It is very clear from the response that there is very little trust for all stakeholders in this complex area. Governments and state organizations came lowest on the list with communications services providers located outside the home country (ISP, mobile, telecommunications company) trusted the most, followed by personal friends/contacts located inside the home country in second and personal friends/contacts located outside the home country in third place. However, the highest score was still quite low at 1.5 out of 5.

With a population of more than nine million, the **Republic of Azerbaijan** is a mid-sized market for its three mobile networks. Government interference with internet content is observed by some users, although not all seem affected. With relatively high mobile and regular internet access availability, Azerbaijan is an opportune market for mobile internet freedom tools: limited use of circumvention technology is observed despite a majority of participants reporting some form of government blocking and monitoring.

The **Republic of Belarus** presents a mid-sized market that has many characteristics of modern western telecommunications markets. Although some restrictive legislation is in place, especially where the sale of services is concerned, Belarus seems a promising, yet non-democratic, marketplace where mobile internet access is concerned. Mobile penetration has reached over 108% of the population. Although mobile penetration is over 100%, the market in Belarus has strong competition. It has a busy apps market and handset options include a range of the most recent smartphones.

The enormous size of the mobile market in the **People's Republic of China** is truly staggering. In Q1 2012 the mobile operators gained an additional 30 million users to the mobile networks. Mobile penetration has reached 74% and continues to grow. The mobile operator China Mobile is the largest telecom company in the world.

For the **Arab Republic of Egypt**, there was insufficient data received from the in-country user survey. Most of the data presented was collected from the in-country expert. This is due to the complex political situation in the country, with the new Egyptian President elected in late June 2012. Mobile penetration is over 100% and there is good competition in the market.

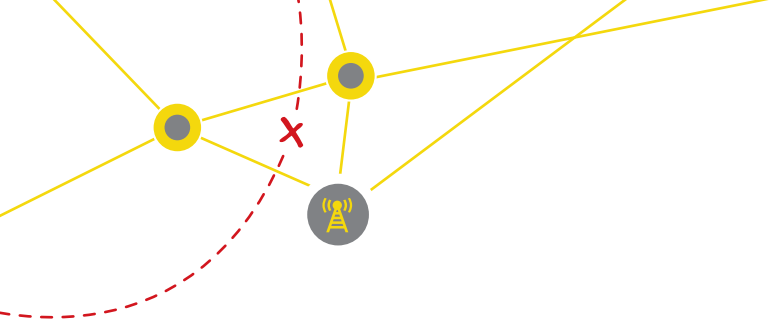
Regulation of the mobile market in the **Islamic Republic of Iran** is very sophisticated and there is significant state ownership of the mobile operators with external involvement from organizations in South Africa and Malaysia. Market penetration has not kept pace with other countries in the region, but there is still a large number of subscribers. Iran has one of the lower mobile penetration markets in the region at 72.3%. Only Syria, with 57.7%, is lower. However, there are still over 54 million mobile subscribers in the country. Fixed broadband has amazingly low penetration with only 0.7% of the population and an absolute volume of 1.7 million.

Libya could not be adequately surveyed for this report. Ample anecdotal evidence suggests its telecommunications market is slowly getting back on its feet, although worries remain, especially around the use of Gadhafi-era monitoring equipment.

Mobile penetration in the **Sultanate of Oman** has almost reached 180% of population and continues to grow. In comparison,less than 11% of fixed lines installed offer less than 3.5% of internet broadband services. This means that the preferred delivery method for content will be over mobile networks.

The **Kingdom of Saudi Arabia** is impressive, achieving almost 200% mobile penetration. Even more interesting is the low penetration of fixed broadband (5.5%) in the country. Market regulation is strong and market competition is very healthy. Almost 82% of users consider themselves intermediate users of mobile handsets, and almost 92% of mobile users in the survey have smartphones from the most recently manufactured range.

The **Syrian Arab Republic** has the lowest level of mobile penetration in the region and among the lowest number of subscribers (11.9 million subscribers). There are only two mobile operators active in the market and operators give a share of their profits to the state. Conveniently, the Syrian market does not have significant competition; it is tightly controlled by organizations that are closely aligned with the government. The government receives significant annual revenues from the mobile operators as specified in the contracts allocated to them.



Mobile penetration in the **Tunisian Republic** is reaching 117% of the population. In November 2011, the Tunisian government set up a national holding company called CDC (Caisse des Dépôts et Consignation) to manage its shareholdings in the country's two mobile operators, Tunisiana and Orange. An independent subcommittee has also been assigned to monitor corruption, approve the general policies of the funds, and evaluate investments. The CDC manages 25% of Tunisiana, 51% of Orange, and the Zitouna bank, which was seized from the former ruling family.

The telecommunications market of the **Republic of Uzbekistan** is reaching saturation and is one of the fastest growing sectors of the economy. Uzbekistan has the highest rate of growth in the number of mobile subscribers in the Commonwealth of Independent States. The growth rate of revenues from mobile services lags behind the pace of growth in the number of mobile subscribers. There were 24.3 million mobile subscribers at the end of 2011.

The mobile market in the **Socialist Republic of Vietnam** has been growing rapidly. Mobile penetration has reached 137% of the population over nine years. Currently there are over 119 million subscribers. Vietnam is also one of the few countries making significant progress in the transition to IPv6 internet addressing technologies on mobile networks. A significant amount of Vietnamese mobile broadband users already access video content on their mobile phone.

Creating the expert questionnaire and the user survey, and collecting data from public sources, were complicated endeavors. Sometimes the need to ensure the safety of individuals administering the surveys in-country had a higher priority than insisting on complete and detailed feedback about day-to-day experiences using mobile handsets and networks. In some countries such as Vietnam, it is illegal to conduct a survey without a license.

As part of the ongoing volatility in the regions being analyzed, specific political upheavals and social unrest manifested in several countries during field work, especially in Egypt and Libya. Whereas it was possible to collect some information about the mobile markets in Egypt, it was not possible to collect adequate levels of data about Libya.

The mobile markets in these countries share a number of interesting characteristics:

- Due to the nature of mobile communication where spectrum is a scarce resource under direct regulation and management by the state, there are easy opportunities for states to implement mandatory requirements to include monitoring and surveillance capabilities.
- The size of the mobile markets across all countries analyzed is huge. China is the largest at 1,030 million subscriptions, and the Sultanate of Oman is the smallest with 4.9 million subscriptions.
- The penetration of mobile subscriptions in the population of every country is also great. The Syrian Arabic Republic has the lowest percent penetration at near 58%. The Kingdom of Saudi Arabia has the highest penetration at 198%.
- Revenues from the mobile market are significant for both mobile operators and the government (in terms of taxes and licensing fees).
- There is relatively low investment in fixed line infrastructure in most of the countries surveyed.
- In several countries, such as Belarus and Vietnam, there is a vibrant black market for handsets. Whatever their provenance, handsets can still be identified and logged by the mobile operator, yet it is encouraging that such handsets would not have been installed with specific software configured by the state or mobile operator.
- In several countries, such as the Sultanate of Oman, the government has implemented a handset labeling requirement for authorized devices, and spot audits are performed on the retail outlets selling handsets to ensure compliance.

Since many mobile operators are multi-national in nature and operate either wholly-owned or partly-owned subsidiaries in many markets, it will be difficult to control the sale and distribution of surveillance and monitoring technologies or dual use technologies. Due to the global nature of the internet, either the equipment will find it's way to the undesirable country or the data can be moved to the location of the equipment for analysis.

CONCLUSIONS

In the early months of this study, it became apparent that there was a lot of data and information on the mobile markets and operators, but data on the use of mobile networks and handsets by activists was very sparse. The focus on handset use and the particular interest in apps on smartphones was a challenge. During the first weeks a literature review highlighted the shortage of material in the area of interest. There was also a dearth of information available on smartphone security.

However, it was also an area that was generating increased interest and attention from many different sources. There was growing attention to mobile malware by anti-virus companies, and a number of excellent reports were released providing up to date information on specific risks for mobile handsets. At the same time, the issue of mobile risk was in regular discussion in the media and on relevant security mailing lists.

Many mobile manufacturers and government agencies released reports describing the security models inside the operating systems (e.g., Apple) and the approach to implement mobile security in the enterprise (e.g., Australian Department of Defence, United States National Security Agency).

It became very clear at the beginning of this study that there were enormous, almost unavoidable, risks to security, privacy, and, therefore, safety for any person using a mobile network in regions of the world that have poor history of respect for human rights. Many applications are not built around the assumption that network traffic cannot be trusted. These apps reflect the situation in western countries where some trust is placed in the mobile operator or ISP to secure communications.

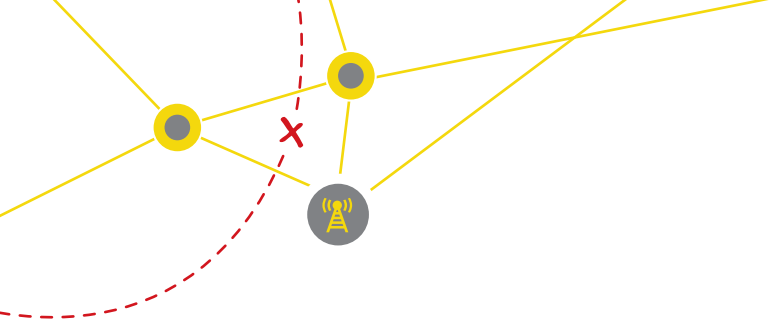
It is clear from the countries analyzed in this report that there is a phenomenally high level of penetration of mobile handsets in almost all the markets, and that these markets generate a high level of revenue for the mobile operators and a high level of license fees for the states in which they operate.

The bad news is that there are significant risks at the hardware level, the mobile operating system level, at the regulatory level, at the mobile network level, at the apps level, and at the end user level. In addition there are significant risks from (targeted) malware employed by states to spy on citizens.

RECOMMENDATIONS

This study has highlighted several issues that exist in the current landscape of applications and services available for circumvention of state censorship in oppressive regimes. Clearly, it will be impossible for any single actor, working in isolation, to change this situation, since both platform security developments at the OS level, as well as application development stakeholders, have, so far, left users in these regimes outside their mainstream development goals. Only niche stakeholders have taken the responsibility and have developed true and purpose-built tools for circumvention on mobile devices.

As a first recommendation, these developers deserve support from U.S. entities working in this space, since they both help elevate these initiatives towards the next professional level, and have the unique opportunity to provide leadership towards a more robust and secure censorship-circumvention



landscape. Entities working on internet censorship issues should also foster the development of new tools, insofar as they provide new and innovative ways of opposing state censorship and monitoring.

It is recommended that efforts be made to bring together the major application developers in this area on a more regular basis, not only to share knowledge and understanding of best practices, but also with a view to developing a number of short term goals that include:

- Working to bring true circumvention tools to the major mobile platforms used in oppressive regimes – in the near term, this will primarily require application developers to build these applications themselves.
- Improving support of VPN services for circumvention scenarios on all major operating systems, with special attention to Symbian (which has a large legacy user base), and supporting IPv6.

At the same time it has become apparent that there are many factors and players that are relevant for this development. Although a narrowly focused group like the one suggested above could probably deliver most results in the near term, we suggest more focus on creating a collaborative environment by sharing these goals and efforts with a broader set of actors over the long run.

Mobile operating systems, for instance, focus largely on the needs of western consumers. They build applications, security features ,and platform security models on the basis of a certain amount of trust being placed in network operators and their respective states of operation. However, this is not a safe assumption to make in the countries we studied. Most operators are firmly controlled, either directly or indirectly, by the regime they operate in.

These states also use or allow many American and European suppliers to deliver enhanced mobile coverage and connectivity to their citizens. Out of all mobile operating systems, not one is written primarily in a regime we studied. A large portion of the mobile hardware in the hands of end users is also designed by western companies, though we note that China is rapidly becoming a world class player in this area.

At the same time, the research conducted for this report makes it clear that a larger pool of expertise is required to develop and test applications in greater depth and in a timely manner. It would be fitting and appropriate for government entities to bring relevant actors together and ask them to focus attention (and real development effort) on the needs of citizens in these new, rapidly expanding telecommunications markets. Many actors in this area are dependent on each other and yet do not seem to be in regular contact. The actors who could benefit from such efforts include application developers, circumvention application developers, OS developers, hardware manufacturers, security solution providers, NGOs working in repressive regimes, government agencies, and foreign counterparts working in the field of communications security and foreign relations. A selection of activists and bloggers with specific experience in the field could also benefit.

Together, these actors, in a safe and vetted environment, could then work together on strategies, development goals, and best practices to help foster unfettered access to the internet on mobile devices. Parties interested in secure mobile communication should also undertake a media campaign to raise awareness about the risks and best practices for using mobile devices.

At the same time, the role that individual actors play cannot be ignored. This report will first highlight recommendations in the field of awareness raising and then move to recommendations for

other areas.

AWARENESS RAISING

- The level of influence that handset manufacturers have on the safety and security of handsets is significant.
- The complex environments in which mobile operators function creates challenges for government, industry, and mobile users. A balance must be struck between current trends in sharing significant amounts of data online while protecting that data from abuse.
- In a tightly regulated market with a limited number of operators and a highly regulated telecommunications infrastructure, governments can easily dictate mobile policies in total disregard of international human rights. As such, they can implement policies which can have devastating effects on democratic principles.
- The modern handset is a complex computer with a vast range of sensors and capabilities. Users need greater knowledge of, and training in, the capabilities of today's handsets.
- There is a lack of understanding of the safety and security challenges that users face while living in restrictive regimes. Some circumvention strategies work to bypass blocking and filtering systems but do not offer anonymity or security for the user. This can be dangerous for users who can be identified by the state. Alternative systems offer both circumvention capabilities and high levels of security which strive to prevent state agencies from collecting any forensic evidence that could be used in a court of law. However, even these systems can be dangerous to users. This is because state agencies in these restrictive regimes are often not searching for high levels of forensic evidence; rather, they see a simple system to reduce the high number of potential suspects to a smaller number of individuals for increased levels of monitoring and interrogation. Using complex secure tools that cannot be decrypted or hacked by the state can in itself be a dangerous, identifying criteria.

HANDSET MANUFACTURERS

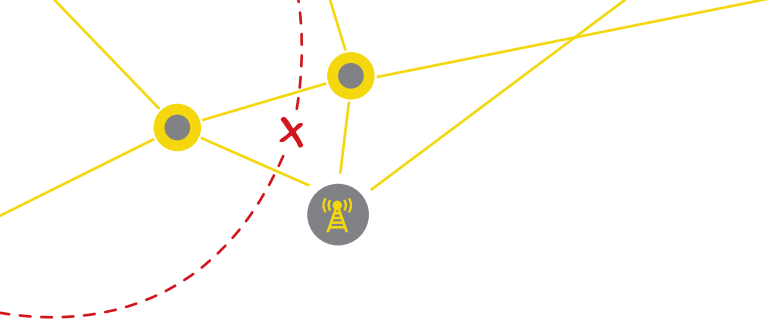
- Manufacturers should provide security and privacy architecture by design in hardware and firmware, including the ability to disable the remote control of the camera, microphone, GPS, and radio transmission, and to ensure the user's ability to securely turn off these features. Disabling the capacity for unauthorized remote software updates and reconfigurations without the owner's knowledge/permission would also be helpful.
- Secure data encryption in hardware is a key necessity, as is the capability for secure communication using encrypted SMS, voice, and data.

OS DEVELOPERS

- Developers should provide security and privacy architecture by design in operating systems.
- Better networking and routing APIs that enable circumvention tools to operate without "rooting" or "jailbreaking" the handset.
- More support for security enhancements to their platform, either through dedicated APIs or through adoption of such enhancing technologies into mainstream OS.
- Openness and transparency about dealings with states that have a direct effect on freedom of speech.
- Support for good security practices.
- Foster non-western security threat models that assume the untrustworthiness of state controlled operators.

APPS DEVELOPERS

- Developers should create more circumvention and anonymity tools to complete the landscape.
- Use security features of the OS as much as possible.
- Make an effort to develop circumvention applications for all platforms, rather than focusing on only one.
- Think about how apps could enhance OS security.
- Release privacy statements.



- Increase transparency of purpose, intention and implementation.

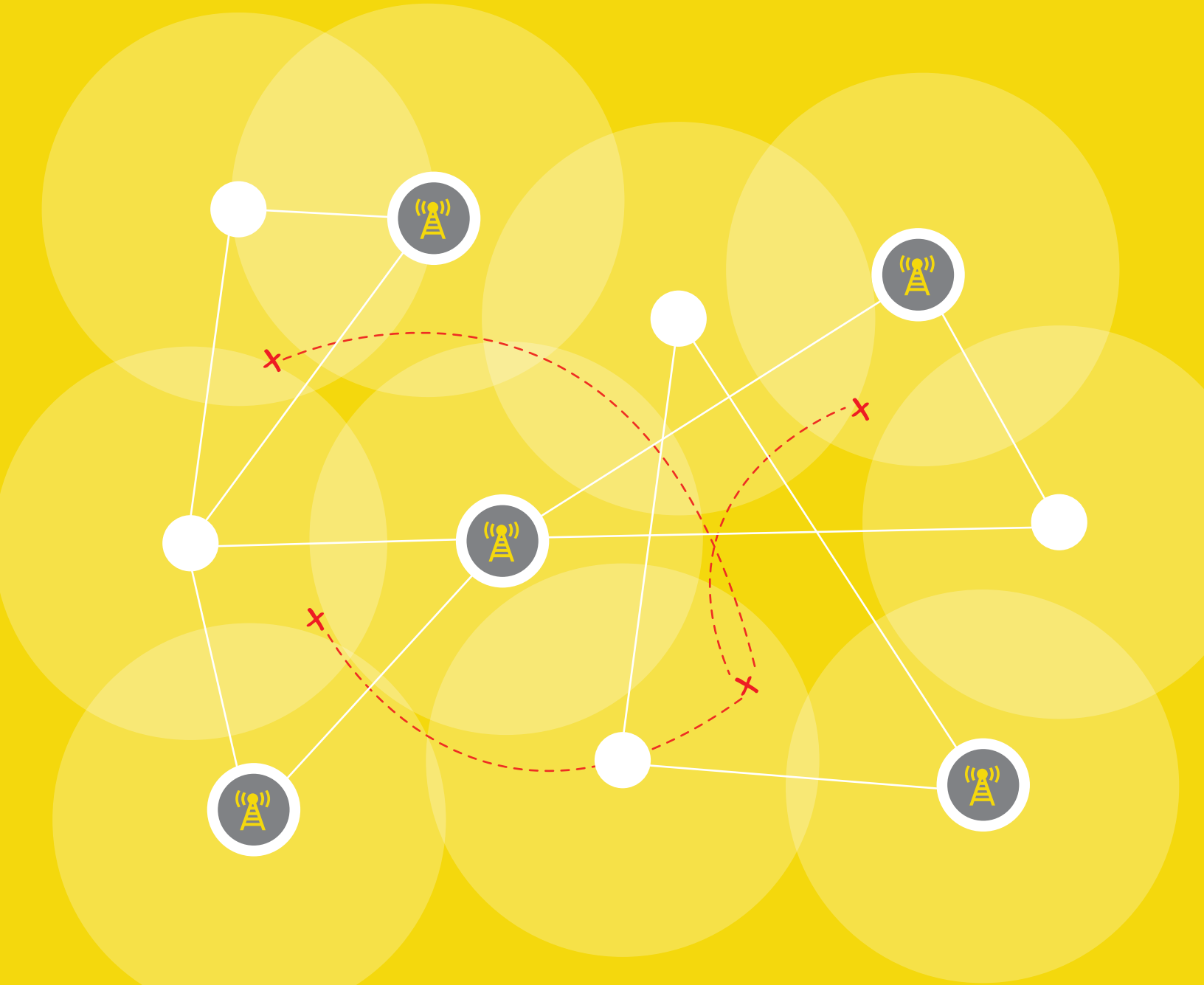
IN-COUNTRY ACTORS (REPORTERS, INTERNATIONAL AGENCIES, ACTIVISTS)

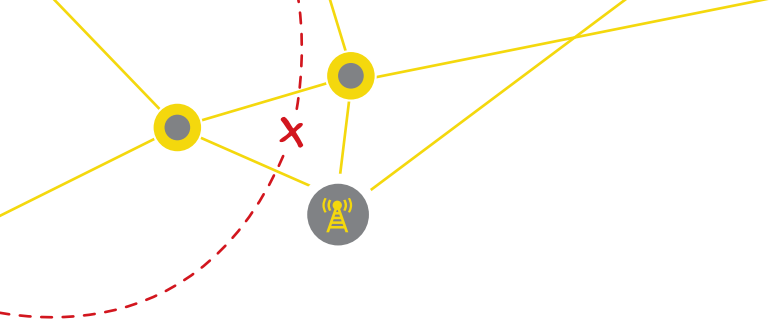
- Undertake basic and intermediate training on risk assessment and risk mitigation. Attention to high-risk environments and activities, especially when risks, and the resultant consequences, cannot be eliminated.
- Regular formal risk assessment (for security, privacy, and safety) of each country, government, handset in use, OS, app, mobile operator, and individuals.

FUTURE WORK

- Additional research in each country profiled is merited, particularly in an effort to further engage local experts.
- The speed of change in all aspects of the mobile environment is astounding. The focus of this report should be repeated at regular intervals to stay up-to-date and relevant.
- Detailed, independent, and transparent test procedures and laboratory manuals need to be created, which would permit regular, repeatable analysis of apps specifically developed for circumvention. These apps could be tested upon request of the developers, or independently analyzed at the request of end users.

Chapter 2:
Introduction





Introduction

The purpose of this report is to evaluate the supporting role of mobile phone services and apps towards encouraging democratic freedom and supporting freedom of speech in 12 countries of the world.

Rather than focus on a single technology, multiple mobile technologies were analyzed – including operating systems, applications and mobile protocols – to determine how they would work to assist free speech and to combat the threat of censorship and surveillance. Throughout the research conducted by the project team, the protection of mobile phone users was of paramount importance.

The project facilitated rigorous assessment of the security threats and risks to mobile phone users and executed a country-by-country analysis of mobile usage in 12 preselected mobile markets.

This project was managed by Freedom House and was supported by the Broadcasting Board of Governors (BBG).

FREEDOM HOUSE

Freedom House is an independent, nongovernmental, nonpartisan organization that champions the expansion of freedom around the world. Freedom House translates the values of freedom intro strong tangible impact by combining analysis, advocacy, and action.

The foundation of Freedom House's work is its analysis. Freedom House's rigorous research methodology used to monitor global freedoms has earned it a reputation as the leading source of information on the state of freedom around the world. Over the past several decades, Freedom House has created standard-setting publications that serve as critical resources for policy analysts and as valuable tools in supporting the work of civic and human rights activists worldwide. The flagship annual surveys are Freedom in the World, started in 1971, and Freedom of the Press.

COUNTRIES ANALYZED IN THIS REPORT ARE:

- **Republic of Azerbaijan**
- **Republic of Belarus**
- **People's Republic of China**
- **Arab Republic of Egypt**
- **Islamic Republic of Iran**
- **Libya**
- **Sultanate of Oman**
- **Kingdom of Saudi Arabia**
- **Syrian Arab Republic**
- **Tunisian Republic**
- **Republic of Uzbekistan**
- **Socialist Republic of Vietnam**

In order to examine internet freedoms and illuminate emerging threats, Freedom House also publishes Freedom on the Net. The latest edition, published in April 2011, covered 37 countries in six geographical regions. Cyber attacks, politically-motivated censorship and government control of internet infrastructure have emerged as especially prominent threats.

BROADCASTING BOARD OF GOVERNORS

The Broadcasting Board of Governors is an independent federal agency that oversees all U.S. civilian international broadcasting. The BBG's networks – Voice of America (VOA), Radio Free Europe/Radio Liberty (RFE /RL), Radio and TV Martí, Radio Free Asia (RFA), and the Middle East Broadcasting Networks' (MBN) Alhurra TV and Radio Sawa – serve as indispensable sources of accurate and reliable news for people who often lack access to independent information.

In 2011, BBG broadcasts reached a record 187 million people every week, up 22 million from 2010, in more than 100 countries. The BBG is responsive to

U.S. foreign policy priorities, while remaining fully independent editorially. Our programming reaches people in their languages of choice; in countries where independent journalism is limited or not available; and where governments jam broadcasts and censor the internet.

The BBG employs state-of-the-art anti-censorship techniques and works with global partners to encourage the research and development of effective circumvention technology. For example, daily e-mail newsletters include news summaries, instructions for bypassing government filters, and links to proxy websites that enable users to connect to our networks' news sites and other uncensored websites. In addition, BBG-supported client-based software aids users in restrictive cyber environments to browse the internet unfettered.

Given the restrictive media environment and repressive government tactics in some countries where our journalists operate, the BBG takes seriously the need for anonymity and security for users of internet anti-censorship tools. In response to active campaigns to censor online news, the BBG continuously experiments with anti-censorship tools. We regularly test new techniques, keep the ones that work, and drop those that do not.

Through constant innovation and technical evaluation, BBG engineers open gateways for audiences seeking access to a free and uncensored internet. Our anti-censorship programs are a natural component of the BBG's mission, to inform, engage, and connect people around the world in support of freedom and democracy. For more information about the BBG, visit www.bbg.gov.

STRUCTURE OF THIS REPORT

This report is divided into seven major sections. This **Introduction** will explain why this project was started, the role of the various actors and provide an explanation of why there was a need to focus on mobile phone environments. We provide a short overview of the mobile marketplace, the state actors in each country and a review of what areas and technologies are not covered in this report.

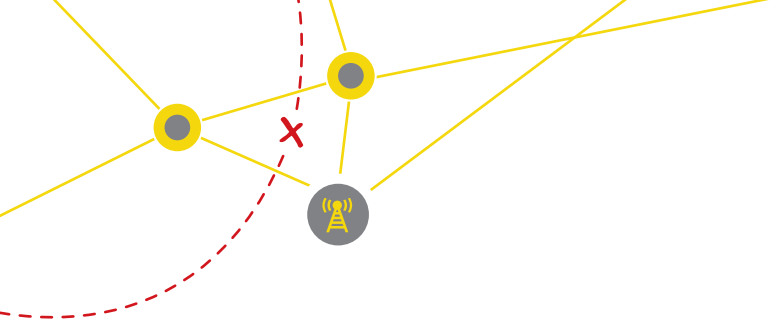
The **Background** provides a comprehensive, detailed description of available mobile phone technologies with particular emphasis on smartphones. We describe how most common mobile internet hardware works, what networks it connects too, and provide a technical background for the non-technical reader. This will illustrate a model of the mobile internet environment that will be easy to understand and can be used to assess specific threats.

Technical Testing describes the testing that was undertaken for this report on the five primary operating systems for smartphones: Apple iOS, Google Android, Nokia Symbian, Microsoft Windows Phone, and RIM BlackBerry OS. This section describes the methodology of testing, identifies the focus of the testing, summarizes the results, and concludes with a series of recommendations to mobile phone manufacturers, operating system developers, app developers and mobile operators.

A **Threat Assessment** looks at the challenges faced by citizens who own and use mobile phones and the different risks faced by mobile internet users. The purpose is to provide an overview of the range of threats which needs to be an essential element of the risk assessment of every citizen in their daily use of these technologies.

The next section **profiles 12 countries** by assessing recent key performance indicators for their respective mobile markets, the mobile operators in the market, the range of handsets in use in each country and the scale of mobile penetration for each country. The purpose is to identify the commonalities and distinctive elements of each country's mobile market, which will enable identification of the key challenges to freedom of speech and human rights on mobile platforms.

The next three sections analyze the knowledge gained by combining the technical testing and the country profiles to reach some **Conclusions** about the core challenges and issues with the use of mobile



technologies in these target countries. The report makes **Recommendations** about what risks exist for users, what can be done to mitigate those risks, the roles and responsibilities of different actors in this space and what further work would be recommended.

Finally, the **Appendices** describe the methodology that was adopted to conduct the in-country surveys, include the surveys themselves and identify other sources of information that were reviewed as part of the ongoing input to this report.

EVOLUTION OF MOBILE MARKETS

GSM technology enabled the development of a mass market of mobile communications. In mobile communications, the spectrum required for radio transmission between users and base stations is a very scarce resource and in the past, analog systems used spectrum inefficiently, so that only a small number of customers could be served and a small number of providers could be licensed. With the transition from analog to digital technology (the introduction of GSM – Global System for Mobiles) there was a major improvement in the efficient utilization of the radio spectrum.

The licensing of spectrum is a lucrative financial activity for countries and their governments. Apart from enticement to corrupt decision making, ensuring efficient use and fair allocation of radio spectrum is a complex area. In order to ensure minimum political interference, and also independent decisions, many countries have created an independent agency with responsibility for telecommunications issues.

Most countries decided to license the use of the radio spectrum for a fee. This was sometimes done through public auction of selected radio spectrum, sometimes using a tender process and sometimes by state decision. The large sums paid at auction are funded by the large annual revenues of mobile operators and it is clear that network operator has been one of the fastest growing industries in recent years. Table 1 below indicates the value of the mobile market for the top 5 global mobile operators.

In 2000, some European countries gained huge revenue by the auctioning of third-generation (UMTS) spectrum frequencies for mobile communications, including €37.5 billion to the UK state, and €50.8 billion into the German state. In 1999, the Nigerian government decided to issue four digital mobile licenses using a comparative selection process that failed in February 2000, due to allegations of corruption. In January 2001, Nigeria awarded three GSM spectrum licenses (using a hybrid auction featuring an ascending clock phase and a sealed-bid phase), which raised US$855 million.

TABLE 1: TOP 5 MOBILE COMPANIES OF THE WORLD BY SUBSCRIBERS[1]

Rank	Mobile Operator	Subscribers (millions)	Revenues ($ millions)
1	China Mobile	677.5	82.9
2	Vodafone	404.0	72.3
3	Telefonica / Movistar / O2	241.0	78.7
4	América Movil	236.5	47.8
5	Telenor	164.0	16.4
	TOTAL	1,723.0	298.1

A SIMPLE BUSINESS MODEL

"We buy licences that give us rights to spectrum bands and we build networks over which we provide calls, SMS and mobile internet services to customers."

Vodafone Annual Report 2011
31 Mach 2012

The scale of a mobile network is now huge. For example, in 2012, Vodafone Group reported that in the previous year:

1 http://www.telecomindiaonline.com/top-10-mobile-operators-in-world-at-telecom-india-daily.html

Nearly one trillion minutes of calls were carried and more than 216 petabytes of data were sent across our networks – in other words enough data for 2.8 trillion emails. We have more than 238,000 base station sites transmitting wireless signals. Data is already the fastest growing segment of the Vodafone group, with data revenue up by 22.2% over the financial year, compared to a 4.4% rise for messaging revenue and a 4.0% fall for voice revenue. This demand is being driven by three key factors – a widening range of powerful and attractive smartphones and tablets, significant improvements in mobile network quality and capability, and an increased choice of user friendly and useful applications for business and social use.[2]

COMPARISON OF INTERNET SERVICE PROVIDERS AND MOBILE NETWORKS OPERATORS

Whereas most countries have a large number of (usually unlicensed) internet access and service providers, the number and type of mobile network is strictly controlled, limited by radio spectrum availability licensed by national governments for a significant fee and subject to comprehensive conditions.

Often there is confusion over the significant differences between mobile networks and internet access providers. It is important to understand the different business models and network management capabilities, especially in the area of blocking access to internet content and the possibilities to circumvent such blocking activities. The table below highlights some of the key fundamental differences between these areas.

Mobile Network	Internet Access Provider
Limited Radio Spectrum	Unlimited Bandwidth
Strictly Licensed	(Mostly) Unlicensed
High Entry Cost	Low Entry Cost
High Revenues	Low Revenues
Strict Regulation	Developing Regulation
Expensive Equipment	Low Cost Equipment
Handset Subsidization	Highly Competitive Pricing
Restricted Market	Open Market
High Profits	Low Profits
Significant Reporting Requirements	Minimal Reporting Requirements

MARKET ACTORS

A complex ecosystem of actors facilitates mobile communications systems and the interoperability of national systems at a global level.

GOVERNMENT

Most countries have a **governmental department for iInformation and communications technologies (ICT)** responsible for setting and implementing government telecom policy facilitating the delivery of broadband internet and administering the electromagnetic spectrum for communication and broadcasting. A robust, modern and efficient telecoms infrastructure is vital to the economy. Therefore, governments tend to view the ICT sector as a source of sustained national economic growth and competitiveness. This can be achieved by promoting investment modern infrastructure, providing a supportive legislative and regulatory environment and by developing a reputation for cutting-edge research and development in ICTs.

TELECOMMUNICATIONS REGULATOR

The **telecommunications regulator** is usually independent of direct political control and is responsible for regulating the TV and radio sectors

2 http://www.vodafone.com/content/dam/vodafone/investors/annual_reports/Vodafone_Annual_Report_12.pdf

and all aspects of telecommunications including fixed line telecoms, mobiles, and the airwaves over which wireless devices operate. For example, in Europe these agencies are the national regulatory authority for these sectors in accordance with EU law, and their authority covers all kinds of transmission networks including traditional fixed telephone wire, traditional television, and radio communications. In the USA, the Federal Communications Commission (FCC) is an independent agency of the United States government, created by congressional statute[3], and with commissioners appointed by the President. The FCC has six areas of responsibility including broadband, competition, spectrum, media, public safety, and homeland security. In the countries which are covered by this report, very few of these agencies were independent of government or from political influence.

TELECOM OPERATORS

The telecommunications sector is comprised of individual companies called **telecom operators**, which are a type of communications service provider (CSP), or more precisely a telecommunications service provider (TSP) that provides telecommunications services such as telephony and data communications access to consumers and businesses in each country. There are many ways to deliver voice and data services, including fixed lines services, point-to-point wireless services, satellite services, cable services, and mobile services (such as GSM mobile operators). Some operators offer a choice of many services in a range of countries and some operators offer a choice of services in a region or one country only. Examples of such operators are China Mobile, Verizon, Telefónica, Vodafone, and Saudi Telecommunication Group.

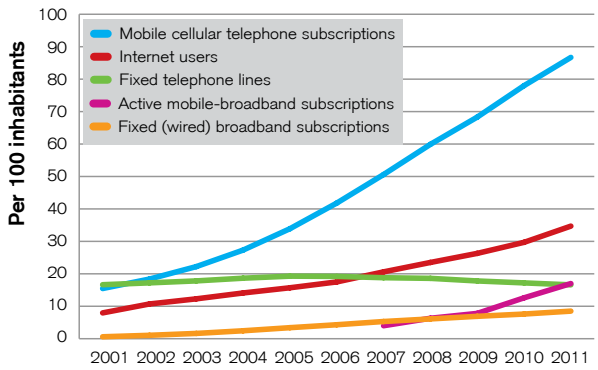
MOBILE HANDSET MANUFACTURERS

Mobile handset manufacturers are responsible for the design, development, and manufacture of mobile devices in compliance with mobile standards, which are then, subject to state approval, sold in different mobile markets around the world. Often, handsets will be adapted for different markets depending on the requirements of the state in which they are sold. The design of mobile handsets requires expert knowledge of user interface design, mobile phone operating principles, systems and network infrastructure, radio protocols, hardware anatomy and chipsets, software design, internal components, and circuits. Examples include Nokia, Sony Ericsson, Apple, Samsung, and LG.

MOBILE OS DEVELOPERS

Mobile operating system (OS) developers are responsible for the interface installed on mobile handsets. Smartphone operating systems include many of the features of a personal computer, often adding touchscreen, radio cell communications, Bluetooth, WiFi, GPS mobile navigation, camera, video camera, speech recognition, voice recorder, music player, near-field communication, personal digital assistant (PDA), and other features. Historically, handset manufacturers developed an OS along with the handset and each manufacturer was linked to a specific operating system. In recent years we have seen handset manufacturers using a variety of operating systems from different software vendors on their handsets. Nokia now develops and supplies phones installed with Microsoft Windows Mobile or Symbian and Samsung supplies phones with Microsoft Windows Mobile, Google Android, and Symbian. One new mobile OS currently under development is called Firefox OS (formerly known as Boot to Gecko) from Mozilla.

GLOBAL ICT DEVELOPMENTS, 2001-2011*



* Estimate
Source: ITU World Telecommunication / ICT Indicators database

3 (see 47 U.S.C. § 151 and 47 U.S.C. § 154)

APPLICATIONS DEVELOPERS

Applications developers create application software for mobile devices. These applications are either pre-installed on phones during manufacture or can be downloaded by customers from various mobile software distribution platforms. Android applications are written in the Java programming language. The Android Software Development Kit tools compile the code—along with any data and resource files—into an Android package. All the code in a single package is considered to be one application and is the file that Android-powered devices use to install the application.

INTERNATIONAL ACTORS

At the international level, the **International Telecommunication Union** (ITU) is the United Nations specialized agency for information and communication technologies – ICTs. ITU allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide. ITU currently has a membership of 193 countries and over 700 private-sector entities and academic institutions.

BLOCKING AND MONITORING

Internet censorship poses a large and growing challenge to online freedom of expression around the world. This report analyzes mobile technologies – including operating systems, applications and mobile protocols – to determine how they may work to combat censorship and surveillance and provide an overview of the challenges that mobile technologies provide.

The preservation of human rights is usually considered as intrinsic to democracy. This is especially true for human rights that could be in conflict with an internet blocking measure, i.e., the right of private life or the right to freedom of expression. Internet blocking systems as operated by the state can significantly interfere with a citizen's fundamental human rights.

The primary objective of internet blocking is that internet users are prevented from receiving and viewing specifically targeted content. Often the blocking system prevents users inside one country from communicating with others outside that country's borders.

Tools such as Herdict[4] measure the extent of blocking in certain countries and are extremely useful; widespread adoption should be encouraged. Herdict Web aggregates reports of inaccessible sites, allowing users to compare data to see if inaccessibility is a shared problem.

During her remarks at the Newseum in Washington, D.C. in January 2010[5], U.S. Secretary of State Hillary Rodham Clinton stated that during his visit to China in November 2009,

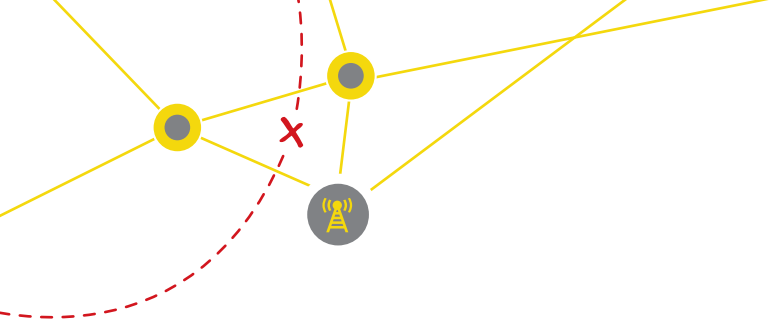
> President Obama held a town hall meeting with an online component to highlight the importance of the internet. In response to a question that was sent in over the internet, he defended the right of people to freely access information, and said that the more freely information flows, the stronger societies become. He spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity, and entrepreneurship.

Secretary Clinton went on to say that,

> Technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights. In the last year, we've seen a spike in threats to the free flow of information.

4 www.herdict.org/web (last accessed 4 April 2011)

5 Hillary Rodham Clinton, U.S. Secretary of State, The Newseum, Washington, DC, January 21, 2010. Available at http://www.state.gov/secretary/rm/2010/01/135519.htm (Last accessed 4-Mar-2011)



China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These 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." With the spread of these restrictive practices, a new information curtain is descending across much of the world. And beyond this partition, viral videos and blog posts are becoming the samizdat of our day.

"Annual global internet bandwidth growth has exceeded 50% the past 4 years. Nearly as much capacity was added in 2010 alone (13.2 Tbps) than the total capacity in service in 2008 (14.7 Tbps)."

In 2010, international internet bandwidth was over 35TB.

http://www.telegeography.com/page_attachments/products/website/telecom-resources/telegeography-presentations/0002/2315/RSchult_Capacity_China.pdf

In 2008, members of the European Parliament asserted that 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.[6]

Internet blocking systems as operated by the state can significantly interfere with a citizen's fundamental rights. In recent years, some democratic states have also promoted the use of internet blocking technologies in relation to a variety of narrowly specified types of content. They cite public interest to request specific blocks even though the characteristics of the internet cause enforcement issues. The subject matters vary from the availability of Nazi memorabilia via online marketplaces to gambling websites hosted in countries with liberal regimes in relation to online gambling. State regimes with little regard for human rights have adopted wide scale internet blocking as a technical resource for extending their practice of information control into the online world.

It is important to note the intrusive nature of many blocking strategies. This is especially true for the more granular, content based filtering mechanisms that require insight into the content of the material being exchanged between individual users. The required investment by the state and the network operators is, invariably, high (financial, time, and skills) for internet monitoring and blocking and it is also problematic from a broader, societal point of view.

This report focuses on mobile technologies and the various ways monitoring and blocking can be performed by states – particularly restrictive regimes – and then provides suggestions and recommendations to mobile handset manufacturers, mobile operators, OS and application developers about strategies to improve safety and security.

6 European Parliament resolution of 10 April 2008 on cultural industries in Europe, 2007/2153(INI), § 23, accessible at this address : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0123+0+DOC+XML+V0//EN. See section 6.3.2.2.

WHAT IS INTERNET BLOCKING?

Internet blocking (sometimes called internet filtering) is not a new activity. It has been around for many years. However, the term covers such a broad range of policies, hardware, software, and services that it would be a mistake to think that all types of internet blocking are the same or equally effective, legally equivalent or even that one system can easily be used in relation to more than one type of content.

The primary objective of internet blocking is that content is blocked from reaching a personal computer or computer display by a software or hardware product that reviews all internet communications and determines whether to prevent the receipt and/or display of specifically targeted content.

The term "Internet Blocking" itself is somewhat a misnomer since it seems to suggest that internet blocking is easily implemented and it is simply a choice to switch on or switch off. Nothing could be further from the truth since the capabilities of internet blocking technologies are quite complex and often can be bypassed with little effort. There are various reasons for this, the most fundamental being that the internet was designed to be decentralised, with a build-in capacity to ensure that data can flow "around" any barriers that are put in their way.

Attempting to block internet content that is legally made available outside the country, but is considered to be illegal inside the country, may sometimes also be considered as a possible option for countries to attempt to maintain their own national cultural standards in times of global access.

Monitoring and blocking is frequently employed in repressive regimes, whose primary purpose is to limit access to certain content the regime deems politically or ethically undesirable, or to prevent the spread of crowd-sourced information that is damaging to such regimes. The technical infrastructure required for this is complex and significant, but is, unfortunately, widely available (together with standard network monitoring tools) and specifically designed in western democratic states where they are implemented with strict legal oversight and approval.

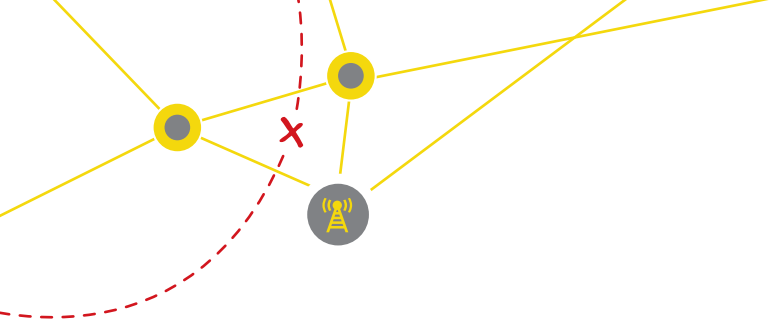
Strategies to disrupt circumvention tools include:

- Technical measures to disrupt usage, prevent access to content, monitor usage, and, where possible, identify the parties involved.
- Legal and self-regulatory measures to sanction circumvention or prevent distribution of tools.
- Propaganda promoting state sponsored ideologies, stimulating fear and uncertainty about the security of circumvention tools, and unreasonably stressing the effectiveness of monitoring and blocking systems in operation.

The most appropriate balance between a safe society and democratic freedoms is a very complex issue that needs to be determined on a national level through extensive debate among relevant stakeholders in each country and with regard to relevant international instruments.

MOBILE THREATS AND RISK

The global adoption of mobile technologies has dramatically increased the risks and challenges for businesses and citizens using mobile internet access. Every business user uses their mobile handset to access corporate information assets from remote locations. Users in restricted regimes use their handsets to share sensitive information with friends and family. These handsets are at risk to malware created by criminals or on contract for state agencies such as that described by F-Secure about FinFisher



products in Egypt[7]. State agencies can use network monitoring and crowd profiling software to profile activities of a large volume of users on mobile networks. It is complex challenge for organizations and users to assess the level of risk in the usage of mobile phones. This section describes these issues in more detail.

> "Although the need for mitigating mobile security risks and threats is acknowledged, risky behaviors and weak security postures are commonplace"
>
> Mobility and Security -Dazzling Opportunities, Profound Challenges - Carnegie Mellon CyLab and McAfee

MOBILE MALWARE

The McAfee Mobility and Security Survey[8] states that "there is a serious disconnect between policy and reality in the mobile computing environment – both IT directors and users are unhappy." The McAfee 2011 Threat Predictions report[9] states that,

> threats to mobile devices have been a hot topic within the security community for several years". They expected attacks to erupt at any time, yet they never quite seem to happen. "McAfee Labs predicts that 2011 will be a turning point for threats to mobile devices. This year we saw many new, but low-prevalence, threats to mobile devices: rootkits for the Android platform, remote "jailbreaking" exploits for the iPhone, and the arrival of Zeus (a well-known banking Trojan/ botnet). The widespread adoption of mobile devices into business environments combined with these and other attacks is likely to bring about the explosion we've long anticipated. Given our historically fragile cellular infrastructure and slow strides toward encryption, user and corporate data may face serious risks.

Spyware is a type of malware consisting of programs that secretly or duplicitously collect information and profile a mobile user's habits, online activities such as browsing and social networking, search strings, site preferences, and preferred applications. This collected information is either sent out to a third party or stored on the phone for later retrieval.

Note that most mobile malware is currently related to financial gain. For instance F-Secure reported[10] in Q4 2011:

> Most of the newly discovered or existing malwares were created to reap profit, most commonly by sending premium-rate SMS messages. Most of these can be classified as fake applications or installers, posing as a free version of a legitimate application. Unsuspecting users who downloaded these applications are usually not aware that they are subscribing to a premium rate service.

TABLE 2: NUMBER OF MALWARE IDENTIFIED ON EACH MOBILE OPERATING SYSTEM

MOBILE THREAT STATISTICS BY PLATFORM, 2008-2011 F-SECURE MOBILE THREAT REPORT Q1 2012					
	2008	2009	2010	2011	Total
Android			9	120	129
iOS		2			2
J2ME	2	7	2	5	16
PocketPC	7	8	19	2	36
Symbian	19	21	50	58	148
TOTAL	**28**	**38**	**80**	**185**	**331**

Note, however, that, mobile phones are personal devices and they tend to spend most of their existence physically close to their owner, fully charged, and connected to a mobile network. These sophisticated

7 http://www.f-secure.com/weblog/archives/00002114.html

8 Mobility and Security -Dazzling Opportunities, Profound Challenges - Carnegie Mellon CyLab and McAfee

9 http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2011.pdf

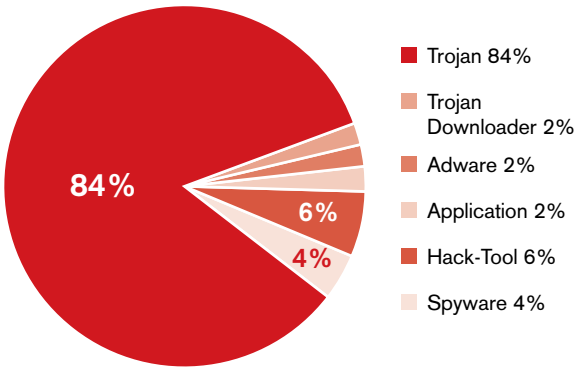
10 F-Secure Mobile Threat Report Q4 2011

devices include all the elements of an excellent covert monitoring tool. They are small, portable, and include microphones, cameras, speakers ,and storage capacities for SMS texts, recordings, lists of contacts, calendar entries and activity logs and copies of personal documents. They are connected to a radio data network on a 24 hour/365 day-basis that is managed and controlled by the network operator which can manage the network and the handsets, who access that network remotely with little to no oversight by the end user.

> "The most credible threat is coming from attackers who want to profit monetarily with their attacks, and right now we're seeing more profit-motivated mobile malware than ever before."
>
> Mikko Hyppönen
> Chief Research Officer. F-Secure
> Mobile Threat Report Q4 2011

The use of similar technologies by oppressive states should clearly not be ruled out. The capability of states to monitor and track owners of mobile phones has, significantly increased with the advent of mobile malware.

MOBILE THREATS BY TYPE, Q1 2012
F-SECURE MOBILE THREAT REPORT Q1 2012



The Federal Bureau of Investigation (FBI) released an advisory document in early 2012 with the title "Safety and Security for the Business Professional Traveling Abroad"[11] which clearly warns that,

> In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. All information you send electronically can be intercepted, especially wireless communications. If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained. **Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.**

Since mobile technologies are in widespread global use there is a large number of manufacturers designing, developing, and selling equipment to mobile operators, states, companies, and end users which can monitor and intercept mobile communications. There is a vibrant competitive landscape for the manufacture and sale of these interception systems.[12]

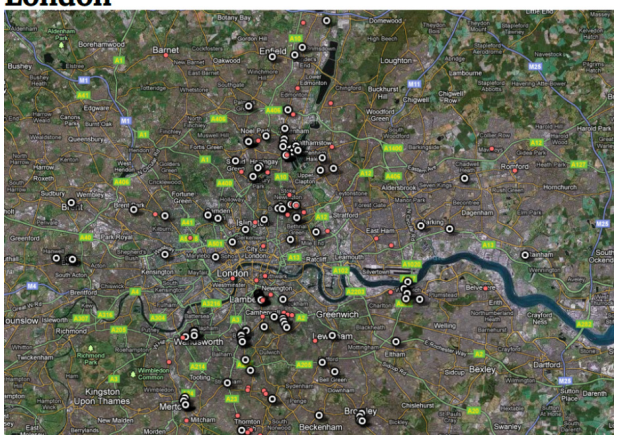
CROWD ANALYSIS

A byproduct of the design of the mobile networks is easy access to a large volume of profiling data on every handset in use on the network. This data can be easily processed to generate short term and long term profiles of the handset's user. The arrival of the smartphone has further exacerbated the range of data available and potentially accessible by the mobile operator, covertly and remotely, which includes all data stored on the device such as detailed GPS level location records and all data requested by and received by each handset.

11 http://www.fbi.gov/about-us/investigate/counterintelligence/business-travel-brochure (accessed 14 June 2012)

12 http://projects.wsj.com/surveillance-catalog/#/

London



Users often do not realize that combining all the log data from network towers, or of a large volume of handsets, enables the complex analysis of the phone records and the creation of crowd profiles, and a deep understanding of crowd dynamics. Applying crowd analysis and crowd modeling[13] theories to the data available from mobile networks with high penetration of smartphones is a dangerous tool in the hands of restrictive regimes.

With access to the relevant mobile operator databases it is possible for mobile phone networks to generate these maps in real time and to map movements of known suspects. This could be based on IMEI (International Mobile Equipment Identity) and/or IMSI (International Mobile Subscriber Identity) in conjunction with known registration details on the mobile database such as name, address, tax number (if collected), payment details (especially relevant for credit cards) providing interesting capabilities in conjunction with online mobile internet usage logs.

The use of video (CCTV, handheld or from mobile phone) recordings and telecommunications data, around riots and marches in two different parts of the world highlights the effectiveness and pervasiveness of modern technology in the state response to criminal or, in some countries, anti-government activities.

The Guardian Datablog[14] analyzed over 300 records of people on riot-related charges before English magistrates' courts to see where people lived and when the riots took place in London. The map shows where riots and looting took place in each part of the city.

CCTV cameras in London, recorded thousands of hours of video footage of looters and rioters. Operation Withern[15] at the Metropolitan (London) Police is an operation to collect information about those involved in the London riots. Photographs of the rioters were released to the general public in the hopes that witnesses will come forward to identify suspects. Assistant Commissioner Mark Rowley, MET Police, responsible for Specialist Crime and Operations stated that the "Metropolitan Police Service is determined

13 http://www.geosimulation.org/crowds/#overview The goals of the "Modeling crowd behavior " project are to build a reusable platform for modeling human behavior, action, and interaction in social and anti-social crowds, for the purposes of simulating a variety of behavioral, human, and urban geography scenarios. Modeling tools are being tightly-coupled to space-time Geographic Information Systems and social network analysis, for visualization purposes, but also for behavioral analytics. Substantively, simulations are being constructed around a variety of theory-driven scearios, with strong practical currency: human activity spaces, navigation and wayfinding in urban environments, complexity signatures in dynamic and adaptive socio-spatial systems, rioting and civil violence, hazards and emergency evacuation, crime and defensible space, retailing and business geographics, among others.

14 http://www.guardian.co.uk/news/datablog/2011/aug/11/uk-riots-magistrates-court-list

15 http://facewatch.co.uk/cms/app-public/

to exploit the opportunities presented by CCTV to solve crime. The general public can support us in this – both by providing us with images – and helping us to identify those who are responsible for comitting crime".

On August 9, 2011, the Guardian reported[16] that Everything Everywhere (T-Mobile and Orange brands), which operates more than a third of UK mobile phones, had begun receiving requests from police for information about the phones used to organize the wave of looting and riots that hit British cities under the Regulation of Investigatory Powers Act (RIPA). It is not hard to see why this would be requested: location data may confirm presence at one of these sites, and will clearly be used to build a case against an individual participant in these events, especially when combined with video footage.

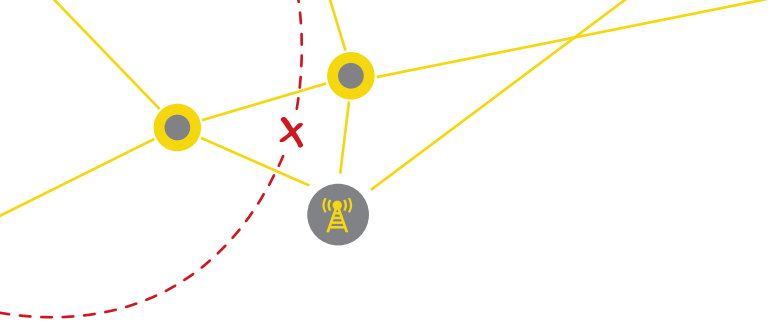
Secondly, in Iran, the Revolution Guard Cyber Defense Command (RCDC) use similar techniques to place photos online[17] and request that citizens identify rioters. It is clear that this type of technology is widely used for good and for bad and is part of the extensive international debate on dual-use technologies. As a result of concerns about dual use technologies, on April 23, 2012, US President Barack Obama issued an executive order[18] recognizing that,

> The commission of serious human rights abuses against the people of Iran and Syria by their governments, facilitated by computer and network disruption, monitoring, and tracking by those governments, and abetted by entities in Iran and Syria that are complicit in their governments' malign use of technology for those purposes, threaten the national security and foreign policy of the United States. The Governments of Iran and Syria are endeavoring to rapidly upgrade their technological ability to conduct such activities. All property will be blocked for persons

16 http://www.guardian.co.uk/uk/2011/aug/09/uk-riots-mobile-phone-operators

17 http://www.gerdab.ir/fa/pages/?cid=422 (last accessed 28 June 2012)

18 http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer



indicated in Section 1(a)(ii)(A) to have operated, or to have directed the operation of, information and communications technology that facilitates computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or the Government of Syria; or section (1)(a)(ii)(B) to have sold, leased, or otherwise provided, directly or indirectly, goods, services, or technology to Iran or Syria likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or the Government of Syria.

It is clear that the analysis and use of mobile data is increasing, both in democratic and oppressive regimes. The two examples above also highlight the problem of tools with dual uses. The identifation tool can be used to combat criminal behavior or can be used to surpress democratic movements. The US Global Online Freedom Act 2012[19] is an important element of future debate and strategy in the fight against abuse of technological capabilities in support of human rights around the world. The purpose of this act is "to prevent United States businesses from cooperating with repressive governments in transforming the internet into a tool of censorship and surveillance, to fulfill the responsibility of the United States Government to promote freedom of expression on the internet, to restore public confidence in the integrity of United States businesses, and for other purposes."

The examples show that it would be advisable to consider crowd sourcing technology in this debate.

SECURITY AND SAFETY STRATEGIES

Developing security and safety strategies for users of mobile handsets in countries with a poor history of respect for human rights is complex. There are several key safety objectives to consider:

- Do you want to protect the content of your communications?
- Do you want to prevent identification of who you are communicating with?
- Do you want to remain anonymous and undetected by the state security systems?

For example, it is often suggested that users should switch off their phone or use different phones or SIM cards to ensure safety and confidentiality. However, this advice is dangerously insufficient. It can be a trivial exercise for a profiling system to identify which handsets are switched off and on during times of identified risk and, in so doing, identify those persons requiring enhanced, in-depth, and regular monitoring. It is also trivial to identify multiple SIM's used in the same phone since the serial number of the SIM (IMSI) and the phone (IMEI) are both recorded by the mobile operators. Users with separate phones could also be identified by matching SIMs or phones that are frequently travelling together along the same route. Using different SIM's from different mobile operators does create an extra level of burden to governments attempting to analyze the log records. This is possible in countries where all the mobile operators are owned by the state or where legislation mandates unrestricted access to mobile records. Since SIMs from other states access the national mobile network can also be tracked. It should be clear from this example that creating a separate identity for each handset/ SIM card in use by the same person is expensive; requires sophisticated training, planning, and strict implementation; and is subject to user error over longer periods of time.

Security strategies also need to reflect on the intention or target of the protective measures.

- Do you need to protect your mobile activities from others in your close circle?
- Do you want to protect your mobile activities from

19 http://www.govtrack.us/congress/bills/112/hr3605#

employer, business partners, or competitors?
- Do you want to protect your mobile activities from state organizations?

SECURITY DESIRED → ↓ AGAINST WHOM	ANONYMITY and →	HIDE CONTENT OF COMMUNICATIONS and →	HIDE WHO YOU ARE COMMUNICATING WITH
Close Circle (family, friends)	Use unknown SIM Use unknown handset	Ensure physical privacy Encrypt messages and voice	Delete Logs prevent physical access to phone
Employer	Use personal handset and SIM Don't use employers equipment	Use obscure language Encrypt messages and voice	Use personalhandset from random location Use trusted intermediaries
Competitors	Vary communications channel	Use obscure language Encrypt messages and voice	Use handset from random location Use trusted intermediaries
State Organizations	'Throw away' handsets & SIM Vary location Crowd hiding	Use obscure language Encrypt messages and voice	Use trusted intermediaries

CAPABILITY ASSESSMENT REQUIRED

RISK ASSESSMENT

Performing a comprehensive risk assessment is complex. The purpose of a risk assessment is to identify potentially dangerous use of mobile technologies as accurately and comprehensively as possible. It should address the concerns of affected users and makes this risk information understandable and accessible. Inherent in risk management decisions are uncertainties and value assumptions about the nature and significance of the risk[20]. User's themselves will bring local information and relevant perspectives that are important to this process. The purpose of this report as a whole is to describe the range of risks at a political and technical level in the use of mobile handsets in different areas of the world.

The handset owner must consider all aspects of daily handset use and reflect how such use can be seen and recorded by persons with malicious interest in their activities. Risk mitigation must become part of the.

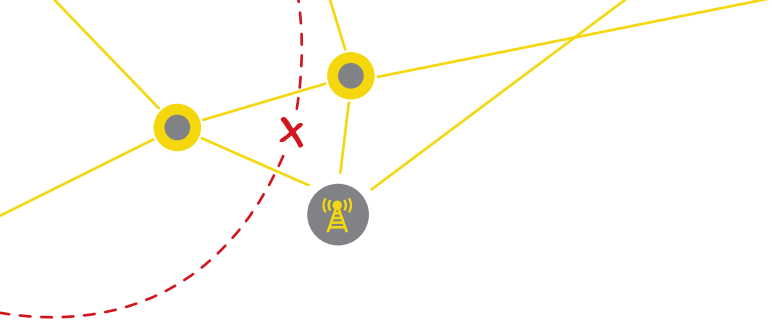
How could your phone be used against you in its everyday use?

- Data Recorded on phone and on mobile operator
  - Record of regular travel routines for analysis (using GPS location)
  - Record of all contacts, frequency of contact, duration of phone calls, types of contact (use contact database, call records, sms records)
  - Record of all emails, phone calls and SMS messages sent or received on your mobile phone.

CONCLUSION

Despite the risks inherent in mobile technologies there are still some good applications available. The mobile environment is still evolving and there are opportunities to influence this evolution to provide safer and securer solutions to users in high risk areas of the world.

20 http://www.irr-neram.ca/pdf_files/primer/communication.pdf

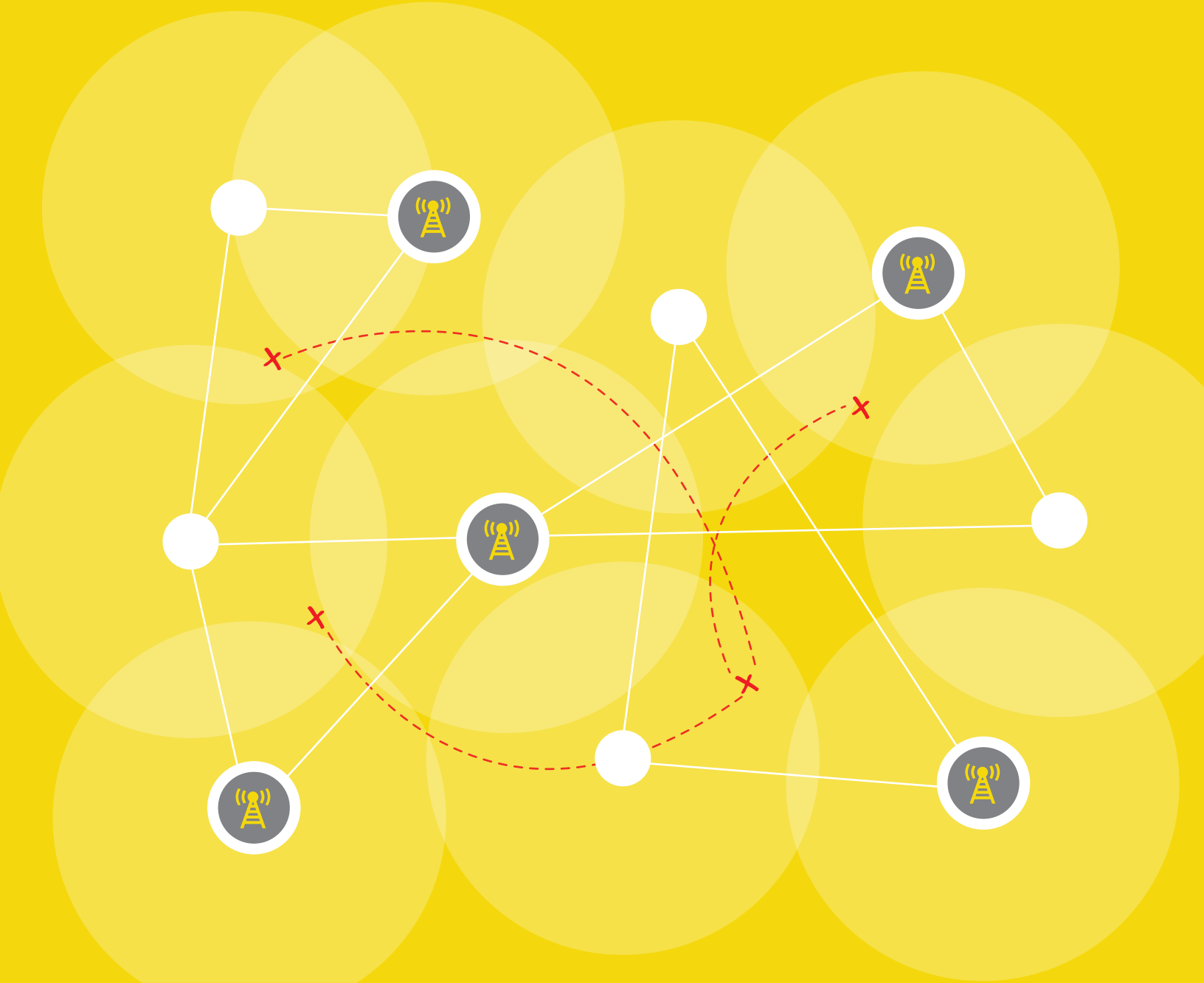


DESIGN CRITERIA FOR A GOOD SURVEILLANCE DEVICE?

- ✓ **Undetectable**
- ✓ **Lifetime battery life or renewable energy**
- ✓ **Audio/telephone surveillance**
- ✓ **Voice and conversation analysis**
- ✓ **Historical log records – local and remote**
- ✓ **In-field upgrades and repairs**
- ✓ **24/7 access to mobile, non-deterministic target**
- ✓ **GPS tracking**
- ✓ **Visual surveillance**
- ✓ **Hidden and trusted**
- ✓ **Remote verification records**
- ✓ **Remote access**
- ✓ **Remote backup**
- ✓ **Network of contacts**
- ✓ **Proximity Detector**

= a mobile handset, hiding in plain view, recharged by the owner, carried everywhere, even into the bedroom and the bathroom, fitted with all the right sensors, and receiving lots of care from the owner.

Chapter 3:
Background

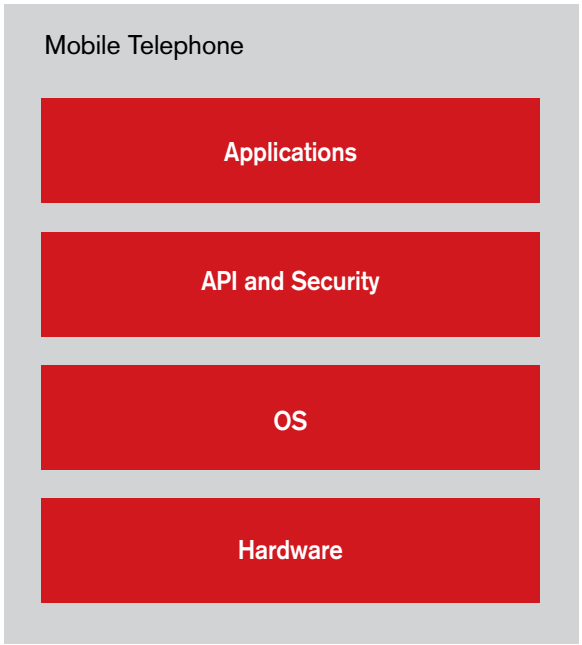


Background

This chapter will describe how the most common mobile internet hardware works, what networks it connects to, and will provide a technical background to these technologies suitable for the non-technical reader. This background will illustrate a model of the mobile internet environment that will be easy to understand and can be used to assess the specific threats that exist.

SMARTPHONES

Globally, access to the internet through mobile networks typically involves the use of smartphones or tablets. These devices have the means to connect to a variety of communications networks (most notably WiFi and mobile networks) and provide internet access to applications running on them.



Although laptops and netbooks are typically capable of accessing the internet through mobile or WiFi networks they were not part of the scope of this study. Our research shows that, in the countries we investigated, the usage of mobile networks to access the internet is not uncommon.[21]

The main characteristic that defines a smartphone is the ability to run applications that enhance its functionality above and beyond the common features of voice calling and text messaging. Essentially, a smartphone is a pocket computer rather than a traditional telephone. It is prone to the same risks and security threats that exist for a modern personal computer. The smartphone marketplace, however, is confined to certain points of sale, with several operating systems and an even greater variety of handsets available.

Although many different manufacturers of hardware exist, it is important to note that the basic functions and design of mobile phones is similar. The diagram above explains the various layers present in most smartphones. Note that the OS architecture and hardware platform typically vary for each OS, and that several sub-layers are left out from this diagram for the sake of simplicity.

HARDWARE AND OS LAYERS

Mobile phones run on a hardware platform that is capable of various types of digital transmission. The most common technology for this is GSM (Global System for Mobile communications), which has seen rapid development ever since its inception in 1987. It is almost universally supported worldwide. It has evolved over time to support the transmission of data according to several defined protocols (such as GPRS, EDGE, HSDPA and LTE), the characteristics of which will be discussed later in this chapter. In addition, smartphones typically support communication and networking through WiFi and Bluetooth as well as through cable bound protocols, such as USB and/or proprietary data exchange mechanisms.

The hardware is made available to the phone's

21 Two thirds of the expert survey responders reported that this was common in their country.

software or operating system, which is run on a programmable device similar to a computer. Typically smartphones have some added security features to ensure that the base OS (and firmware) software is not corrupted. A check is usually done by the operating system to see if any updates or changes to the OS software are downloaded from a trusted source (such as the manufacturer of the OS and/or the hardware).

The hardware itself often contains programmable areas, for efficiency and security purposes. The radio transmission hardware, for example, typically has programmable firmware to allow for the update of transmission methods. This enables "firmware updates" to be installed to the phone to enhance its capabilities (the phones baseband radio system is typically upgraded to save bandwidth or increase battery life, for example). It is important to note that these programmable hardware updates may happen outside of the regular OS update system, and often even without the users knowledge.

Typical parts of smartphones hardware include:

- A screen and (limited) keyboard
- A radio module for connections to the network
- A separate WiFi module for connecting to WiFi networks
- A GPS receiver to provide accurate location data
- Often, a local file-system and an adapter for reading and writing data to external sources, such as memory cards.

The operating system contains many of the most basic functionalities that require a smartphone to work with this hardware. It will, for instance, take care of storing settings and data on a file-system. Modern mobile operating systems usually provide ways to enhance security of this data through encryption. The OS also takes care of basic system protection (such as requiring a password and phone locking and unlocking mechanisms), data entry, and display functionality.

APIS AND SECURITY

Advanced programming interfaces, or APIs, are commonly used to allow applications on the device to use the functionality available through the hardware. The OS presents these hardware functions through unified APIs that enable programmers of applications to direct commands toward the phones hardware. They may, for instance, be used to (securely) store a password or to fetch a user's location from the built-in GPS sensor.

The use of APIs prevents applications from requiring direct communication with the underlying hardware. This enables the OS to implement security features related to applications using certain features. Apple smartphones, for instance, require certain actions to be confirmed by the user (such as when an application requests access to the user's list of contacts), and Android phones require users to grant permission to applications in order for applications to use certain functionalities during installation. The characteristics of these security features differ between smartphone operating systems.

For most mobile operating systems, specially designed software helps application developers make the most of the phone's functions. These software development kits (SDKs) are often supplied by the OS manufacturer, although cross-platform software development models are becoming increasingly fashionable. These allow developers to develop applications for several platforms at the same time, foregoing the need to port applications individually. Although this practice is more efficient from both a time and cost savings perspective, it may hinder full use of security features on the OS, which, invariably, are closely related to application design.

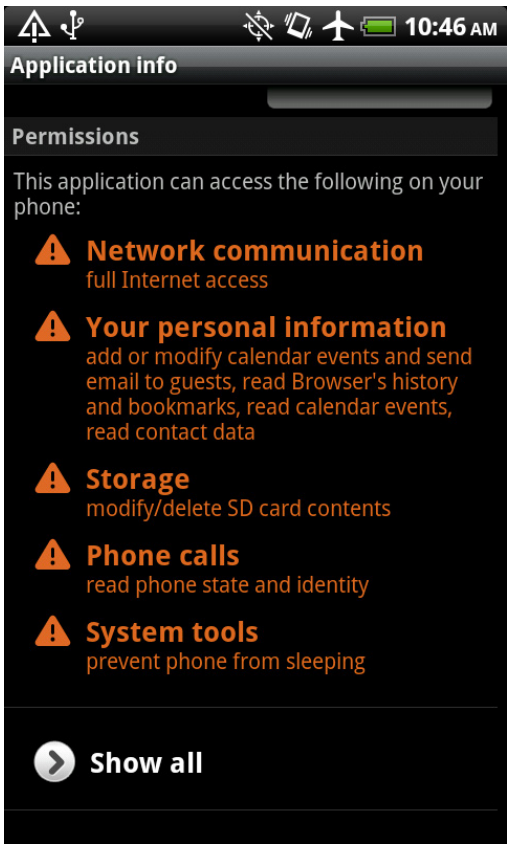
OPERATING SYSTEMS: DIFFERENCES IN ARCHITECTURE AND SECURITY

ANDROID

Android is an operating system for smartphones

developed by Google. It is based on the Linux kernel, although its architecture is far from the average Linux desktop computer in many ways.

Android employs a virtual machine layer to run the operating system (the Dalvik Virtual Machine, as it is called), meaning that the actual kernel is employed in a relatively secure environment. Applications can be developed for the OS in the JAVA programming language.



To create a more secure environment, such applications have limited access to each other, to the core OS, and to other phone components such as contact or location data. Not only are applications run with their own username (meaning they can only access a limited part of the phones file system) they are also restricted in communicating with each other or other mobile phone components by the operating system's security design. In order to achieve such "inter component" communication they need to negotiate access through a variety of APIs.

At install time, applications need to make their intentions known through what is called a manifest file. This contains the permissions the application would like to gain on the OS. The user can then decide if he is willing to trust the application with these resources. Only when a matching entry is found for the specific component can the application contact that specific resource. In other cases the operating system should disallow the communication. Google refers to this as the Application Sandbox and Permissions model.

Android users depend on their network provider as well as the hardware manufacturer for updates to the phones core OS. Although Google regularly releases updates for the Android OS, it is up to manufacturers and operators to test, accept, and implement them on the hardware they supply. Due to the large number of handsets with different versions of Android operating systems that are shipped, many phones never or only rarely receive updates over the air. A recent overview showed a majority of phones had still not received the latest major version update within a year after their release.[22] Also, due to the large number of Android versions on the market, support of the latest OS features cannot be guaranteed for application developers, meaning they will often be inclined to write applications for the lowest common denominator. This is especially problematic for security measures (such as file system encryption) that are only implemented in later releases.

Android supports multiple application repositories, although the one maintained by Google itself (currently named Google Play) is universally installed on Android phones. Google has been criticized for not monitoring its application store (Google Play) enough to identify

22 http://theunderstatement.com/post/11982112928/android-orphans-visualizing-a-sad-history-of-support (Last accessed 15 june 2012)

malicious applications, and has since made limited improvements to Google Play. Applications installed through Google Play can be uninstalled (revoked) centrally.

Android natively supports different VPN protocols and, as of version 3.0, has native support for file system encryption (so far this is meant to be used primarily for application data storage and not for encryption of the entire OS file system).

Applications deployed on Google Play must be digitally signed, ensuring the identity of the author. However, there is no requirement that the code be signed by a third (trusted) party; self-signed certificates can also be used to sign application code, so no check on the identity of the author is performed. There is a limited automated scan of the applications in place to prevent malware, but compared to Apple's App Store, the checks on the applications in the Play store are less rigorous.

The boot up of the Android OS is often secured on the device using code signing (the key being used originating from the device manufacturer and installed in the hardware). This feature is commonly hacked in order to install "after market" versions of Android, developed by an active open source development community. Often, these also require the user to gain "root" access, a practice known as "rooting." The root user has the ability to use access all features of the OS and, therefore, this procedure breaks some of the user based permissions for apps that were mentioned earlier.

IOS / IPHONE

iOS is the operating system that drives Apple's iPhone, iPad, iPod touch and Apple TV products. The version available in June 2012 was iOS 5.1.1, although it is not uncommon for Apple users to maintain older iOS versions on their devices.

Much like Android, Apple also employs a virtual machine to run the operating system's core components. This allows for enhanced security features that limit applications from breaking out of a restricted environment and accessing core OS features.

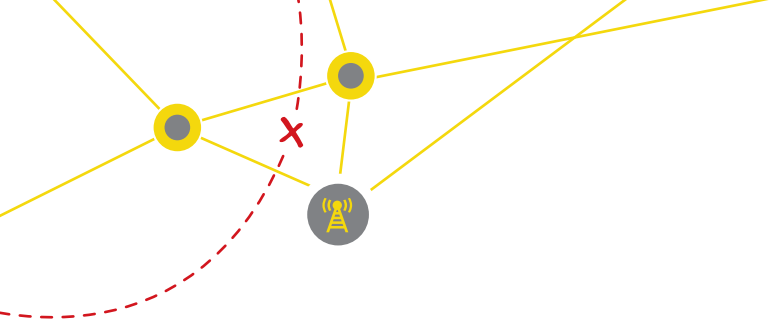
Permissions management is less focused on the installation process, rather permission for access to certain resources is specifically requested from the user where privacy-sensitive data is involved, such as access to location data services or the contact list. However, Applications do have a set of "entitlements" describing the resources they require.

Since version 3.0, iOS supports the Apple App Store, a repository containing many applications that can be downloaded and run on iOS devices. Applications in the App store are tested by Apple and only allowed under strict conditions. One of these is that a developer has to submit his photo ID before being allowed to submit applications.

iOS 5 employs file system encryption by default, and manages the keys required for unlocking files on the device in different key chains. By only unlocking these keychains when needed for certain apps, the risk of someone accessing these protected files while the OS is running, but locked, is somewhat mitigated. Unlike Android, the encryption of the file system covers the entire storage volume (Apple does not support the use of separate memory cards).

The iPhone supports similar VPN technology as Android (L2TP/IPSEC and PPTP), but has a much better track record in maintaining and updating previous iOS versions, also due to the ubiquity of its hardware.

Code signing is implemented in much stricter fashion in the Apple App Store: every application has to be



countersigned by Apple and the signature of the application provider is matched to a real world identity. Apps can only be developed in C, C++, or Objective-C. Applications are tested rigorously, and a requirement that in-app payments flow through Apple adds a further check on malicious application behavior.

The OS's origin is also checked using cryptographic keys at boot time in order to ensure it was signed by Apple. For this function an Apple certificate is built in to the phone. The BootROM of most iOS versions can be hacked, however, to enable customizations to the OS that would otherwise be impossible. In Apple-speak this is called "Jailbreaking" and is, in effect, similar to "rooting" an Android phone.

SYMBIAN

Symbian is a mobile OS series developed by Nokia and based on earlier operating systems (the EPOC series) from mobile device manufacturer Psion. It has a much longer track record than both Android and iOS, and is still in wide use on many devices today. Despite Nokia recently favoring Windows Phone 7 as its flagship OS, it is by far the most common OS for Nokia smartphones, and is still the most widely distributed smartphone OS in many markets.

Symbian's base OS runs in a slightly less protected environment compared to Apple and Android, making it more susceptible to attack by mobile viruses. Some of the first mobile viruses to see wider distribution targeted from this platform (such as Cabir in 2004, which simply displayed the text "Cabir" on startup but was otherwise harmless). It does have separate storage permissions per application, but lacks the dedicated virtual machine for the OS. It was the first smartphone OS to be successful at multitasking, and has seen significant development over the years with many different versions having been marketed.

Symbian's design is renowned for efficient memory and resource usage, and it is still a reference OS for true multitasking ability (the ability to run several applications real time at the same time, sharing system resources). Multi-tasking had been difficult in early Android and iOS versions).

Unlike other smartphone operating systems it is quite common for Symbian apps to be distributed outside of the OS manufacturers' marketplace (the latest reincarnation of which is called the OVI store). Instead, 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. Most permissions however can be granted by the user on install. Nokia currently signs most Symbian apps for free. Development can be done in several languages. Symbian has limited VPN support and only supports native IPSEC VPNs.

BLACKBERRY

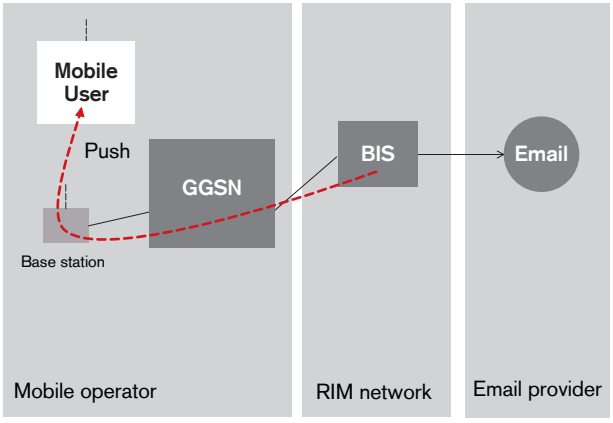
BlackBerry, the operating system that drives all RIM BlackBerry devices, was developed with (corporate) security in mind. While adoption of the technology was at first driven by larger corporate players, wishing to secure both email and data traffic, BlackBerry soon became the platform of choice for non-corporate text-based communication as well.

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 communication between its services network and the BlackBerry hardware.

For email and calendar sync, the dominant apps for the BlackBerry users, RIM provides a push mechanism through which messages can be delivered to a BlackBerry device upon delivery to the (provider or corporation based) BlackBerry/RIM server. The option for non-corporate BlackBerry users is called BIS, or BlackBerry Internet Service (as opposed to the corporate "BlackBerry Enterprise Server (BES), which integrates similar technology into corporate networks).

This method is "relatively secure" when implemented inside a corporate network using unique keys specific for the enterprise, and when no traffic leaves the organization. However, these conditions do not apply to BIS users, and so their use of BlackBerry devices is much less secure.

For a regular POP3 email service, for instance, usually only unencrypted, plain text username and password are used to retrieve email. Although these will perhaps be safe in the hands of RIM, operating their own infrastructure (as in the diagram below). For protection against many other threats, the non-corporate use of the BlackBerry infrastructure is only as secure as the link between the RIM service and the email provider of the BlackBerry user. RIM also emphasizes that the connection to the BIS infrastructure itself is also unencrypted:[23] "Email messages sent between the BlackBerry Internet Service and the BlackBerry Internet Service subscriber's BlackBerry smartphone are not encrypted. When transmitted over the wireless network, the email messages are subject to the existing or available network security model(s). When you log in to the BlackBerry Internet Service, the data is transmitted over a Secure Sockets Layer (SSL) connection."



23 See the RIM knowledgebase: http://btsc.webapps.blackberry.com/btsc/viewdocument.do?noCount=true&externalId=KB03652&sliceId=2&dialogID=3718757&cmd=displayKC&docType=kc&stateId=0+0+3716689&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl

So while intra-corporation-BlackBerry-service-traffic may be secured, and the device's data can be encrypted, security is only achieved if it is implemented end-to- end by using BES.

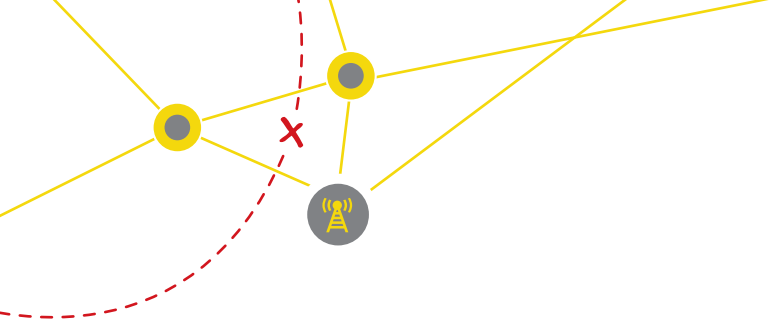
BlackBerry Messenger (BBM) is encrypted in a similar fashion: it can be encrypted using a company key in the BES environment, but in the BIS environment, users have to fall back to a global encryption key, which allows decryption on any BlackBerry device. RIM can therefore provide access to these messages as they are relayed through its services.

As would be expected, BlackBerry uses code signing and various other security features to secure its mobile operating system. Unlike Android and Apple, it is neither easy nor common to "jailbreak" or "root" BlackBerry devices. They implement encryption for data in transit (the BlackBerry internet service) and on the device (file system encryption is used when the device is locked). File system encryption is not enabled by default, however, again leading to a situation where only corporate users appear to receive maximum protection.

Since encryption is supposed to be a feature of BIS and BES service by default, BlackBerry supports no external VPNs (although custom VPNs to the BlackBerry Enterprise service can be set up through a management interface).

WINDOWS PHONE

Windows Phone is the successor to Microsoft's Windows Mobile series of mobile phone and PDA operating system. Although it has a distinct name, and is actually a new operating system, built from the ground up and, hence, not a successor to the older Windows Mobile OS (similar the current Windows version), it is often called Windows Phone 7. Unlike the desktop based Windows versions, Windows Mobile applications are incompatible with Windows Phone 7 (even from the latest version, WM 6.5).



Similar to other modern Smartphone OS's, Windows Phone uses the concept of sandboxed application execution. This means that applications do not have direct access to each other's data, nor to most core phone functions such as location services or address book entries directly. They must use a strictly defined API for this and are also restricted to their own data storage.

Windows Phone uses code signing and strictly limits app distribution to the Windows Phone Marketplace. Apps can be developed using Microsofts .NET platform.

A key design feature of Windows Phone 7 is real-time information displayed in tiles on its start screen. This interface (also known as the Metro interface) is to be introduced in Windows Desktop OS as of version 8.

Although Microsoft has an extensive partnership with Nokia for further development of Windows Phone OS, other manufacturers have also launched devices based on the OS.

Mobile Networks

INTRODUCTION

Mobile networks have evolved rapidly in recent decades. While the first commercial GSM networks were deployed in the nineties, today these networks have global reach and have become the standard for mobile communications the world over.

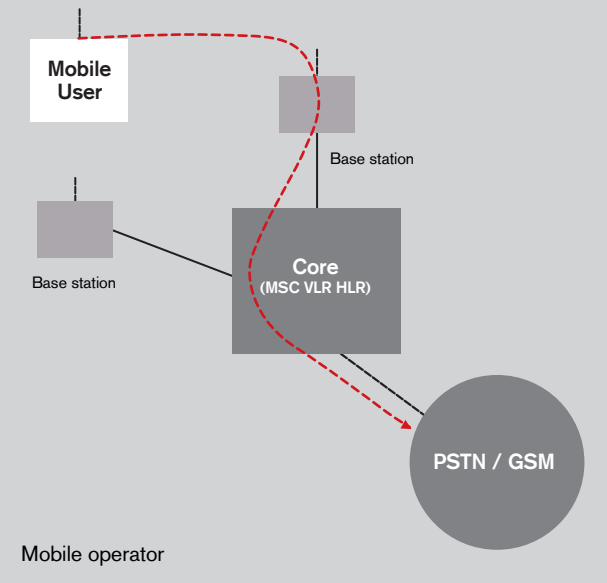
By far the largest contributor to the success of mobile telephony (and later SMS and mobile internet access) was the relatively low cost of rolling out the required radio networks. Although the cost of handsets slightly mitigated this advantage, broadened access to ubiquitous, standardized (GSM) networks turned mobile telephony into one of the major milestones of 20th and 21st century communications.

VOICE

As the first service provided on any mobile network, voice calls are the basic service expected on every handset and network.

Voice calls on mobile networks are carried over a radio network that operates in regulated frequencies. Digital transmission technology enabled ETSI, the European Telecommunication Standardisation Institute, to devise a standard that allowed expansion and upgrading more easily than was possible in the age of analog radio telephony. This standardization led to several services being added on to the original GSM design that enhanced and upgraded its capabilities, both in terms of network efficiency and in capability.

GSM is based on a modular design in which a transmission network consisting of base stations relays calls from mobile equipment to a core network. This network enables such functions as call routing and interconnects with other networks, and has been upgraded to handle data connections (today mostly internet access) and text messaging (SMS).



The core of the network handles call routing and enables the GSM phone call to move from base station to base station without interruption of (most) active connections. Due to the ubiquity of the GSM protocol it has become common practice to have national (and international) roaming agreements, whereby users from one network are allowed to connect to and use other networks. Their presence in various networks is registered in both the visited network (in a VLR, or Visitor Location registry) as in the home network (HLR, Home Location Registry). Billing is invariably done through the home network, so intricate use of various identifiers was required to enable roaming while maintaining a unique customer relationship between the home network and the user.

The typical identifiers that are used are:

- IMSI – the International Mobile Subscriber Identity, which is unique to the SIM card of a mobile phone. A temporary version (TIMSI) of this gets created so that the operator does not to have to use the original in network radio traffic.
- IMEI – The International Mobile Equipment Identity, which uniquely identifies mobile phone equipment. This is hard coded in mobile phones.
- MSISDN – the unique mobile telephone number belonging to the combination of the latter. This number is assigned by the network core upon connecting to the GSM network.

GSM ENCRYPTION

Encryption of traffic is also described in the standard. All voice communications are encrypted with the A5/1 or A5/2 protocol, the latter being a deliberately weaker crypto algorithm used for export outside US and European markets. A5/3 became available later (based on the Japanese MISTY1 algorithm) but is currently not in widespread use.

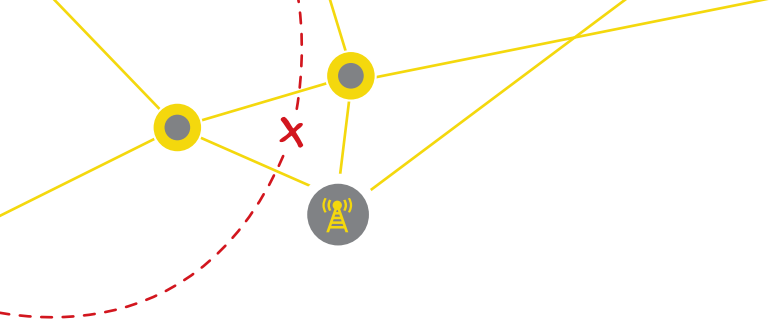
For the purpose of encryption, a fourth important identifier is linked to each user: a secret key that is known to both the user device, as it is built into the SIM card, and to the network that issued the SIM (HLR). The A5 algorithms use the key to create session keys.

Using cryptographic attacks on A5/1 and 2, Elad Barkan, Eli Biham and Nathan Keller released a paper that described practical attacks against implementations of these algorithms in modern mobile phones. They not only broke the algorithm, but also showed that in real world implementations, phones can be made to downgrade to lower cryptographic standards. Although this is often required to remain interoperable with all GSM networks, this also meant that the weakest algorithm could be used to crack a conversation. Since the same key is used in all protocols, this hack effectively breaks even the upgraded algorithms, if they are used in later sessions.[24]

Besides the deliberately weaker cryptography often found outside of the US and Europe, a host of attack strategies against A5/1, has recently rendered relying on default A5/1 GSM cryptography hazardous at best.[25]

24 Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication? Elad Barkan1 Eli Biham1 Nathan Keller, see http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf

25 See, for instance the presentation of Karsten Nohl and Sylvain Munaut deliverded at the 2010 CCC congress http://www.youtube.com/watch?v=ZrbatnnRxFc



Certain practices of mobile network operators leave mobile users open to attacks. They often leave the generation of new authentication keys and generation of new TIMSI numbers set to a large interval, whereas these were envisaged to change per call. Next to this they send many predictable messages making cryptanalysis of the network traffic much easier. Until the implementation of added measures and new A5 cryptographic ciphers for GSM, voice encryption should be considered easy to break. Since cryptography is only applied to secure the wireless part of the call, it is also by no means a measure against state monitoring, since the network itself can, of course, decrypt the call and relay it.

SMS

SMS was first invented as a byproduct of modern GSM networks. It enables the use of the signaling network between a mobile station (a user device on a mobile network) and the GSM network to deliver short (up to 140 or 160 characters) messages. For interoperability, the common signaling system between carriers was initially used as a transport (Signaling System 7 – SS7).

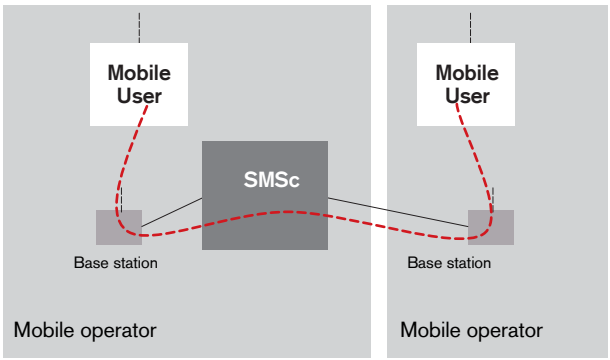
The main idea behind SMS is that it allows short messages to be delivered outside of the voice band of the network. Since the signaling network usually has some extra capacity, SMS made very efficient use of the network infrastructure.

The uptake of SMS service soon dramatically exceeded expectations and further work has been done to optimize the delivery of messages. In modern networks, the transport for these messages is no longer necessarily based on the signaling network, but often involves IP-based protocols that allow direct communication to (or between) SMS Centers (SMSCs) and mobile stations.

SMS messages are sent and delivered to mobile phones using a store and forward-type messaging protocol. The main network element involved is the SMSC, which, in a mobile telephone network, handles all messages sent by its users. The mobile station – a mobile handset, in most cases – first submits a message to the SMSC, which then starts a delivery attempt.

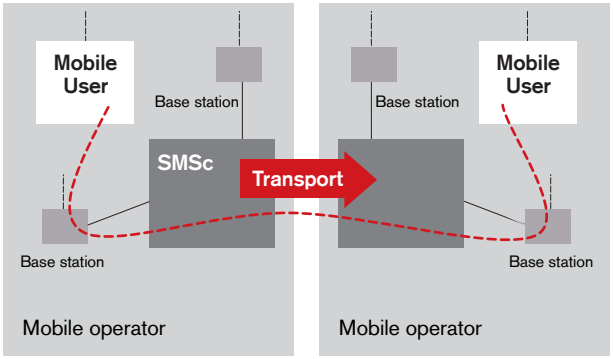
The original configuration of SMS routing only envisaged one SMSC involved in the delivery of a given message, so most carriers would have agreements in place to allow the delivery (termination) of messages. This, however, lead to “abuse” by certain SMS gateways, when certain network operators allowed messages to be sent through their network for destinations worldwide.

Also, more and more fraudulent traffic gets sent through SMS and this design means there is no opportunity for the “terminating” network to control the influx of text messages. What is worse, for this system to work, the SMSC needs access to the terminating mobile station’s Home Location Registry (HLR), where details are kept on the user’s whereabouts. For this purpose, this database is therefore opened up to anyone that has access to the SS7 (inter carrier) signaling network, creating a significant privacy risk.



A technology called home routing of SMS messages was therefore developed to prevent many of these drawbacks. In this model, messages take a path across multiple SMSCs (or other SMS network elements, increasingly IP-based protocols). Increasingly, IP-networked infrastructure performs the transport of messages, rather than the SS7 signaling layer. Also, receiving operators in the direct delivery model are

exercising control over who can deliver messages to them, usually requiring "SMS interworking" agreements to be in place before allowing delivery to their customers.



The fact that messages are always routed through the home network makes this model safer from a privacy perspective.[26] In the standardization documentation for home routing, special mention is made of the requirements often imposed by/for law enforcement, that providers must be able to deliver all text messages for a specific subscriber. So in effect, this model also brings with it the rule that control and access to text messages is handed to both sending and receiving carriers, and makes exercising control over messaging a more centralized network feature.

Although encryption of SMS messages by the GSM algorithms mentioned earlier was foreseen in the standardization track, it is optional, and the universal cipher that is used for this optional encryption is inherently weak so that anyone with the right (and fairly cheap) equipment can inspect messages sent on the fly if they are within range of the transmitter.

MOBILE INTERNET ACCESS

Mobile internet access has evolved over time from a relatively slow "dial-up mode" transmission method to high speed broadband connections that are in use today on 3g and 4g (LTE and WIMAX) networks. In order to understand the development of this technology it is important to note that the development of this technology is often taking place in richer, western markets.

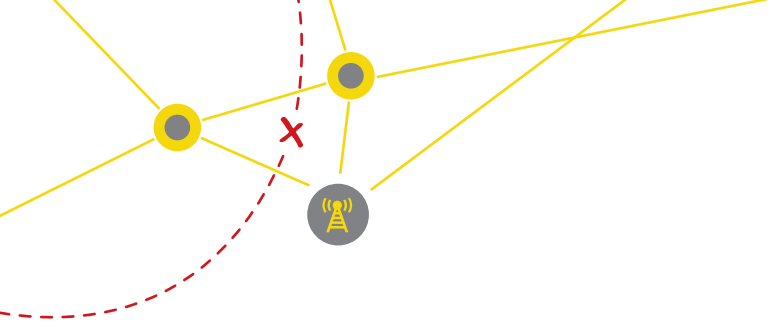
Uptake on other markets, however, usually follows closely behind and, due to the relatively low investment of setting up a mobile network, mobile technology has been quick to arrive in less developed markets. To better understand the development of each country's mobile internet market, the following section provides a description of the main technologies in use. The country profile for each market, presented later in this report, describes the predominant access method.

DEVELOPMENT OF TRANSMISSION TECHNOLOGY

The old analog mobile telephony standards used a very simple method to transmit audio: a single channel (frequency) was given to a single user. In order to make frequency usage more efficient, GSM, one of the earliest digital mobile phone standards, shares a single channel among several uses. This is done using a technique called "time division multiplexing" (TDM), wherein the devices take turns transmitting on the channel. Each device has a fixed "time slot", similar to how a TV channel broadcasts different programs at different times. With GSM, every radio channel is shared by up to eight users, who are each assigned a time slot.

The earliest data service over GSM used the same time-slotted circuit as the voice service, for data speeds of 9,600 to 14,400 bits per second. The later High-Speed Circuit-Switched Data (HSCSD) data service allowed the use of multiple time slots concurrently, for increased speeds of up to 57,600 bits per second. However, HSCSD was still hampered by the limitations of circuit switching, where a user is assigned a fixed amount of time to transmit and receive, irrespective of the data bursts and quiet periods that are both common in most data communication. The user was generally still billed per minute.

26 The 3G forum 3GPP TR 23.840



A later addition to GSM was the General Packet Radio Service (GPRS). With GPRS, the time slots not used for regular circuit-switched voice or data are used to carry packet switched data, allowing for faster transmission of individual packets and better bandwidth utilization because a user with a lot of data can make use of the capacity left unused by other users who are temporarily idle (statistical multiplexing). GPRS speeds are up to 56 to 114 kilobits per second shared by the users on a channel. GPRS is a software upgrade to standard GSM. By today's standards, GPRS is considered very slow. GPRS is (almost) universally supported in GSM networks as the lowest common denominator mobile internet access mechanism.

The next step up from GPRS is Enhanced Data rates for GSM Evolution (EDGE). EDGE introduces newer ways to modulate the radio signal that allow more bits to be transmitted per unit of time under good conditions, increasing the data rate by a factor three over GPRS. GPRS to EDGE is a larger upgrade than GSM to GPRS, but EDGE is still completely compatible with GSM and GPRS. However, EDGE support is far from universal, with some networks even removing the EDGE capability in recent years.

UMTS is the successor to GSM, but it uses a completely different method to transmit signals over the air. This means that GSM and UMTS cannot coexist on the same frequency. (In fact, the definition of what constitutes a radio channel is very different between the two.) However, UMTS and GSM share many higher-layer protocols, so it is possible to have seamless handovers from UMTS to GSM, and the other way around. So a user may start a session on UMTS but then drive outside the UMTS coverage area. The connection will not be lost, but will be handed over to the GSM network using GPRS or EDGE.

UMTS no longer uses fixed time slots, but rather wideband CDMA (W-CDMA), which allows multiple users to transmit at the same time. The original UMTS data rate is 384 kilobits per second, but this is per user rather than the per channel rates shared by multiple users for GPRS and EDGE.

UMTS received backward-compatible enhancement in the form of High-Speed Downlink Packet Access (HSDPA) and High-Speed Uplink Packet Access (HSUPA). When used together, they may simply be referred to as High-Speed Packet Access (HSPA). HSDPA increases the downlink speed (from the network to the user) to typical values of 3.6 or 7.2 Mbps with future extensions to 21 Mbps and higher planned. HSUPA increases the uplink speed (from the user to the network) to 2 or 5.76 Mbps with further extensions planned.

In most documentation GSM is referred to as 2G, being the second generation of digital mobile networks. UMTS is 3G. Sometimes GRPS is called 2.5G and EDGE is called 2.75G, with HS(D)PA being 3.5G.

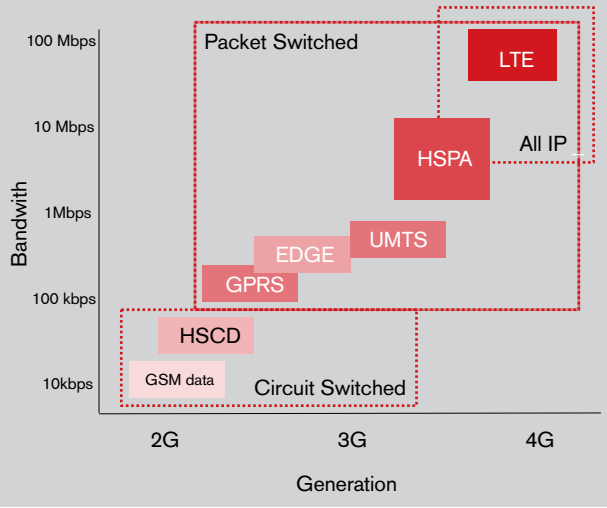
Fortunately, the naming convention for the next generation of all the aforementioned technologies is more ubiquitous. The next generation (4G) will be 3GPP Long Term Evolution (LTE), which will provide much higher data rates than 3G. It will also allow the network infrastructure to be based on cheaper IP based hardware and will make use of the internet protocol in its internal components. LTE is currently in early-stage deployment in many developed markets, and will be rolled out fully in the coming years.

An important feature of LTE, which may also appear in future releases of UMTS, is that is was conceived as an "all-IP network." Not only will the network be IP based, it may increasingly feature handsets communicating exclusively over IP based networking links as well (through VOIP and IP-based messaging, for instance). It will therefore be required for LTE equipment to have an IP address assigned from the moment it is switched on and attached to the network.

Note that in LTE networks, the central internet gateway and supporting nodes have slightly different names although they still perform roughly similar functions to

their 3G counterparts (a PDN Gateway hands out IP addresses instead of GGSN for instance).

An overview of the transmission speeds of the various technologies is provided in the following diagram.



Although the all-IP network is important from the service provider's perspective, because it means being able to use off-the-shelf IP devices such as routers, for users this probably won't change much as user packets will still be carried as payload in IP packets flowing through the service provider's network in tunnels.

Using direct IP communication (instead of tunnels) towards the user would limit the way mobile networks can be built and could have adverse security implications. For this reason, all traffic inside mobile networks can be easily correlated to an individual user. This is not only required for billing, but can also lead to easier identification of individual usage patterns.

ARCHITECTURE

From a user (or rather, a user's networked application) perspective, all services from GPRS to HSPA are the same. This means that all mobile network connections are set up in the same way and only the last mile (the radio transmission part of the connection) is different across the generations of data network access technology.

Provisioning network access for mobile data in modern networks (3G/UMTS or 2G/GPRS) therefore happens very much on the fly. In view of the need to reduce the usage of the available spectrum (the scarcest and often most costly resource of mobile networks) a connection is set up only when an application actually requests access to the internet.

When this is noted on the mobile device, a "PDP context" is set up on-demand as the mobile device initiates network activity. The PDP context is a mechanism that retains data on the session's specifics on the network side. This allows for better handover of connections between various base stations or even between transmission technologies (where these are compatible).

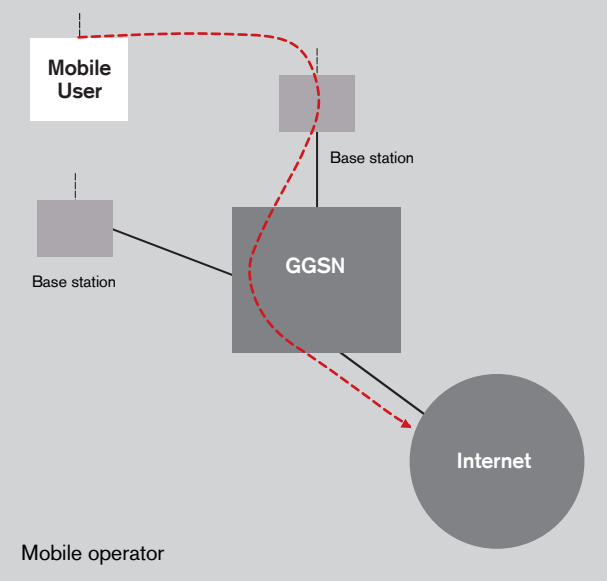
An address is assigned to the mobile device by the system that terminates the other end of the PDP context: the GGSN. This is the device that connects mobile clients to the wider internet and allows for accounting and traffic management within the mobile network.

The IP address remains assigned to the mobile device while the PDP context lasts and is released as soon as the PDP context is explicitly torn down or lost for some other reason. Mobile devices will typically tear down the PDP context as soon as applications cease network communication to preserve resources. However, although not common today, PDP contexts may remain active for some time even though network sessions are idle. There is no (or very little) radio traffic in this case.

In many cases the addresses handed out to mobile users are private addresses, meaning they will have to be translated to be usable on the wider internet. This means that correlation of externally visible public IP addresses (usable on the internet) with specific devices (with private IP addresses such as 10.x.x.x or 192.168.x.x) becomes hard for parties that do not have access to the logging that takes place in the network.

The mobile operator and, through the mobile operator, third parties (such as law enforcement bodies) may obtain a correlation between an IP address used at a certain date and time and the user's identity. Within the mobile network, the MSISDN (the mobile subscriber's phone number) is used as a unique identifier for billing purposes and the like. The figure below shows a schematic overview of a mobile network.

It is important to note that traffic inside the network is typically carried in tunnels in order to identify the traffic, and the originating MSISDN in the GGSN and related billing infrastructure. This means that all traffic is passed in a very identifiable manner through the GGSN before reaching the edge of the provider network. This provides the operator, and those exercising control over the network and it's users, with a very convenient location where a user's traffic can be easily monitored, blocked, or otherwise intercepted.



BLOCKING AND MONITORING

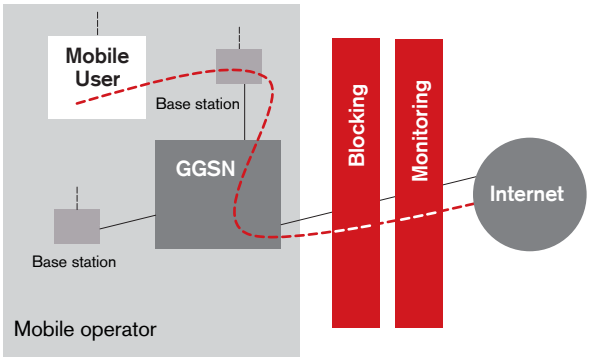
Blocking is the practice of stopping traffic from reaching an otherwise accessible destination. It is usually done as an act of re-territorialization in which states seek to prevent citizens from accessing global content that violates national laws or standards.

Monitoring is the practice of listening in on voice, text, or data conversations taking place on the network. In the case of data networks it can be easily automated using pattern recognition in the data stream. Deep packet inspection, a technology whereby every packet is read and analyzed, is often required to employ this type of monitoring. In the case of voice traffic it is often impossible to fully automate the task of extraction of the most relevant information, due to the resource-intensity of speech recognition.

From a technical perspective, blocking can be performed in many different ways.

The most important characteristic of blocking in the context of this report is the level at which the blocking is taking place. In many day-to-day internet applications there is blocking functionality present for a different number of purposes. Examples of these are e-mail services, which have spam blocking capabilities, and child pornography blocking lists, which are employed by internet service providers in most countries. In democratic societies that avoid censorship, most users have a limited need to circumvent this type of blocking.

For the purpose of this report, the focus is on blocks preventing the sending or receipt of specific content at a national level. This type of blocking is frequently employed in repressive regimes, where the primary purpose is to limit access to certain content the regime deems politically undesirable. Since the practice of blocking requires significant infrastructure to control all traffic flowing through the network, it is often combined with similar monitoring capabilities, employed at the same level. The technical infrastructure required for this is significant. A functional diagram representing such blocking and monitoring infrastructure on mobile networks (for the data infrastructure) looks like this:



There are significant differences in the blocking and monitoring schemes of the countries we studied in this report. The fact, however, that the central government wants control of the characteristics of the blocking means that generally a central blocking list or set of criteria is present. In some countries, the application of such a list is effected by centralizing the infrastructure so that all internet access of both mobile and fixed networks takes place through government controlled networks or central nodes. In other countries the block is implemented by imposing requirements on service providers offering service in the country.

Either way, an operator or government implemented blocking system will need to be fed with characteristics (like keywords or internet addresses) of the content to be blocked. When such a characteristic is found, the block is implemented and the content made inaccessible. At the same time, details that could identify the user accessing the content are often logged by authorities for later analysis, monitoring, or in some cases, prosecution.

Monitoring of voice traffic is not uncommon, though pro-active blocking is a rather rare phenomenon for voice traffic.

IDENTIFIERS OF CONTENT

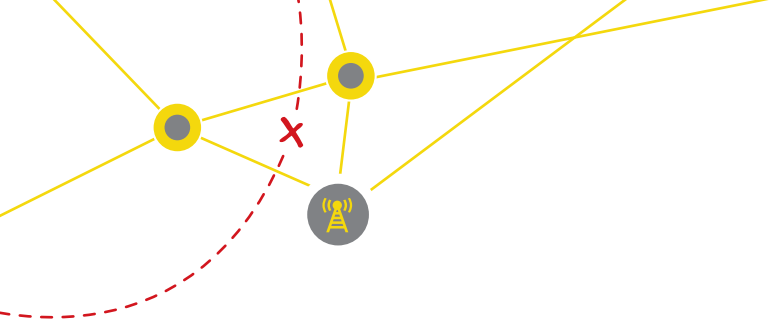
In order to attempt to block content or identify targets to monitor, identifiers are needed whereby a blocking (or monitoring) decision can be implemented. For mobile networks these are not very different from "normal" internet access blocking. The following identifiers are in common use:

- **IP Addresses -** Blocking an **IP address** means that other internet services and users that use the same address will also be blocked.
- **Domain-Names -** Blocking by a domain-name will block **all** content residing under that domain.
- **Uniform Resource Locators (URL's)** – The most specific blocking can be achieved by filtering on a URL basis. Due to the ease of evading these filters, blocking by this identifier can lead to under-blocking.
- **Content Signatures -** Content can be blocked using signatures that allow for classification of content flagged as illegal. New content is easily missed by the filter. Encryption of the content will render this method useless.
- **Keywords -** Blocking based on keywords found either in the filename, the URL or the text at the location of the content being accessed. Complex analysis of the recognized keywords in the context of their use needs to be performed.

SMS and MMS blocking is sometimes also implemented. This is usually based on keywords.

Since mobile networks produce more limited sets of data, blocking implementations on these networks often do not suffer the same scalability and over-blocking problems.

This table lists characteristics of every blocking strategy discussed. It shows the likelihood of over- and under-blocking according to our estimates, lists the resources required to execute the blocking strategy, the block-list type, and maintenance effort required for such a list and, in the last column indicates whether the communications contents needs to be analyzed extensively for this strategy (DPI technology or alike) for blocking to be effective.



MEDIUM	BLOCKING	EFFECTIVENESS				BLOCKLIST		DPI
		Over-Blocking	Under-Blocking	Resources Required	Circumvention	Maintenance Effort	Identifier	
Web	DNS	Very Likely	Likely		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	+

MOBILE SPYWARE

The monitoring layer represented in the previous diagram is restricted to network based monitoring. Although this is often employed and should not be discounted as a major threat for users under regimes employing such technology, the mobile phone hardware and OS are increasingly under attack.

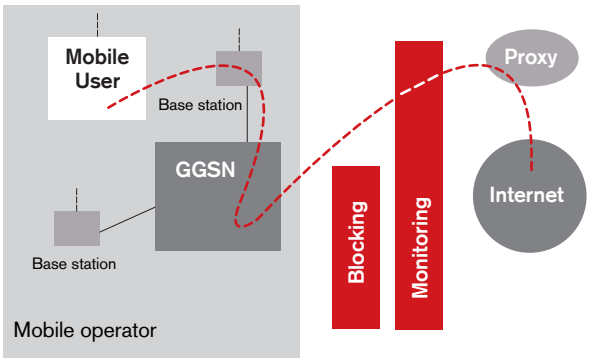
With the advent of smartphones with stronger processing power, more and more investment is being made in device-based monitoring strategies. This kind of monitoring makes use of vulnerabilities in the various layers of mobile phone hardware in order to install malicious software or functionalities that can be used to monitor both data and communications emanating from the device.

At the application layer, for instance, it has been observed that targeted threats against individual phones are attempted by both state and non-state actors. In this category we could, for instance, think of states employing "trojan" copies of well-known applications, either through online application repositories (Apple App store, Google Play, etc.) that users are tricked into download or are installed through other means. Alternatively, pre-installation of monitoring applications on a new mobile phone, or targeted "drive-by attacks" on mobile devices, present a new category of risk that is more difficult to detect and harder to defend against.

CIRCUMVENTION

Circumvention technology aims to bypass blocking mechanisms that are in place in many countries. As blocking is primarily implemented on data connections, the general technologies that are available for circumvention on mobile phones do not differ much from regular, desktop computer oriented tools.

Blocking web traffic effectively, (i.e., blocking the access of the user to the content and not merely using DNS filters) requires significant investment in proxy deep packet inspection infrastructure and interception of all internet communications.



- **PROXIES**

  Circumventing internet blocking that prevents direct access to a foreign website is quite trivial. To circumvent a filter blocking access, a user can ask a foreign proxy to access the blocked content on his or her behalf. As long as that foreign proxy itself is not being blocked, the user can then gain access to the content to bypass local filtering.

  One disadvantage of proxies is that the application that the internet user wishes to use (such as a browser or email program) must be "proxy aware"; it should have the option to set a proxy as an intermediary access server. On mobile phones it is not always easy to find applications that have this option. Not all mobile operating systems support the use of proxies on all outgoing connections.

  This approach also requires that the channel to the proxy not be blocked itself. To make monitoring and interception of the information harder, encryption of the traffic to the proxy is required. Otherwise it cannot defeat state-based monitoring on the outgoing connection. For a regular proxy, this is not standard practice, but is generally supported by proxy protocols.

  A diagram displaying a proxy server used to access content, despite blocking, is as follows:

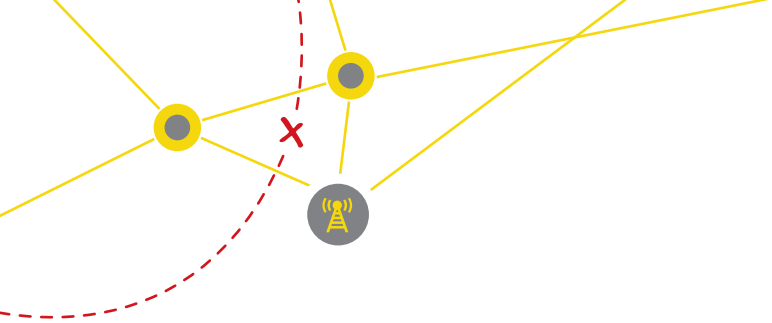
  Although most proxy servers use a purpose-built proxy protocol, certain proxies can be accessed by more common protocols, such as secure https connections. In this case, the proxy acts as a web server, displaying content available from elsewhere on the internet.

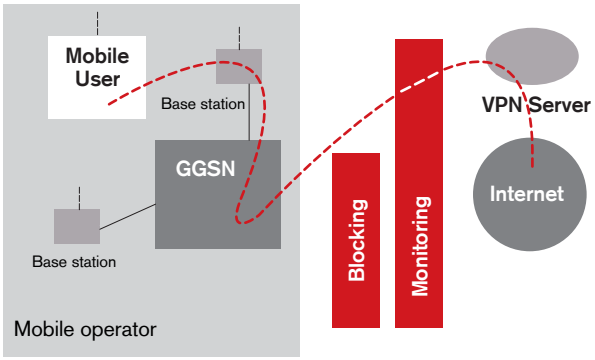
- **TUNNELING / VPN**

  Tunneling software allows users to create an encrypted "tunnel" to a different machine on the internet that prevents the filtering software from seeing web requests. Once a tunnel is created to the other machine, all internet requests are passed through the tunnel, to the machine on the other side, and then to the internet.

  The access method is similar to the use of a proxy, except that a tunnel is recognized by the operating system as a separate internet connection: this means that it is possible to use tunnels without a specific setting in the application.

  Similar to proxies, VPN tunnels should be encrypted so as not to be susceptible to snooping (interception and monitoring of traffic).





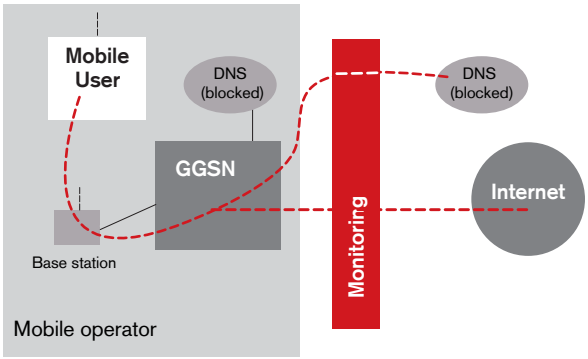
Various VPN technologies were tested for this report. The following table lists their generic properties as they were tested. Because some settings on VPN server and client machines may influence the strength of the cryptographic algorithms (or even the use of these) they are "dual rated" accordingly.

Type	Crypto	Authentication	Ease of Use	Native OS Support
PPPTP	Optional	Weak/Medium	High	Android, iOS
L2TP/ IPsec	Medium/ Strong	Medium/Strong	Medium	Android, iOS
IPSEC (aka IKE)	Medium/ Strong	Medium/Strong	Medium	Android, iOS, Symbian
OpenVPN	Medium/ Strong	Medium/Strong	High	Apps for Android (4.0 Native, >2.3 if Jailbroken) iOS (Jailbroken)

- **DNS-BASED FILTERS**

  DNS-based filters rely on a translation mechanism that translates the domain name of a site or resource into an IP address.

  DNS-based filters are easy to bypass, as long as the internet connection to the blocked website or resource itself is not blocked. Merely changing the DNS server of the provider to a different one (which is not part of the blocking system) or (frequently) using the IP address of the remote website is enough[27] to completely circumvent this blocking method.



  On mobile phones, however, it is not always easy to change the DNS service, as it is part of the operators' network. Next to this there is the inherent risk of monitoring, if the connection to the internet is not encrypted.

- **TELESCOPICCRYPTOGRAPHY(ONIONROUTING)**

  Telescopic cryptography or "onion routing" uses advanced public key encryption. A private key is available only to its user and is used for decrypting. The related public key, however, can safely be shared with the rest of the world and can encrypt communications destined for the private key holder. Only with the private key can encrypted data then be decrypted.

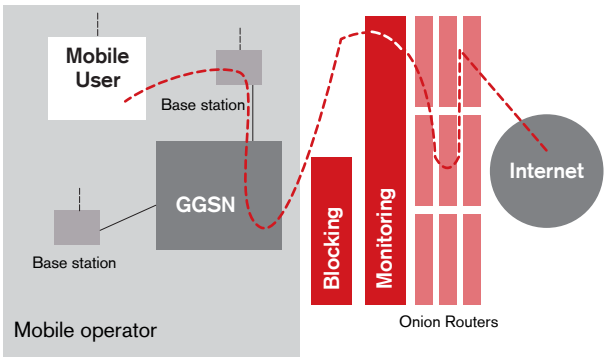
  Using this technology, traffic being sent is encrypted with pre-shared public keys of servers (often called onion routers or mixers) and transmitted to them. It is decrypted once received (often through several stages, passing several routers or mixers along the way) until it reaches the final (exit) node on the network. From that point on, plain, decrypted traffic to the open internet is provided.

27 Whether this works depends on whether a http- host: statement is required to access the website. Many sites operate on virtual hosting servers with shared IP addresses where direct IP access rarely works.

Using this principle makes it possible to employ layered cryptographic safeguards on tunneled traffic (hence the reference to an onion or a telescope; every cryptographic layer needs to be peeled off before plain text traffic is visible at the exit-node).

A common combination for circumvention tools is to create a local proxy for local applications to use. Traffic sent to this proxy is then tunneled to a server outside of the regimes reach, and from there sent to the public, "free world" internet.

A representation of traffic flowing to a webserver through three onion routers and an exit node is as follows:



PERSISTENT TARGETED ATTACKS

Increasingly, repressive states are known to use targeted attacks to monitor or infiltrate social networks of those they perceive as enemies of the state. This means they employ significant resources, especially against certain persons or organizations, and persistently try to infect or infiltrate their network and equipment. For this purpose, these states may even develop custom malware or set up social engineering operations to install monitoring software on the end users' equipment or network.

Due to the level of technical expertise this requires it should be noted that these attacks are likely to affect fewer users than network-based blocking and monitoring. In the case of modern smartphones, this threat is especially dangerous since limited (if any) security against mobile-focused malware is usually in place. Modern smartphones are powerful enough to get infected and can easily duplicate traffic streams, and redirect screenshots and data for interception purposes without the user becoming aware of this.

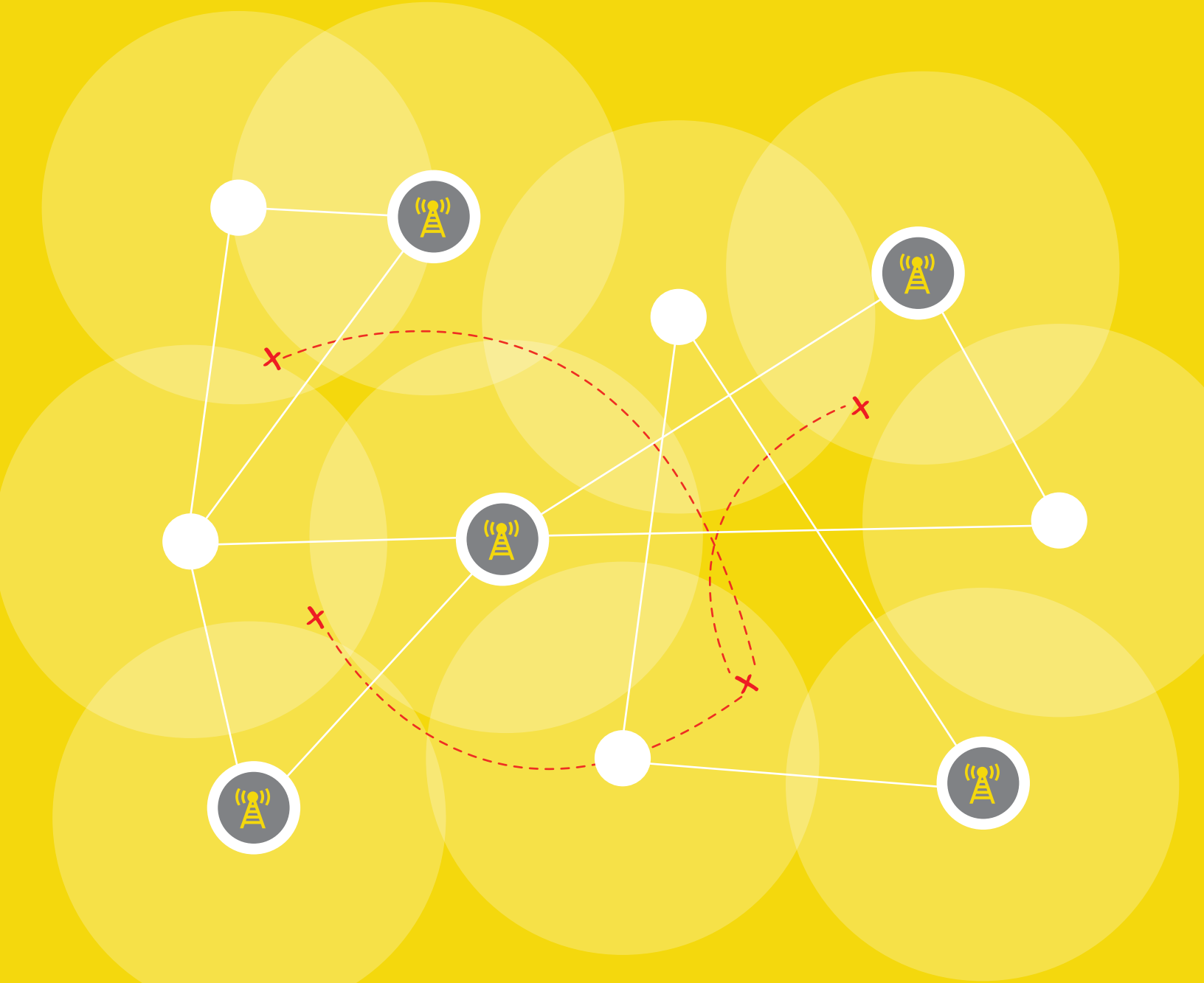
This means that network-based monitoring and blocking may, increasingly, be abandoned for more targeted, and more intrusive, technologies.

CONCLUSIONS

A study of the technical aspects of GSM and later mobile networks used for both voice, text, and internet access teaches us that there are significant flaws in the security of mobile networks that could be exploited for the purpose of blocking and monitoring. Most importantly, the standard encryption present in GSM will not protect against state-controlled networks. To the contrary: their design is well suited toward tracking and monitoring individuals.

For blocked content, and for prevention of such blocking and monitoring practices, several technical options exist.

Chapter 4:
Technical Testing



Technical Testing

INTRODUCTION

This chapter describes the technical testing performed for this study, mainly focusing on applications that are used for circumventing blocking and monitoring systems or for replacing the ubiquitous voice and text services provided by GSM networks with potentially more secure alternatives.

An overview of the app-specific outcome of the testing is presented in the next chapter, as a part of the threat assessment we performed. General remarks and a more general overview of the outcome are presented here along with certain remarks that did not fit within the format of the threat assessment.

Although the advent of these alternate voice and text applications may well be driven by the wish of western consumers to evade the cost of using these services through the GSM network, they could, if implemented securely, also serve to evade monitoring and blocking in oppressive regimes.

Therefore, the security of such services, as well as the security of mobile circumvention tools, is of increasing importance to mobile phone users in repressive regimes.

SELECTING APPLICATIONS

For the purpose of these tests, applications were selected that were identified in the results of the user survey we executed, as well certain applications that were specially selected on the basis of their pedigree. The latter included, for instance, the Orbot: Tor on Android application that enables Tor on Android devices, which only received a few mentions in the survey results.

The testing focused primarily on text and voice tools with security or circumvention characteristics, as well as general circumvention tools, which provide unfettered internet access to users, regardless of the application they use.

A specific risk of selecting applications is the need for them to function across many smartphone platforms. Applications that only work for one platform may require users to employ more ubiquitous, but insecure services such as email, voice, or text chat.

All of the applications selected provide a form of security by design or a (basic) circumvention method. This means that applications with no security mechanism (or only weak security) were not tested, insofar as we could predict the outcome.

For example, the following services were deliberately omitted from the survey as they are known to be susceptible to relatively simple man-in-the-middle attacks on the SSL/TLS handshake they use[28]:

- MSN
- Jabber/XMPP (The protocol used by Gtalk)
- ICQ/AIM
- Yahoo
- IRC

In some cases this is admitted by their developers; Google, for instance, makes it no secret that interception of messages is trivial.

Another risk that we aimed to eliminate is the need for "optional" encryption. The well-known voice protocol SIP, for instance, uses no encryption by default. It is usually made optional. With SIP it can be provided either by the SRTP/TLS or ZRTP protocols. So even if security is added by one user, if a connection needs to be set up between a secure and an insecure user application to make a SIP call work (one with and one without ZRTP, for instance) the connection to the insecure client will still expose the conversation and SIP signaling channels.

This provides a difficult challenge to the user, even

28 See for instance IMSpector, an open source tool for performing such attacks: http://www.imspector.org/

if he has secured the path to his service provider: can you allow a non-secure channel to connect and communicate with your device, thereby exposing the conversation? We have, therefore, aimed to use applications that enable security by design.

Note that this strategy comes with a price: many open protocols have "added" security features (OTR for Jabber or ZRTP for SIP, for instance) that can enhance their basic security significantly. Without these apps being universally available across platforms, and many service providers only providing unsecure services, the use of these protocols may create more problems than they solve in the short term.

The overall aim of the laboratory testing is to determine the most secure platform possible that includes the principles of:

- Security-by-design
- Cross platform interoperability
- Resilience to blocking and monitoring by the government

TESTING

Testing focused on a number of criteria, for each of which a score of 1 to 5 was awarded. Note that certain test criteria were omitted from the average scores when they were not relevant, or when (in a limited number of cases) a score could not be established objectively.

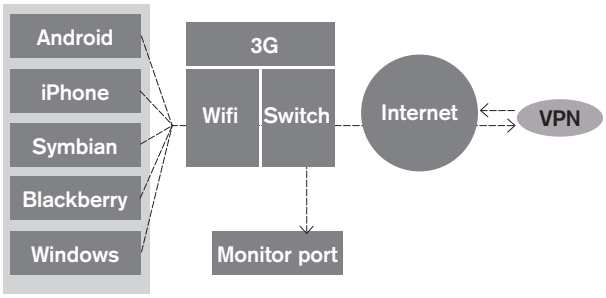
An un-weighted average of several factors was used to create a score for three aspects of the tool in question:

- Security
- Usability
- Resilience (to blocking of the tool by the government)

Although this approach led to an objective test result, some differences between applications were not well-reflected in the outcome, partly due to missing data, specific aspects of tools being "averaged," or scores being rounded in the un-weighted average. This caused some differences in the tools to go under-represented in the 5-star scoring mechanism. Where this was considered misleading or unfair, the score was adjusted (usually only by tenths of points, to prevent rounding up or down) to reflect a maximum difference of one star in the final category score.

SET UP

In order to test the performance of the various applications and operating systems, 5 different mobile phones were used in a controlled test environment (see the appendix on Methodology). A WiFi router (with controlled access to DNS) was used to provide internet access, as well as a 3G connection to a UMTS capable mobile network.



Phones

Testing of various applications was usually done on the WiFi network, although speed and carrier-change behavior was tested using the 3G connection. In order to further influence certain parameters of the VPN connections used by the various operating systems, a VPN service was set up on a dedicated server running CENTOS in a different network.

For VPN services, OpenSwan (IPSEC), Xl2tpd (XL2TP), Poptop (PPTP) and OpenVPN were used to provide VPN-based access to the internet. If necessary, a firewall could also be introduced into the local network, in order to allow for the blocking of specific IP addresses or to block DNS queries. DNS servers were provided locally to the phone by DHCP, using dnsmasq.

The VPN server had separate DNS servers not used by the test clients.

A monitoring port on the switch connecting the WiFi router was used to capture traffic to and from the mobile device, allowing for further analysis. For this purpose, tcpdump was used on an Ubuntu machine. Packet capture files were then analyzed in Wireshark.

The following phones were used for testing:

- Android: HTC Desire S (Android 2.3.5)
- iPhone: iPhone 4 (iOS 5.11)
- BlackBerry Curve 9360: (BlackBerry OS 7.0.0)
- Windows Phone: HTC Radar (Windows Phone 7.5)
- Symbian: Nokia N8 (Symbian Belle)

TESTING CRITERIA

For the test we used the following criteria (all criteria were rated 1 to 5):

- **PRICE**
  A score was awarded to represent the cost of using an application where it was deemed relevant. Where third party services were concerned, their cost was factored in and the score adjusted accordingly.

- **APP AVAILABILITY**
  Where non-OS-native applications are concerned a score was awarded for the security and availability of the application. If the application was only downloadable from a default repository, no full score was awarded, unless added security measures were present or the app was also presented from another source.

- **OS INTEROPERABILITY**
  The availability of applications on other operating systems was rewarded a score, which was higher if universal presence could be guaranteed. This reflects the need for cross-platform interoperability of the application.

- **HARDWARE LIMITATIONS**
  A score was added to rate if the application was limited to only specific hardware on the operating systems it was designed for, or whether it was universally supported.

- **REQUIRES ROOTING**
  A score was awarded for the application to reflect its usability without "tinkering" with the mobile phones security features, or root-user privileges. A full score was awarded only if the application could run with all features in the normal application environment.

- **PROPORTIONALITY OF "PERMISSIONS"**
  The proportionality of the application permissions was rated, based on an estimate of the likely need for the permissions for the core features of the application.

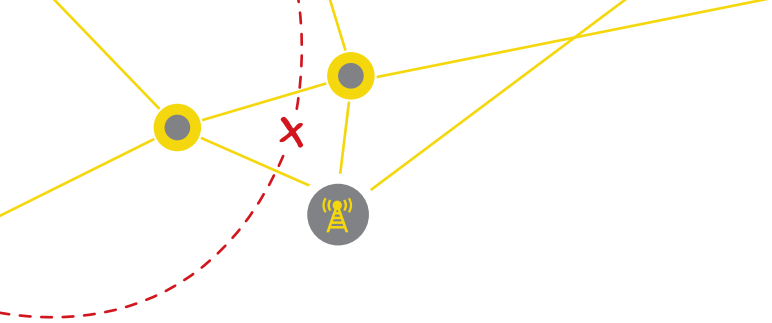
- **ANONYMITY (PERSONAL IDENTIFIERS, PERSONAL DATA)**
  A score was awarded for the availability of options that allowed anonymous usage of the service, without the use of personal data to register or use the service.

- **PREVENTS TRACKING**
  Points were awarded for the presence of anti-tracking technology in the application.

- **APP SUPPORTED**
  For circumvention tools a score was awarded based on the usage other apps can make of the "circumvented" internet connection. The more apps that can readily use it without difficulty, the higher the score.

- **CRYPTO - ON THE WIRE**
  The presence and nature of any cryptographic security during the transmission of messages was awarded a score.

- **RESILIENCE TO BLOCKING**
  By blocking IP addresses and DNS entries, a score was awarded for the ability of the tool to function if



blocking at either of these levels were to take place.

- **PLAUSIBLE DENIABILITY**
  Points were awarded if it would be possible to deny usage of the tool, either through obfuscation or other measures.

- **SYSTEM FINGERPRINTS**
  Analyses how much of the tool's data is retained on the system, and how sensitive this may be when captured. Most differences in score surrounded the storage of usernames and passwords on the device, as well as storage of communications data on the device.

- **CONTROLLED CARRIER CHANGE**
  A carrier change from WiFi to 3G and back was made through the operating system connectivity settings in order to test if applications could handle these changing connections appropriately, or at least would present a warning of the fact they might stop functioning, given the change of IP carrier. During these tests the "mapped" IP address (the public address) was detected at a webserver at regular intervals, to see when the change took effect and whether any warnings were timely.

- **FORCED CARRIER CHANGE**
  Similar to the previous test, only a now the change of carrier was simulated by disabling the WiFi router signal, and forcing the device to 3G (and back).

- **EASE OF INSTALLATION**
  The ease of installation was awarded points.

- **INTUITIVE GUI**
  The clarity, transparency, and functionality of the GUI (user interface) was awarded a score.

- **AVAILABLE DOCUMENTATION**
  The clarity, and (appropriate) level of detail of the user documentation was awarded a score.

- **LANGUAGES SUPPORTED**
  Where possible, the availability of the app in other languages was researched, and awarded a score.

- **SPEED OF OPERATION**
  Circumvention apps were tested against a video, a voice service and a website in order to measure speed of operation, with a view for audio-visual content and real-time content delivery.

  Where this was possible we developed further criteria for rating tools equally, by linking certain features or numerical properties to certain scores. A further table specifying this scoring methodology can be found in Annex I.

Forensic data extraction

Lastly, to test the resilience to mobile phone extractions by persons with direct physical access to the phone, we tested all handsets with the Cellebrite mobile forensics solution (UFED ultimate) and the Oxygen mobile handset forensic suite.[29] The combined hardware and software forensics solutions provided were used to try to extract two types of images from the mobile phone. The Cellebrite solution requires hardware drivers for the phone in question, while Oxygen also relied on an agent to be installed to the phone.

One attempt was made to retrieve an image through logical access, directly to the file system using the mobile handsets' file system and export utilities. The other was an attempt to retrieve a file system image of all data on the mobile phone. In the case of the iPhone, additional software called Evigator was eventually used to retrieve such an image. It makes use of the iTunes backup of the iPhone ion order to retrieve the data.

The data was then studied using the default report manager and reporting tools provided by these forensics solutions in order to try and retrieve details from the phones and from various applications. For the purpose of testing messaging applications, a message with a unique keyword was planted on the device.

29 See http://www.cellebrite.com

Selected results

OVERALL

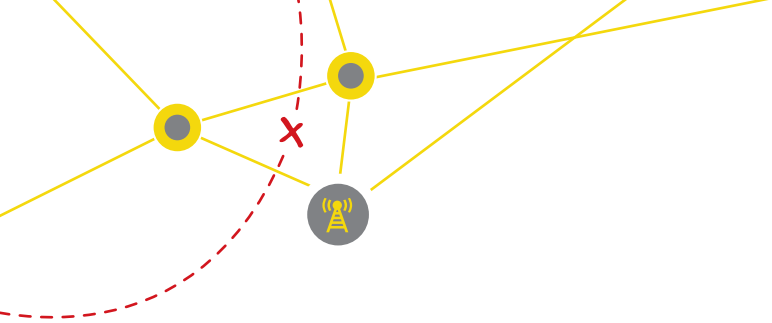
Our first impression of the circumvention and blocking ecosystem for mobile phones is not favorable. Only one purpose-built tool was deemed sufficiently mature to merit testing, while at the same time, users indicate using non-purpose-built tools, like VPNs, for the purpose of circumvention. This raises several questions, since these tools will often provide no more anonymity or security than a regular internet connection, even if they allow the use of the "free," uncensored internet.

In cases where merely retrieving information is required, this may be sufficient, but given the increasing complexity of smartphones, this area remains a risky proposition: a device with your location, close personal communications and contacts, and little to no added security measures other than those provided by the OS, is more a threat than a tool for free speech.

Though VPNs are hardly an ideal tool, they do seem to be reality for most of the interviewees, thereby meriting further research.

VPN TECHNOLOGY

Technical testing of the available VPN solutions (mostly built-in, OS-native, VPN clients and a few add-on applications providing VPN connectivity) provided more insight into the practicalities of running a VPN on a day-to-day basis. Although many performed well from a technical perspective (delivering packets from sources that would otherwise be blocked, using reasonable encryption, and at usable speeds) the design of many VPN systems seemed to be geared mainly towards western world risks and uses, rather than the needs of users in repressive regimes. The latter group requires more insight and knowledge into the VPNs' security. We found the following issues that illustrate this:



- **Encryption and Security: Not Transparent to User**
  In many cases the native OS or the application provides limited to no insight into the strength of the encryption that is actually used on the connection. Especially where only weak encryption is available or made optional ("Auto"), this is important information to the user. No OS or App provided this information in a clear and concise manner, although some applications did log details (without presenting them to the user, however) or provided a test facility.

- **Inadequate PPTP Security and Resilience**
  The 'point-to-point tunnel protocol' (PPTP) is offered by many VPN service providers as the cheapest option. It is, however, the least secure and most trivial protocol to block. It uses a control channel at a well-known port (TCP over port 1723) and requires a separate protocol (GRE) to be passed by the network in order to function. This is easy to spot and often does not work by default on home networks due to network address translation. This may force users to use 3G networks, which are often less anonymous. Encryption is optionally available only up to 128 bits, using MPPE. Authentication can be done in many ways, with MSCHAP v2 being the only common method that is not overly vulnerable. Even so, it is not a very strong VPN technology, with many known vulnerabilities that could be exploited.[30]

- **PPTP Compatibility Prioritized Over Security**
  We encountered several instances where service providers had not enabled encryption by default, probably for reasons of compatibility. In other instances the option to negotiate older encryption standards, as well as the options to use vulnerable authentication methods, were left open ("optional'), leaving the VPN open to degradation attacks and well known exploits.

- **IPSEC Resilience to Blocking**
  Although security is less of a problem for the xl2tp/ipsec tunnels we tested, it does remain an easy protocol stack to block. IPSEC is designed to be natively supported on the network and is, therefore, easy to spot. The ESP protocol it requires to operate is often not recognized on local WiFi networks that operate with NAT (Network Address Translation, which allows the use of private – RFC 1918 – address space in the local network) since NAT commonly breaks ESP and GRE protocols.

- **Inter-platform Compatibility**
  Apart from encryption being disabled on PPP VPNs in order to be more compatible, we also encountered a number of compatibility issues between Android, iPhone, and the OPENSwan IPSEC server we used for testing. Although it was not determined which side caused these incompatibilities, it does show that building a strong, universally compatible set of mobile VPN clients and servers is a challenge and may require significant effort, especially with a fragmented OS like Android – even though we found many reports of iPhone users suffering similar problems.

- **Limited OS Compatibility**
  For Symbian, BlackBerry and Windows Phone, VPN support was limited, either by requiring (extensive) policies to be set on the machine (BlackBerry and Symbian) or by absence of native VPN support or APIs (Windows Phone). BlackBerry requires a policy set by the phone's administrator through a service primarily intended for enterprises (this was not tested), a similar profile is required by Symbian – although here a free tool was available. We were not able to establish a working profile to a native IKE2 openswan server, however, and gave up testing after the complexity level reached one that is well beyond the grasp of the average mobile phone user. During desk research, only one VPN

30 For a more technical background see http://www.sans.org/security-resources/malwarefaq/pptp-vpn.php

provider offering appropriate default settings for Symbian was found.

- **Local DNS Access**
  In one case (Openvpn on Android), we found that the client invariably used the local DNS, instead of the servers presented by the VPN service. This is a security issue, as it will make both the traffic pattern visible to the (unprotected and usually state-controlled) access network, as well as enabling the possibility of DNS blocking.

- **Significant Risks of Connection Failures**
  Lastly, several issues arose with using VPNs while internet connections were being switched, either forcibly or through the native OS connection selection function. Many VPNs did not crash with a visible warning, nor with a block on any outgoing traffic (to keep ongoing communications secure). Although this is understandable for a business usage scenario, this failure handling is dangerous behavior in a circumvention usage scenario – especially when combined with no warnings of the VPN failure. In normal business usage, a VPN is usually used to gain access to an internal company network ("intranet") and access to company content would be prevented when the VPN connection breaks down.

REMOTE BROWSERS

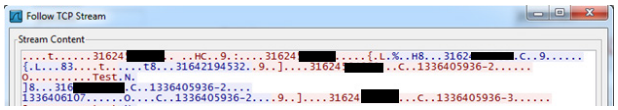
Two remote browsers were tested in the test run. Both rendered web pages to mobile devices, meaning the content is downloaded to a cloud-server belonging to the operator (Opera or Puffin), and the website is then rendered as if in a browser. The contents are then compressed and sent through an encrypted tunnel to the mobile device.

Although this does not expose the traffic to monitoring, this technology (if widely adopted) is very susceptible to blocking: only the service provider's cloud service needs to be blocked in order to block this type of software. Similar to VPN technology, the use of these technologies is only safe for retrieving information. As soon as the connection is used for connection to another service the encryption is no longer used.

Another specific risk identified is the use of login cookies and other information stored on the service provider's server. Although no post data or contents of the streaming data are stored, some trust in these third parties is warranted. Little is known about Cloudmosa, the company behind the Puffin Browser.

WHATSAPP

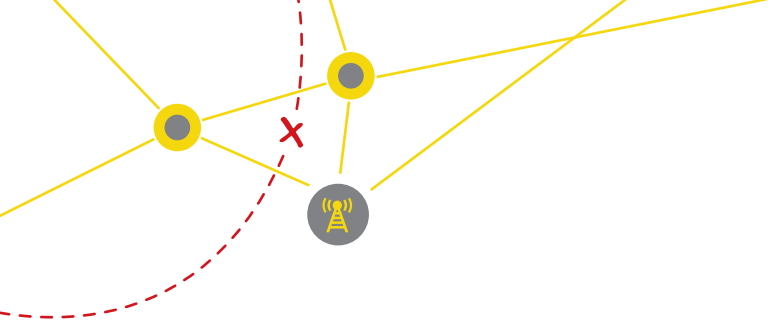
WhatsApp Messenger is a cross-platform mobile messaging app that allows you to exchange messages without having to pay for SMS. Whatsapp was found to use port 443 to send messages to a remote server. Normally this would indicate a TLS or SSL handshake being used to authenticate users or to secure the connection. The TCP stream, however, was far from encrypted, the text messages we sent were clearly readable, as was the destination phone number. Since these identifiers are typically connected to state-owned mobile networks, combining the contents and the phone number will make it very easy to trace networks of "subversive" elements. The following diagram shows the TCP stream, with the messages ("Test") in readable plaintext:



This behavior was verified on Symbian, Apple and Android.

ORBOT: TOR ON ANDROID

Orbot is the official port of Tor to Android. Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the internet. Orbot: Tor on Android is not prone to many of the issues found with VPN clients, and is the only purpose-built circumvention tool tested in this report. Although its test results were good, we did find issues that merit attention:



- For Orbot to fully function it requires the user to root the phone. This is necessary, as limited API functions do not allow the advanced transparent proxying and traffic manipulation that it is required to run the tool. Rooting, however, is not great from a security perspective since other applications can then also have root-level access. Rooting could possibly do more harm than good if some of these additional applications are malicious. In non-rooted mode, Orbot only allows browsing through TOR, or using TOR as a local proxy, offering less protection.

- UDP traffic was not proxied through the tool, when we tested it with Android 2.3.5 and Viber. This may make users vulnerable when accessing websites with video (many transmit video streams over UDP) or sending UDP packets for voice connections. If this is a (known) limitation of the transparent proxy setup the user should be notified. Using Orbot's associated browser, Orweb, ensured this behavior was no longer detected.

Other than these issues, Orbot is a very promising tool. For the moment, availability is limited to Android.

Although we were notified of various other "traditional" circumvention tool developers working on a mobile version, none were tested as they were still in development.

IPV6: JUST A BLIND SPOT OR A SECURITY RISK?

Although IPv6 functionality was not explored in the course of the technical testing, one of the WiFi networks to which the handsets were exposed to during testing did have native IPv6 available. This led to various unexpected results, upon which IPv6 access was disabled. (Not many fixed-line internet providers, let alone mobile operators, support IPv6 at the moment, although this is likely to change in the near future, especially on fixed-line and WiFi networks).

Since all of the tools were not tested on IPv6, this report will not go so far as to mention individual tools or operating systems but will summarize the main finding around IPv6.

IPv6 is well supported across many mobile platforms. This means that on any network that has native IPv6, most mobile devices we tested would get an IPv6 address through router advertisements and can thus enjoy access to IPv6-enabled websites.

Increasingly, and especially after the latest "IPv6 Day" on June 6th, 2012, many websites (such as Google, YouTube, and Facebook) have begun to activate IPv6 addresses for their regular domain names (AAAA records). This means that they advertise availability of IPv6 enabled services.

Applications on computers (and some mobile phones) such as internet browsers are usually designed to prefer access over an IPv6 internet connection and will therefore use IPv6 connections to access content available on IPv6 when provided with such access. This can have unexpected results for the user who has implemented circumvention strategies around IPv4 access since IPv6 traffic would ignore such circumvention configurations.

This means that by advertising IPv6 DNS records on an IPv6 enabled network, mobile phones that support this behavior will simply access the content over the IPv6 network. Although this is expected behavior in many environments, it appears that few circumvention tools or VPNs have foreseen that this may effectively bypass the secure IPv4 channel that they create. Moreover, by introducing IPv6 to a network, operators can effectively take over traffic that would have otherwise flowed through circumvention tools.

It is recommended that application writers and OS manufacturers in the circumvention arena pay attention to this behavior and design their tools and services accordingly. This can be done through blocking any IPv6 traffic – and IPv6 related DNS

queries (which can be accessed over IPv4, so this is by no means trivial)— or by routing this traffic through their services.

A quick test of IPv6 characteristics also reveals that while the Apple & Nokia devices provide users with IPv6 privacy addresses that changes at regular intervals to prevent tracking, Android 2.3.5 did not. This means these devices are easier to track since static addresses include the devices' unique MAC address and they have the same address while on the same network.

Note that from the tested devices only Android, iPhone, and Symbian supported IPv6.

JAILBREAKING AND ROOTING

Many (VPN and circumvention) tools require rooting (Android) or jailbreaking (Apple). The technical testing did not involve a study into alternatives for this practice, as available to programmers, although it can be observed that OpenVPN (which regularly requires such measures in order to run) does have a client capable of using the native L2TP API for this purpose: FeatVPN (which works by converting traffic from an OpenVPN tunnel to an L2TP tunnel locally). This clearly signals a lack of modular APIs for access to the phone core routing and connection functions.

Although such access may well present severe security risks, it seems that it is preferable to the current situation whereby the entire OS needs to be compromised to run an otherwise fairly ordinary VPN application such as OpenVPN.

Android 4 does present such an interface to developers, while maintaining support for its native VPN clients. Such APIs will also allow different cryptographic code, so that usage of modular cryptographic libraries (PolarSSL, instead of OpenSLL) becomes more feasible.

Results of Forensic Extraction

Each test handsets was connected to a forensics laboratory retrieval system to determine what content could be retrieved from the handset in the physical possession of a laboratory. 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. This device was not (yet) recognized very well, possibly due to its relatively new operating system (Windows Phone 7).

The basic usage information, as well as several other items, could be retrieved from all of the images. These included text messages, call history, and contacts information from the selected smartphones.

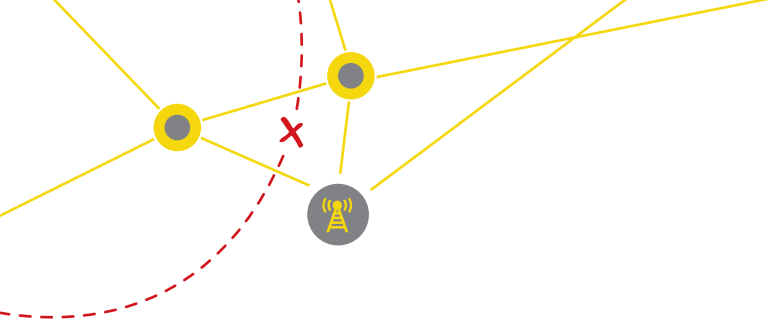
Note that the phones were analyzed while active so in many cases no security against physical access to the phone file system was (apparently) active.

Date that can be retrieved from a mobile handset using forensic retrieval software.

Device	SMS Records/Texts	Contacts	Call Records
Android	+	+	+
iPhone	+	+	+
Symbian	+	+	+
BlackBerry	+	+	+

In many other cases we were able to read selected other areas of the phone as well, such as application databases. WhatsApp messenger was especially prone to leaving data available in unencrypted sqlite databases, so we could retrieve messages.

This highlights the need for added encryption for such messaging applications. Note that Skype and Viber messages were not as easy to retrieve from these images, although a warning is required: no special tactics were employed to retrieve them other than by the default software options of the mobile forensics clients we used.



Conclusion

Current VPN implementations are not the best choice for secure, anonymous circumvention of internet censorship. There is a clear need for special "circumvention-oriented" VPN software. The current solutions can be safely used in a corporate environment when used to access a company intranet, but fail on aspects required to make them usable for circumvention scenarios. When a VPN connection providing access to a corporate network fails, access to the corporate network will no longer be possible. Currently, however, when a VPN, which is being used for circumvention, fails access to the resource will continue by the handset outside the encrypted VPN link, which can be easily detected by any agencies monitoring the internet.

There is a need for more purpose-built circumvention tools tailored for users in heavily censored environments.

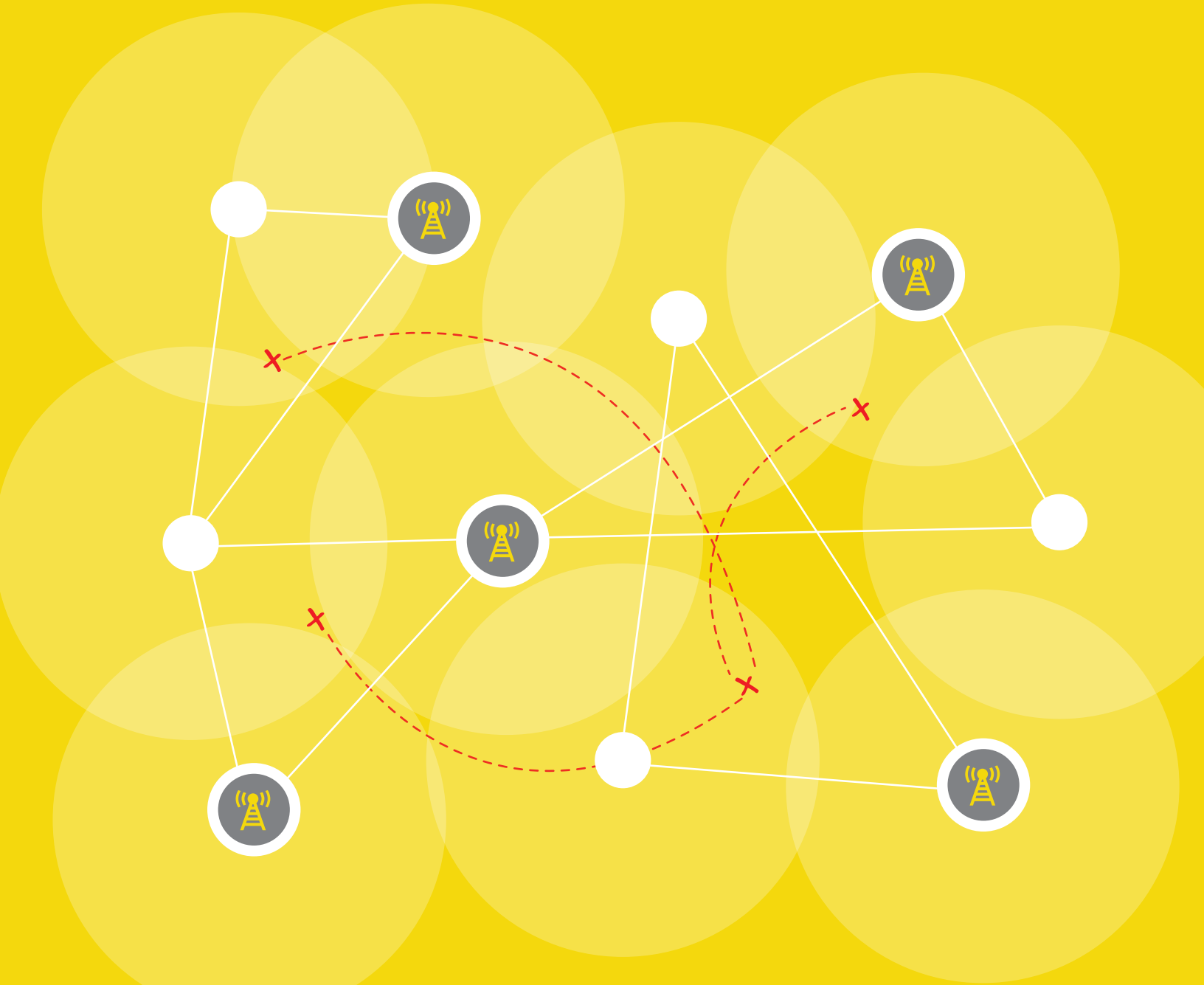
Attention should be paid to the increasing presence of IPv6. Either tools and services should be designed to operate in the IPv6 environment, or they should actively block it. Ignoring the presence of IPv6 will lead to unnecessary risks.

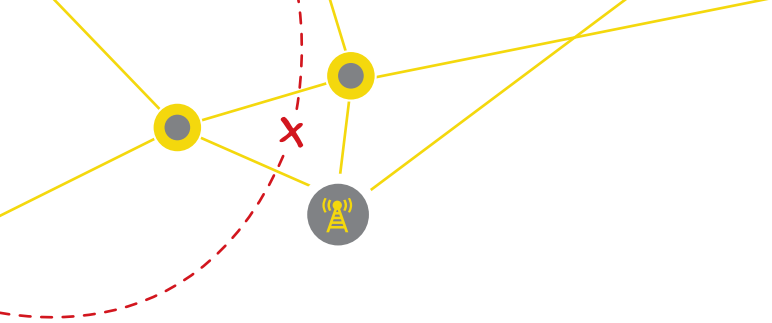
Designers should avoid creating apps which require jailbreaking or rooting of handsets. For this to be possible, OS makers should configure APIs to allow their use for that purpose.

In order to achieve maximum security for messaging and other applications that store data on the phone, it is important that app developers and OS manufacturers use encryption for the data stored on the phone, either by using built-in OS functionality or by using special libraries. Users should be aware that most common usage data can be very easily retrieved off their phone, even if it is left unattended for just a brief period of time.

A simple way to defend against forensic extraction is by leaving the phone in "charge only" mode by default and making it impossible to get into the UI by merely pressing or performing an unlock feature. Setting a swipe pattern or password to enter before the OS is visible makes retrieving this data harder, but certainly not impossible.

Chapter 5:
Threat Assessment





Threat Assessment

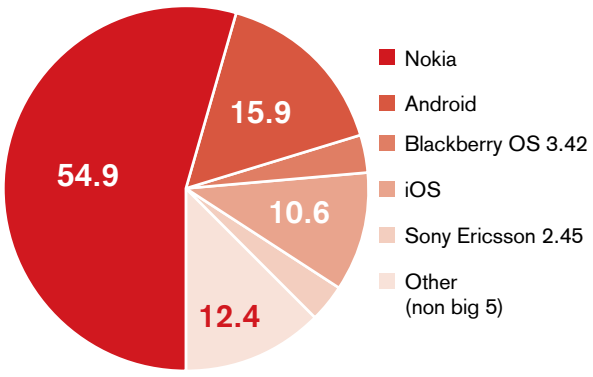
INTRODUCTION

This chapter aims to identify where users - given their regular internet usage pattern as well as the available hardware for mobile internet access – are most vulnerable to blocking and monitoring by oppressive regimes. To further a better understanding of the risks they face a threat model will first be developed that will then be used to identify where the current usage patterns will lead to identifiable threats or opportunities for said regimes to block or monitor internet traffic.

In view of this internet usage, and the threats this involves, applications and solutions will then be identified that could mitigate these threats. Since these are to some extent based on software, we will investigate these mitigating measures per OS as much as possible.

It's very important to understand which mobile operating systems were in broad use throughout the user community in the countries that were investigated. One source for this data is the global StatCounter website, which tracks mobile operating systems on a number of websites throughout the world. According to their (public) data the following is the relative division between the biggest five mobile operating systems (and a category of "others"):

BIG 5 MARKET SHARE MAY 2012

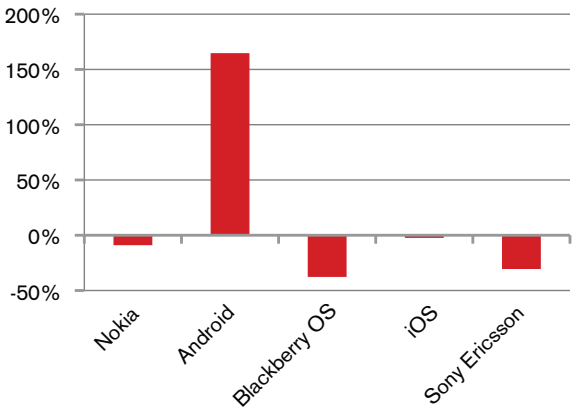


The other OS's (such as Windows OS's and proprietary operator OS's from LG and Nokia, for instance) were omitted for brevity and readability. They totaled 13,38%.

Note that the majority of users are using Nokia based operating systems (predominantly Symbian variants) at the time of the writing of this report. Of the Nokia OS market share, 9.8% of the measured mobile OS systems were Nokia 40 series feature phones – a system that is significantly different from the traditional smartphone OS and which has less abilities to download and use applications.

While the true market shares (in user numbers) may well be different than what would show from these statistics (which based on access to websites), we note that the trend is clearly that Android is on its way to take over a lead role, since most other OSes are even showing negative growth numbers:

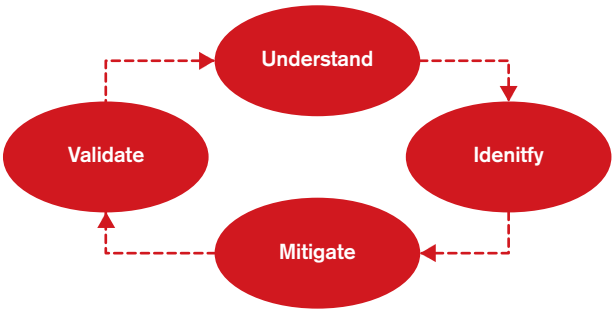
GROWTH RATE



This trend is corroborated by recent figures regarding sales of mobile devices, and seems to reflect the general direction that the market is headed.

Where technical measures were identified, we endeavored to validate the outcome by testing or conducting desk research to see if applications

delivered on the, sometimes implicit, promises in relation to the threats they were to mitigate as much as possible.



Not all measures are software related, and not all measures that were identified could be tested on available hardware. Some software related measures, for instance, would only run on specific versions of OSes or on specific mobile hardware, precluding a large part of the user population from having access to these measures.

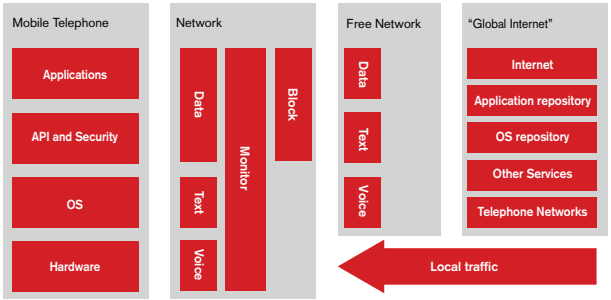
Technical testing was focused around testing of the circumvention and anti-monitoring tools that were available, and hence a more detailed section on these tools will follow later in this chapter.

Modeling the Mobile Environment

In order to model the environment to which users are exposed, we used the following simplified model of the mobile environment.

On the left in the chart below, the mobile phone and its various layers are represented. This is the user device that connects to the network to perform one of three functions: provide a voice, text, or data network access role. For the latter two, both blocking and monitoring infrastructure are in current use for the regimes in which these users operate. They will both have to circumvent the blocking (using circumvention tools on their phone or other strategies), in order to reach the "free world" network where their calls, text messages, and internet connections enjoy relatively free passage.

For any communications addressing local recipients, it is important to note that there is only local access required, meaning that there is not always a need for access to the global "free" internet. This model does imply that unsecure, unencrypted traffic, can be monitored both on egress and ingress to the monitoring and blocking infrastructure. For example, even if a message was to leave the country in a secure (unmonitored) and reliable (unblocked) way, it is important that the "free world" network infrastructure uses a delivery method with similar properties in order for "local traffic" to be secure. This is depicted in the diagram with an arrow pointing back to the egress point for traffic reaching the "free" world.

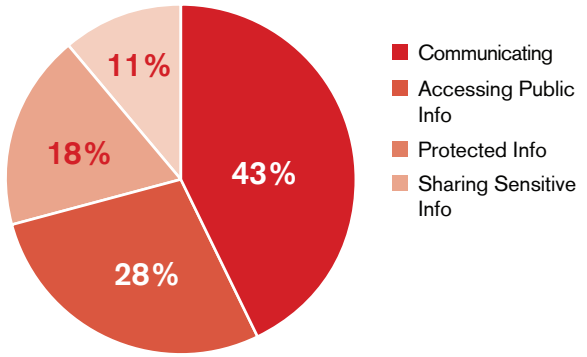


Types of applications

Now that the "mobile environment" has been modeled, it is important to have some understanding of the type of activity users employ online and the type of risk these activities carry. Unfortunately, little information is available on this subject, other than the in country reports that were gathered in the user survey and expert survey. Although these provide useful insight into the actual state of "visible" outcomes of monitoring (i.e. the subsequent prosecution or winding up of activist networks) and generally give an indication of how often "blocking" of content takes place, little insight can be gained into how effective these regimes are in monitoring internet use. This is, however, the biggest threat to users. Especially when they employ more subversive and "activist" ploys.

Some insights, however, can be gained from the user survey insofar as participants were asked about how they spend their time online. We note that only a small percentage was actively engaged in political speech and that most indicated they spent most of their time online engaging with friends and their social network.

Q19 TIME SPENT ON MOBILE INTERNET



This, of course, does not necessarily mean that users would want these conversations to be monitored by the state, but it does imply that only a limited amount of time is spent on activities that could be considered politically subversive.

Generally perceived as less risky, but not less important for the BBG and its audiences, gaining access to blocked and otherwise censored information is the primary reason for users to use circumvention technologies.

Reasons for use of circumvention tools (expert survey):

Accessing blocked content	Preventing monitoring	Faster Access	Personal privacy
81.8%	18.2%	0%	0%

Another important reason for using such technology is to gather unbiased information, presumably from blocked websites. Notably, personal security is not indicated by experts as a reason for using such tools.

The application repositories (app stores) of the various operating systems hold many thousands of Applications. It would be almost impossible to consider every one of these at great detail within the context of this study. We therefore have favored well know applications (since their end-to-end security is potentially better for a larger group of end-users) and applications that provide a generic level of security for all traffic emanating from mobile devices.

The applications that were tested can be divided into the following categories:

- Regular applications
- Voice services
- Text services
- Circumvention tools
- Security enhancements

REGULAR APPLICATIONS

Regular applications can perform all sorts of functions, although most of them serve no direct goal in terms of communicating with other users. For these we have reserved the other categories of voice, text, or circumvention. Since these applications are not written with communication in mind, they were not extensively considered for this report.

It is important to note that many of these applications require an internet connection to function. The connection is often used to update the app, download and show relevant data to the user, or to retrieve other information necessary for the app to function. Depending on the nature of the application involved, the data may even be stored for shorter or longer periods of time, thereby creating a variety of security risks, including the risk of this information leaking to monitoring government agencies.

Some of these risks can be mitigated by other applications, insofar as they are able to encrypt and/or obfuscate the data involved, thereby providing protection from blocking and monitoring. On Apple iOS, for instance, the use of a VPN and the built-in key chains may provide encryption of locally stored and transmitted data respectively.

Apps that only aim to upgrade the operating system's security were considered under the "security enhancements" category.

VOICE SERVICES

Given the state of the security and safety record of regular GSM phone calls (weak cryptography that is not applied end-to-end as was mentioned in the background chapter), there is a real need for the ubiquitous voice service to be replaced by a more secure variant. A problem here is that all of the apps we tested were, in one way or another, limited in their applicability. Skype and Viber for instance, can only be used among users of the same software. Open protocols such as SIP and secure variants of SIP (SIP and ZRTP or SRTP based) are not always supported by SIP service providers or mobile phone OS's.

We did, however, consider a number of such apps to see if they could replace the universal GSM phone service, while providing better security.

These applications invariably use the 3G or WiFi data connection of modern smartphones to provide a form of encryption from the end-user device.

TEXT SERVICES

Similar to the state of GSM security, and even easier to monitor, is the GSM network-based text service or SMS messaging service. We have found a number of applications capable of sending and receiving text messages through data channels, a number of which also provide cryptography.

Some also provide encrypted SMS messages, which may go undetected, provided the government does not use advanced technology to block them.

With the increased use of SMS blocking, these services may become a popular choice for circumventing the government's blocking infrastructure.

SECURITY ENHANCEMENTS

Whereas all the aforementioned applications typically serve one particular function, only a limited number of applications are available to enhance the operating environment of these applications.

This can be explained in part by the many security features that are already embedded in some of the mobile operating systems. These, however, can often be enhanced using separate applications. Most common of these are virus and malware scanners, which are available for nearly every OS. These scanners use a database of known malware and virus related signatures to scan for suspect files. They may also provide other strategies to enhance security.

Most of them also offer separate features that are not always part of the OS, such as phone location services (for making a phone send its location to a trusted address) or remote wipe features, which may come in useful if a phone is lost or stolen.

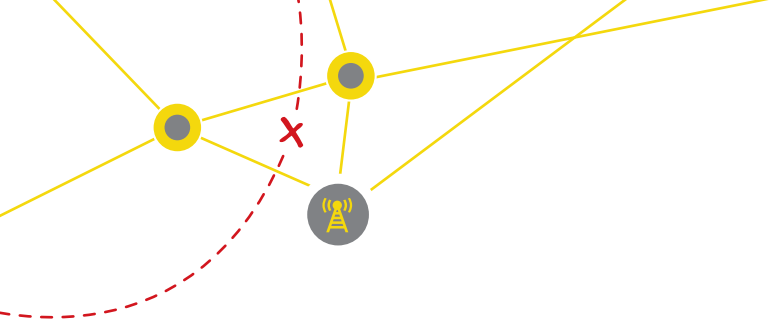
This category also contains some solutions that were not readily available in application repositories, so could not be tested off the shelf, but only through desk research.

Target Audience and Target Use Case

In order to develop an appropriate threat model for mobile internet users in oppressive regimes, a generic user profile or use case is required to limit the threats to the most common risks.

It should be noted that attempts to access free (western) media and independent news sources may pose a significant threat to users in the most oppressive regimes among the countries surveyed.

Users should therefore be provided with relatively secure means of communication that will hinder the government from blocking and monitoring the precise contents of the communications. With the advent of social networking



and the increased use of social networking sites for the distribution of content, secure, unblocked internet access on mobile devices was the main focus of this study.

This report also focuses on applications that have either received, or have the potential for, mass deployment. This means that an application's business model should potentially be able to sustain such growth.

Note that due to the general insecurity and high cost of satellite phones, these were not part of the scope of this study, nor were various commercial platforms that are available to secure phones in corporate or high security environments.

PhasesofMobilePhoneUsage/Threats

In order to analyze the situation of mobile phone users in oppressive regimes we will develop a threat model that is based on the service life of a mobile phone and categorize the related threats accordingly. This, it is our belief, sums up all the threats to the communications privacy and security of mobile phone users in a clear yet concise manner.

PURCHASING A HANDSET

- **Programmable Hardware**
  This threat relates to mobile phone hardware. Increasingly, mobile phones contain programmable components. A typical example of this is the baseband firmware of many phones that takes care of the connection to the mobile network. Firmware is used to update this hardware and use it to maximum efficiency. At the same time the programmable nature of these components exposes users to the risk of unwanted, nefarious changes that could be implemented by the state in "pristine" mobile phones.

  Especially where these states can also block upgrading of this firmware, a threat lies in the pre-installation of monitoring capabilities at a relatively low layer.

- **Programmable SIM**
  A similar threat applies to SIM cards. Since these can be programmed at a basic level it would be possible to retrieve basic data off a SIM card that may benefit oppressive regimes.

- **"Rigged" OS**
  An easy way for government agents to monitor users is to change the phone's OS in such a way that it can be used for monitoring. Safeguards that are applied for access to contact lists, access to location data, or even monitoring of the mobile's microphone and camera, can be easily circumvented. It should be noted that this can be made significantly harder in core OS code if the phone has no OS code signing or boot security in place.

- **Pre-installed Monitoring Apps**
  It is also possible to install software like this as a regular application, running in the background. This will work best if the software cannot be easily detected by the user. A recent case like this was uncovered when a monitoring application used by mobile network operators was unveiled to run, with full permissions, on some of the smartphones as they were delivered to customers with a new contract. The software went so far as to log keystrokes on the phones on-screen keyboard. The company, Carrier IQ, was ousted by many a mobile networks soon afterwards, but remains in business.

- **Registration of Personal Details and Device Identification (ID, Fingerprint)**
  It is increasingly common, on purchasing a mobile device that connects to a GSM network, that the SIM card details and IMEI number of the device are stored in government or carrier controlled

databases with a view to enhance users traceability in the network. These details are then increasingly linked directly to users' fingerprints and identities. Networks in Azerbaijan are also often configured to only allow registered IMEI and IMSI numbers to connect to or roam on the network, so this registration can be easily enforced.

USING A HANDSET

- **Blocking**
  The most common threat around the regular use of mobile phones and devices for internet access, even observed for various, less nefarious purposes, in western democracies, is the blocking of selected content.

  This phenomenon is one of the main reasons behind the drive for increased internet freedom for mobile users in oppressive regimes, and requires users wishing to gain unfettered access in many regions, to use advanced circumvention technology to bypass the state censor.

  Since, in many cases, blocking technology inspects the content of the traffic passing by (deep packet inspection), the side effect of this technology is that often encryption is used in circumvention tools. In the worst of oppressive regimes has this lead to a "rebound" in that the state

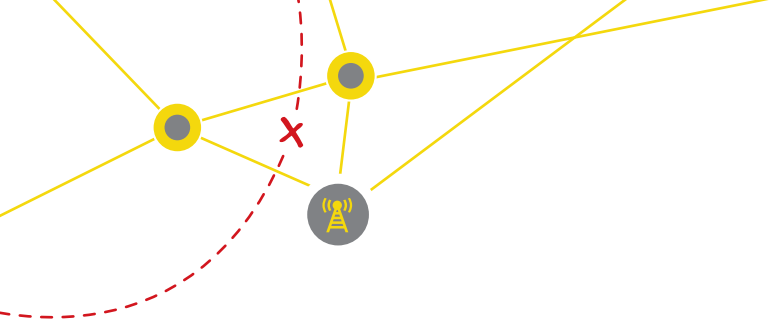
- **Monitoring (remote, network based)**
  In the absence of strong, end-to-end encryption, oppressive regimes generally resort to network-based monitoring with a view to gather specific intelligence against subversive elements agitating against the regime, as well as to gain intelligence on the sort of information gathered or disseminated by their subjects.

  The information gathered may be used to monitor the state of mind of the population, but more often than not it is used to form individual profiles of users. In many cases, targeted, network-based monitoring has led to prosecution and even killing of activists involved in subversive activities.

- **Monitoring (on Phone)**
  Even more invasive than remote monitoring is monitoring performed on the device itself, using software to monitoring anything from voice conversations to location data and messaging contents.

  Specific technical exploits are often used by states to install such apps, but can also be pre-installed before a phone is purchased. Data can be processed real time or stored for later reference and profiling.

- **Trusting Third-Party Service Providers**
  Insofar as third parties are used for providing services in the process of using the phone, threats may also arise insofar as they process or transmit sensitive information through their service. Oppressive regimes often put commercial and political pressure on such third party service providers to gain access to any securely stored or transmitted data that they process. An example of this was BlackBerry, which recently allowed the Indian government to access to its citizens data transmitted through the BlackBerry internet service and the BlackBerry messaging service, by providing these services in-country. It is alleged that the government brought this up as a criterion for market access to India. Similar discussions between the government of China and Google led to Google's withdrawal from this market – at least in terms of physical presence. In essence this threat relates to the trust you can place in these parties to guarantee a user's communications privacy.



INSTALLING APPLICATIONS

- **Application Repositories**
  Application repositories (app stores) are used to download applications to mobile phones. In essence, they are intended to be a central place where all applications developed for a specific operating system reside. Although one operating system has stricter rules regarding the application's requirements than the other, no application repository is 100% secure. These repositories are abused to upload malicious apps, that, either through clever programming, or detection prevention, are able to defeat the repositories security mechanism. Alternatively, the mechanism used to download applications could be subverted by an oppressive regime in order for users to be forced to use a repository that is in under the control of the regime. This may enable the installation of malicious OS updates or applications that allow monitoring. So far the latter has not been observed, but given recent attempts to vector attacks through Microsoft's update mechanism for the Windows OS, it seems likely some attention may be given to opportunities of application repositories in that respect.

- **File System Username - Privilege Escalation**
  Like most regular operating systems, applications on mobile operating systems have specific usernames or are otherwise restricted to their own section of storage space. This means they cannot normally read or write data that is owned by other applications or the operating system. By exploiting security holes in the operating system's code (called "vulnerabilities") it is often possible to circumvent or escalate these rights. This makes it possible for the application to read data it was not supposed to have access to. The threat, in relation to monitoring, is especially present if applications can be run as the "omnipotent," "root," or "administrator" user.

- **Permissions Management - Privilege Escalation**
  Permission to access certain APIs of the OS are usually granted per application, and the setting is often maintained after permissions were granted the first time. Access to these APIs (or resources) may provide applications with access to special resources such as location data and contacts. Through similar methods, as described in the previous paragraph (exploiting vulnerable code), or flaws in OS APIs, it has often been possible to bypass these security features. This makes it easier for attackers to install malicious applications without some of the protection normally provided by mobile operating systems.

- **Application Security**
  Applications themselves are often poorly written. Recent studies show that, in many cases, OS specific, built-in security features are poorly used, if they are used at all. This may lead to glitches such as login details that become available to anyone with physical access to the phone, or credentials that are stored in plain text.

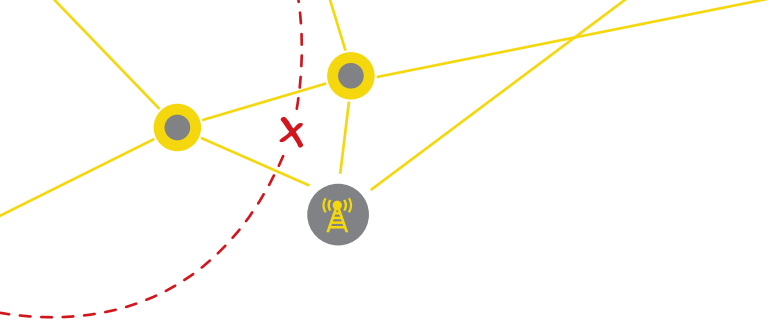
- **Rooting or jailbreaking phones**
  Although some attacks may lead to the attacker gaining super user ("administrator") rights to the mobile phone, it is also common practice to enable the per-user rights management system of the mobile phone OS, in order to allow applications access to any and all resources on it. This type of access is called root access. Additionally – especially on Apple's iOS – the phone can be allowed to run applications from sources other than the main repository (Cydia's app repository, in the case of many Apple iOS jailbreaks). In the case of Apple this is often referred to as "jailbreaking." Often this also leads to an ability to run more software, and from different sources than the original OS repository. The difference with the two forms of privilege escalation is that in the case of jailbreaking or rooting, the user is responsible for the escalation, not a foreign attacker.

ACCESS TO PHONE

- **Remote Access**
  Although most of the previous threats are launched from the network, or before the phone is in the users possession, there is also a considerable attack surface to consider in the proximity of the phone. Bluetooth and wired access methods (in use for syncing or tethering phones for the purpose of gaining internet access) may well lead to access to the phone on several layers. Bluetooth connections are especially trivial to monitor and in most cases can be used to gain access to phone contacts or conversations held on wireless headsets. Flaws in the OSes handling of bluetooth traffic could be further exploited leading to forms of privilege escalation too.

- **Physical Access**
  Physical access is possible if a phone is left unattended for lengthy periods of time. In many cases, suspects that are picked up by security services or are otherwise in the hands of authorities for some time are routinely searched for and relieved of their phone for the duration. Even in western countries it has become customary to use this opportunity to gain access to phones and their file systems to obtain data retained on it. Especially in combination with poor coding practices (such as Apple's "location data glitch" that exposed a database of the phones location for a long period of time) this may lead to the extraction of many types of data available on the phones filesystem. Retrieving phone contacts, email, and SMS data is especially trivial: this is standard information retrieved by off-the-shelf mobile phone forensic hardware and software.

- **Disposal**
  Of all stages this is probably one of the most dangerous. If a phone is not disposed of properly, its details may easily fall in the hands of malicious actors. States interested in contacts or communications will also have unlimited time to acquire the data on the (improperly disposed of) mobile phone, since it will, usually, not be missed. Proper wiping and use of encrypted file systems may partially prevent this threat, but if a mobile phone contains especially sensitive details, destroying it completely may well be a safer solution.



Mitigating threats

Not every threat mentioned above can be overcome by technology alone. Some threats are almost impossible to prevent completely without a regime change. Therefore, for the purpose of this report we will focus on mitigating these threats to a level that is more or less acceptable for the average user of mobile internet, keeping in mind that both targeted efforts by the regime at hand, as well as the behavior of a user, influence the general safety of t a person's internet usage.

In general, threats can be mitigated by any number of measures. For the purpose of this study we have focused on the measures present in the OS, which we have studied based on the documentation. Secondly, separate, installable applications can be used to overcome certain threats. The following is an overview of the types of threats an OS and applications can typically prevent against.

As follows, common threats like blocking and network-based monitoring can be easily overcome using various applications. Many other threats, however, can only be detected or overcome by the operating system, or, alternatively, specialized security applications. For this reason, and because it is related more to BBG's mission, this report will discuss blocking and monitoring separately and in greater detail.

Programmable Hardware	OS	Voice	Text	Circumvention	Security
Programmable SIM	X				X
Rigged OS	X				X
Pre-installed Monitoring Apps	X				X
Registration of PII and Phone ID					
Blocking	X	X	X	X	X
Monitoring (Remote)	X	X	X	X	X
Monitoring (on Phone)	X				X
Third-Party Service Suppliers				X	
Application Repositories	X			X	X
File System Privilege Escalation	X				X
Permissions Privilige Escalation	X				X
Application Security	X				X
Rooting & Jailbreaking	X				X
Remote Access	X				X
Physical Access	X				X
Disposal	X				X

Countermeasures

In terms of countermeasures we have identified the following possible (generic) measures:

- **Code Signing**
  Code signing is the cryptographic signing of application or update code that is loaded by the device. The electronic signature is uniquely linked to the author's private key so the authors public key can be used to validate the origins of the file being loaded. In a word: code signing prevents loading of unauthorized or altered code onto the phone hardware.

- **Secure Boot**
  Similar to code signing, a secure bootloader secures the process of loading the OS. It checks the signature of the OS that is being loaded against a hardware based public key. Any code not signed by the operating system's original author can then be refused.

- **Antivirus Software**
  Antivirus software for mobile devices is increasingly used. It will check signatures of known malware available for the mobile phone OS it is running on. Usually it provides added features such as added phone unlocking steps, remote wiping, and phone tracing facilities.

- **Security Enhancements**
  Next to the former methods, a number of different strategies exist that allow more granular or better management of application and OS security in the mobile device. A good and notable example on Android is the SElinux extension. This extension allows mandatory access control meaning that any access from one process to the other must be explicitly defined in a policy in order to be allowed by the kernel. This prevents many of the unwanted behavior patterns of viruses and malware; these will not normally have policies governing their processes. A recently announced Ubuntu version for mobile devices has a similar function called Apparmor. In short this category comprises generic security enhancements of any type.

- **File System Encryption**
  This is technology used to encrypt the phones file system. While useful for preventing direct access to data if the phone is locked or switched off (and subsequently accessed or stolen), it will only sort any effect if the unlock key is not easily retrievable, and if the decryption is not applied generically at boot time. Since most phones are left switched on, the latter would mean that, in effect, access to the file system can be had as long as the phone remains powered. Instead, unlock codes or passwords should be used to decrypt (certain) files containing sensitive data. The required code should then be entered upon requesting the data, so only when it is strictly needed to be decoded.

  Next to these generic security measures, measures for circumvention and against monitoring will be discussed in a separate paragraph.

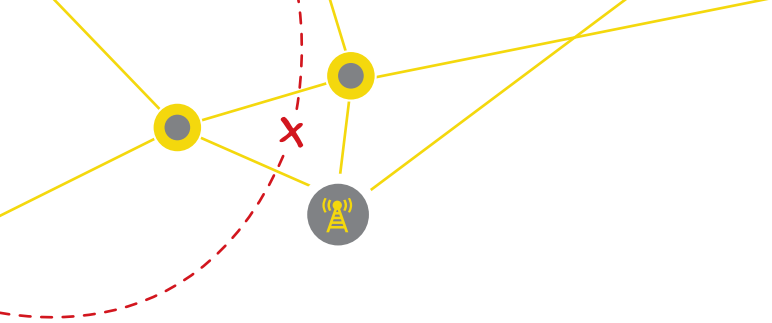
OS SECURITY

It is important to note that while we tested a number of security applications allowing users to guard against blocking and monitoring, only a limited amount of applications are available that enhance the operating system's security level.

As the previous table clearly shows, a large number of security measures can only be implemented on the local platform – either through implementation in in the OS or through specific applications that extend the OS platform security. This means the OS, or its security extension, play a key role in securing any mobile internet device.

We will discuss the possible measures and list their presence in three separate areas:

- The initial execution environment (which is



present after buying a phone).

- The runtime environment (threats when using the phone and installing apps).
- The threats present in relation to direct physical access to the phone.

Initial Execution Environment (Buying a Phone)						
Threat	**Measures**	**Android**	**Apple**	**Symbian**	**Windows**	
+ Programmable Hardware + Programmable SIM + Rigged OS + Pre-installed Monitoring Apps	Secured Boot Environment	X	X	X	X	X
	Antivirus Checks	X		X	X	X
	OS and Firmware (Baseband) Scan					

Pre-installed software is hard to detect since the software to check the phone needs to be installed to the platform that was initially infected in the first place. This makes it possible for makers of such infections to leverage their access to the device by using measures that prevent such software from running, or by faking its results.

Tampering with rudimentary elements of the mobile phone (such as the bootloader and the radio firmware, often called baseband, or the OS) is, however, detected as a matter of course by modern phone operating systems. This does not mean that these features cannot be disabled or circumvented. In case a user decides to install another OS or aftermarket firmware on his or her device, these features are often disabled in the process of "jailbreaking" or "rooting" the phone. Similarly, states wanting to spy on their citizens could easily pre-install such software, or modify phones before marketing them.

In that case, virus scanners may still pick up some changes, especially in relation to higher level sections of the OS. For this they use traditional anti-virus scanning techniques based on signatures of the infection at hand. These, however, have limited effect against lower layer parts of the phone's architecture. Apple, as a matter of course, does not allow such programs on its app store, limiting user take-up of such software.

It would, therefore, be preferable to have an ability to scan lower layers of the phone and OS using specialized applications, in order to check whether they are still in "stock" or "vanilla" condition. We have not found any applications that can achieve this, possibly due to restrictions in place at the hardware and OS layer by default. It would be recommended, to at least research such checks more actively in the course of anti-virus software, and as a matter of general security research. This could uncover any state actors employing these tactics at an early stage.

RUNTIME ENVIRONMENT

Running applications and using the phone is by far the most important area where users are exposed to threats. Not only are there various attack vectors in play, but the main interest of oppressive regimes will likely be in the real time data that is generated from mobile phone use. Not only text and voice, but also location data and other forms of online communication form the main target of many a monitoring operation.

While generic security checks would be helpful here, such as virus scanning the phones data storage, a lot of threats can onbly be mitigated by user behavior (not included in these tables) and by more advanced security mechanisms.

Some of the main threats can also be overcome by not exposing the device to the mobile network that is in the hands of the oppressive regime. This will, for instance, make the use of alternate application repositories, or certain monitoring technology, less feasible. Given the state of censorship circumvention on mobile devices, however, many users are then limited to trusting their VPN supplier – virtually the only technology currently available to circumvent direct access through the censored network.

Runtime Environment, Applications						
Threat	**Measures**	**Android**	**Apple**	**Symbian**	**Windows**	
+ Monitoring (on Phone) + Third=Party Service Suppliers + Application Repositories + File System Privilege Escalation + Permissions Privilige Escalation + Application Security + Rooting & Jailbreaking	Anti virus check	X		X	X	X
	Code signing	X	X	X	X	X
	Enhanced security features (such as trusted path execution)	X				

As can be seen from this table, the most generic defenses against some of these threats are supported by all operating systems. Again Apple is the odd one out since it does not make antivirus software available in the App store. Only Linux-based Android has seen any capacity for more granular security enhancements available as an extension to the OS. The NSA's SElinux project has been ported to Android. Since this tool is only available as a reference implementation, and is not easy to install without specific Android knowledge it remains between brackets.

PHYSICAL ACCESS

Physical access to mobile phones is conceivably the most intrusive of all threats discussed here. By gaining physical access, an attacker exposes it's storage media (both internal and external SD card where available leading to possibilities for extraction of stored data and credentials. Close proximity access (such as near field communications, tethered connections, and Bluetooth can often render similar results.

Physical access						
Threats	**Measures**	**Android**	**Apple**	**Symbian**	**Windows**	
Remote Access Physical Access Disposal	File System Encryption	X	X		X	X
	Remote Wipe	X	X	X	X	X

Although file system encryption was developed a long time ago, not all operating systems systematically implement this option. Android, which previously only guarded access credentials, has recently introduced it in Android 4.0 to counter these threats. Although BlackBerry has gained significant renown for introducing encryption to the mobile landscape, it does not have the feature enabled by default. iOS was one of the first to enable a full disk encryption system, guarding all non-system files with fairly strong, hardware-based cryptography.

If all else fails, many applications offer the ability to remotely wipe user data on the device. The use of faraday cages for captured mobile devices is, however, commonplace, disallowing the use of such tactics in many scenarios involving a well prepared attacker. The picture displays such a faraday "evidence bag" that is readily available on the market today.

Interim Conclusions

ASSESSMENT OF CIRCUMVENTION AND VOICE/TEXT OPTIONS PER OS

Now that the baseline threats and mitigation strategies have been established for the different mobile phone platforms in general, the next step is to perform a more detailed analysis of the blocking and circumvention options open to users of the main smartphone platforms.

The tools mentioned here are divided up in specific categories, depending on the functionality they provide. We have divided them into "voice" and "text" applications, depending on whether they allow text or voice communications to be encrypted and transported, or "general circumvention tools" that simply reroute the entire internet traffic of a device and thereby provide circumvention as a generic service.

TEXT SERVICES

Regular text service, as we have discussed earlier, is not very secure. While regular SMS text messages traverse the radio paths on their journey under the protection of a GSM standards based cryptography algorithm, they provide limited protection against snooping on the network. Because of their "plain text" nature (once traversing the operators wired network and network core) they are also susceptible to blocking, a practice increasingly common among oppressive regimes.

The selected replacement text applications therefore, usually run on the devices various data networks, bypassing the operator's infrastructure. In all cases they provide cryptography, and in many cases they provide more than just text messaging. Sharing of various types of content can usually be achieved using these.

VOICE SERVICES

Similar to text messages, voice service on the average GSM network is also susceptible to snooping. Because without special hardware, no options exist for encrypting GSM voice traffic applications offering an alternative connection all use software based encryption and the smartphones internet connection in order to bypass government-based monitoring. Although blocking of voice traffic is often not based on the individual call, it is often done at a service level. Resistance to such blocking is of importance there, too, as is the level of encryption.

CIRCUMVENTION TOOLS

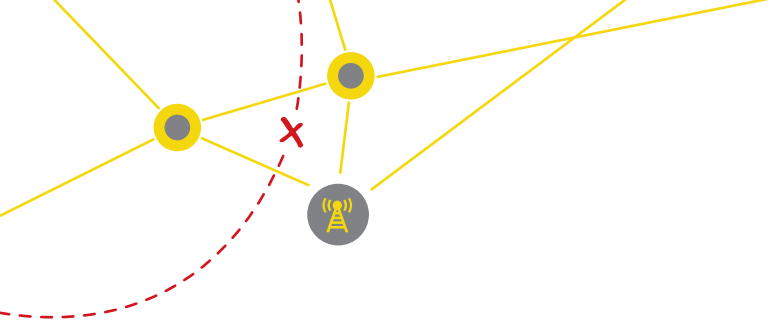
Rather than bypassing the censor at a per-application level, it is also possible to capture and reroute a devices entire internet connection. This requires two layers of connectivity: one internet connection that is capable of reaching a third party service, and another, overlay connection, that is capable of carrying the actual data traffic that is being transported.

With the exception of one or two tools, the tools discussed here are all Virtual Private Networks (VPNs) that relay traffic to a different location, and set up connection from there, relaying any content through a tunnel that passes through any monitoring and blocking infrastructure. Although encryption is commonly used as part of the system, it is not always enabled by default.

The following tables list the score for a variety of applications, insofar as they were tested, and rate whether the outcome, given the availability and testing results of the applications, is insufficient, adequate, or good. Test results for applications are displayed on a scale from 1 to 5. Only categories where two or more applications score 4 points in one of the categories, and both not scoring lower than 3 in any other, are rated "good" overall.

Categories where one or no applications exist, or where apps only achieve a score of one in one of the categories, will be rated insufficient. The rest is deemed "adequate."

Using this method we can then see any areas where specific apps require (further) development, both in terms of type (voice, text, or circumvention) as well as per OS.



The most important results of testing are listed below the tables and serve to further review the understanding of the test results. Each OS section ends with a conslusion.

ANDROID

Function	Tool	Security	Resilience	Usability	Overall
Voice	Skype	★★★	★★★	★★★★	Good
	Viber	★★	★★★	★★★★	
	CsipSimple	★★★	★★	★★★★	
Text	Skype	★★★	★★★★	★★★★	Good
	Viber	★★	★★★	★★★★	
	Whatsapp	★	★	★★★★	
	TextSecure	★★★★	★★★	★★★	
Circumvention	OpenVPN Client FeatVPN	★★★ ★★★	★★★ ★★★	★★★ ★★★	Good
	PPTP native	★★	★★	★★★	
	L2TP/IPSEC native	★★★	★★	★★★	
	Orbot	★★★★	★★★★	★★★★	
	ExpressVPN	★★	★★	★★★★	
	Puffin Browser	★★★	★★	★★★★	
	Opera Mini	★★★	★★	★★★★	

Android displays some of the highest scores in this analysis. As a clear test winner, the Orbot application offers best-of-breed censorship circumvention and anonymity options for mobile users. Even though OrBot: Tor for Android has its shortcomings, it is otherwise a platform where much development work is already taking place.

Notably, a number of tested applications stem from the Guardian Project, which may indicate an early success, on their part, in reaching development goals for further securing Android. On the downside, these applications have no equivalent on other operating systems, leaving users with no option but to use less secure, common circumvention applications, or use other means to secure their communications.

Issues surrounding Android were the interoperability of VPN technology, the inherent safety (and implementation) of PPTP VPN technology and issues around a change of carrier signal. All in all the situation is hopeful, but there is ample room for improvement on many areas, and platform security outweighs any of the risks that are addressed by these tools.

Another issue is the fragmentation of the platform and the abundance of VPN-based applications; it was not researched if these all use best practices, but the practices of certain service provider implementations we did investigate, did give rise to concern during technical testing.

VPN connections are also hardly transparent and may often disconnect without appropriate (immediate) warning. Next to this, although Android is IPv6 capable, there appear to be little notice taken of network behavior in dual stack network environment by either circumvention tool.

Note that for testing the nightly build of Csipsimple was used, which contains ZRTP, PGP based crypto for SIP telephony.

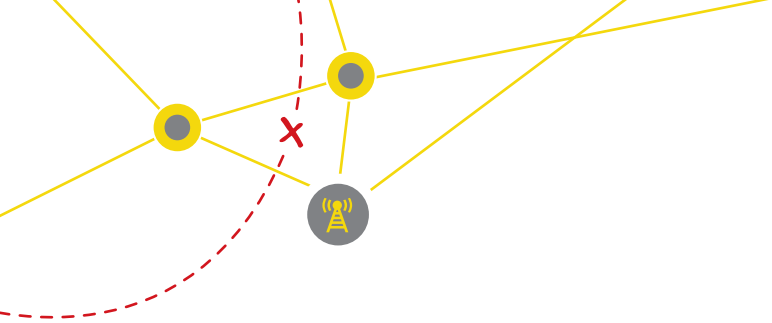
IOS

Function	Tool	Security	Resilience	Usability	Overall
Voice	Skype	★★★	★★★	★★★★	Good
	Viber	★★	★★★	★★★★	
	Acrobits	★★★	★★★	★★★★	
Text	Skype	★★★	★★★	★★★★	Good
	Viber	★★	★★★	★★★★	
	Whatsapp	★	★	★★★★	
	TextSecure	★★★★	★★★	★★★	
Circumvention	OpenVPN	★★★	★★★	★★★	Good
	PPTP Native	★★	★★	★★★	
	L2TP/IPSEC Native	★★★	★★	★★★	
	Orbot	★★★★	★★★★	★★★★	
	ExpressVPN	★★	★★	★★★★	
	Puffin Browser	★★★	★★	★★★★	
	Opera Mini	★★★	★★	★★★★	

iOS displays roughly the same characteristics as compared to Android, with the exception that most tools listed are either OS based or made by independent developers. Although the overall outlook is good, a similar warning applies as to Android: PPT VPN technology leads to problems and may not provide any protection without the user realizing this. More transparency is required.

OpenVPN also requires rooting of the phone, which in itself poses an added security risk.

The positive outlook is by no means a confirmation of the ultimate safety of the user. This will depend as much on the users behavior as it does on the platform.



SYMBIAN

Function	Tool	Security	Resilience	Usability	Overall
Voice	Skype	★★★	★★★	★★★★	Adequate
	Internal SIP	★★★	★★	★★	
Text	Skype	★★★	★★★	★★★★	Insufficient
	Whatsapp	★	★	★★★★	
Circumvention	IPSEC	★★★	★★	★	Insufficient
	Opera Mini	★★★	★★	★★★★	

Although a very popular operating system in in the countries with a medium- to low-national income, Symbian displays a severe lack of circumvention options for its users. With only one, rather user-unfriendly VPN system, and only Skype and SIP to provide safe voice service, there is ample room for improvement of circumvention tools for this platform.

BLACKBERRY

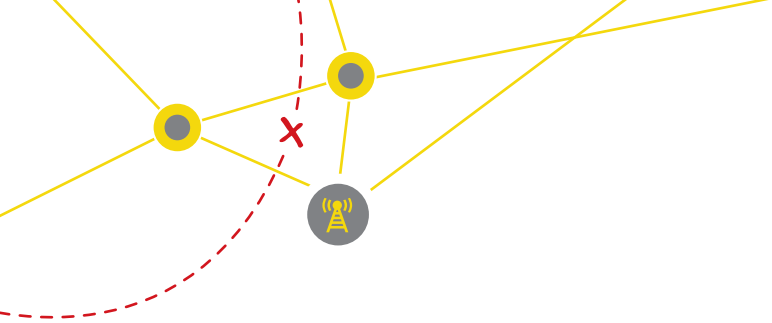
BlackBerry provides many security features, and uses strong public key encryption at the basis for its security design. The business model of the BIS and BES services, however, create significant shortcomings in these models for the "single user" of BlackBerry technology. In many cases BlackBerry still possesses the keys required to decrypt text messages (such as BlackBerry Messenger messages using the global key) and hence is not providing similar protection to BIS users. For this reason we have tested various alternatives to the standard BlackBerry applications.

No alternative circumvention methods were available, however, with the exception of the built-in VPN, which can only be set up through the BES service. This is not likely to be available to single BlackBerry users, so was excluded from the test. The Opera Mini browser is the only viable tool ion that category.

Function	Tool	Security	Resilience	Usability	Overall
Voice	Skype	★★★	★★★	★★★★	Adequate
	Internal SIP	★★★	★★	★★	
Text	Skype	★★★	★★★	★★★★	Adequate
	Whatsapp	★	★	★★★★	
	Viber	★★	★★★	★★★★	
Circumvention	Opera mini	★★★	★★	★★★★	Insufficient

BlackBerry makes extensive use of its own network infrastructure and, as such, provides circumvention options for its users "by default." It cannot be guaranteed, however that applications use these options. The Whatsapp messenger application, for instance, sought direct contact with the WhatsApp service, without using the RIM infrastructure.

This system puts user privacy firmly in the hands of third party developers, and without active enforcement, nor transparency on how data is actually being routed, creates unnecessary and unacceptable risks for BlackBerry users in oppressive regimes.



WINDOWS PHONE

Function	Tool	Security	Resilience	Usability	Overall
Voice	Skype	★★★	★★★	★★★★	Insufficient
Text	Skype	★★★	★★★★	★★★★	Adequate
	Whatsapp	★	★	★★★★	
	Viber	★★	★★★	★★★★	
Circumvention	N/A	N/A	N/A	N/A	Insufficient

With no circumvention options, and limited support for secure voice applications, Windows Phone was by far the least secure choice from the 5 major mobile operating systems. The only mitigating factor here may be that sales of Windows Phone in the countries surveyed was barely measurable according to both the user survey and the operating system statistics retrieved from Statcounter.

Developments

From the perspective of a threat analysis, recent and expected future developments should not be ignored. In this light, we note that in many countries the development of LTE was taken up, and in some countries implementation was already underway.

Since LTE (since release 8 in 2009) foresees the implementation of IPv6, this may serve to underline the importance of raising awareness for both tool makers and operating system manufactures to deal with this technology in a secure and transparent fashion.

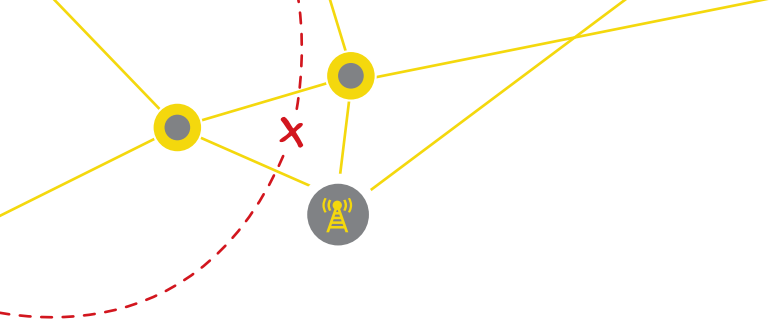
Furthermore there is a trend for applications and in recent weeks even operating systems (or at least large subsets of them) to be entirely web based. This is the expectation of a mobile operating system such as Firefox OS (formerly known as Boot to Gecko), from the Mozilla Foundation. Hopefully, publicly-licensed mobile operating systems would, in future, offer higher levels of security and safety to the end user.

Firefox OS aims to provide applications through an OS that basically presents similar features as an HTML5-enabled browser. Using special APIs, the underlying hardware is made available to the applications, allowing true web based apps (in HTML5) to run on the device.

On July 2, 2012, Mozilla announced[31] that leading operators Deutsche Telekom, Etisalat, Smart, Sprint, Telecom Italia, Telefónica, and Telenor are backing the open Firefox OS. The first Firefox OS powered devices are expected to launch commercially in Brazil in early 2013 through Telefónica's commercial brand, Vivo. Device manufacturers TCL Communication Technology (under the Alcatel One Touch brand) and ZTE also announced their intentions to manufacture the first devices to feature the new Firefox OS, using Snapdragon™ processors from Qualcomm. Mozilla and all other participants are committed to ensuring that the project is fully open and that the reference implementation of the required Web APIs is being submitted to W3C for standardization.

The combination of the two – HTML5 enabled applications and a fast, IP based mobile network – will enable a more IP-centered world, which, on the one hand, may provide users with added independence of OS and handset manufacturers, but on the other raises significant concerns for those users who's internet access is routinely blocked and monitored. Early attention to VPN or proxy access for such users would definitely be recommended.

31 http://blog.mozilla.org/blog/2012/07/02/firefox-mobile-os/

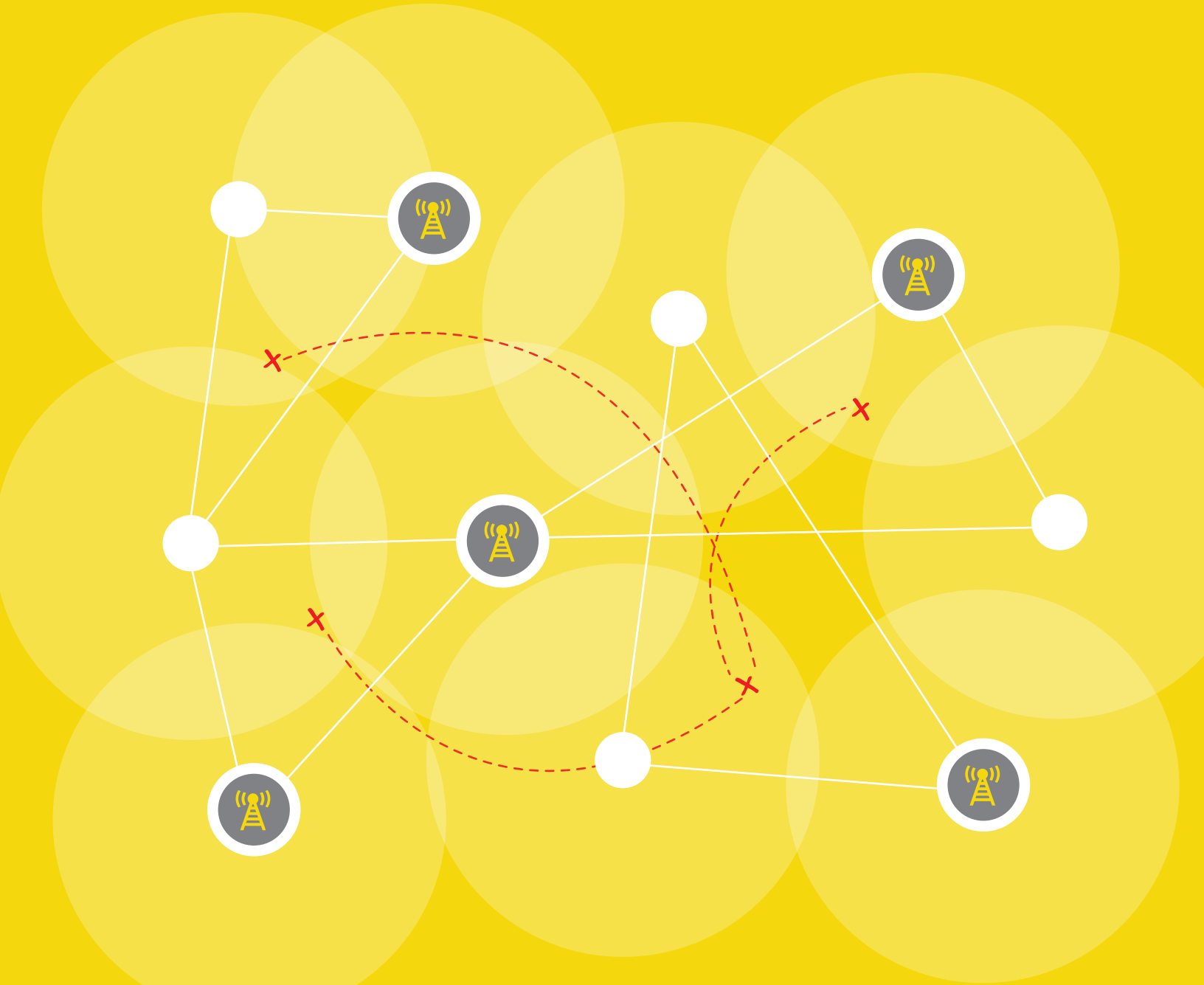


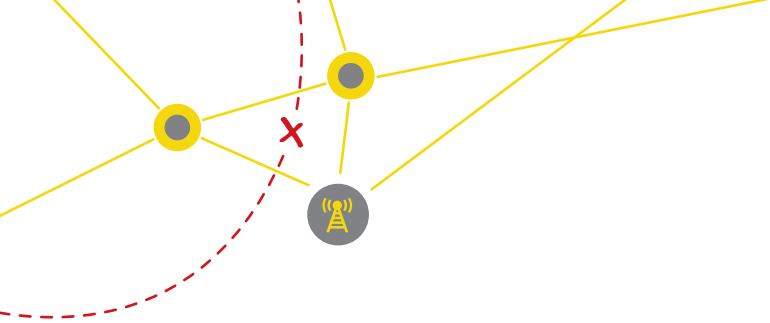
Conclusions

The following lessons can be derived if we look at the strengths and weaknesses of the various mobile operating systems, and the results of technical testing:

- Without further measures to enhance platform security ,the level and maturity of circumvention tools is of little relevance to the mobile security debate: platform trumps circumvention.
- Generally, all operating systems provide some level of circumvention and alternate voice and text messaging that can be considered secure for relatively low-risk communication. Most regular applications should be distrusted, however, since they provide no security, or limited security, or can be easily blocked or monitored. These should always be used with circumvention tools, if security is required.
- Circumvention on mobile devices appears to be largely reliant on VPN technologies, which differ greatly in their OS implementation, and all require service outside of the country in question.
- Using VPNs as a circumvention tools puts users at risk when switching connection type and where cryptographic implementation is concerned. Both OS manufacturers and service providers could do better and display more and better information and warnings about the availability and security of the VPN connection.
- Of all the platforms, Android scored the most complete “circumvention” and “voice/text” replacement options landscape. Although Android is up and coming, it would seem important to focus some development efforts at “legacy” Symbian phones, as their market share seems stable, and feature phones may reach an ever greater audience in countries with lower GDP.
- TOR is only available on Android, and was the first true circumvention tool available during the test period. A better landscape in OS support and different tools would be more conducive to the security of mobile users in oppressive regimes.
- IPv6 is overlooked by many manufacturers, as a security issue. It creates an easy way to monitor many users’ traffic, since it is hard to switch off and most phones support IPv6 routing and addressing on the fly. It should, at the very least, be disabled locally if circumvention tools are used. Id

Chapter 6:
Country Profiles





Country Profiles

The country profiles in this section were created from analysis of publicly available data from inside and outside the country, which was further developed and described by research conducted by in-country experts supported by an in-country survey of mobile use by users and activists. The purpose is to supplement the knowledge gained from the complex, comprehensive technical descriptions above and fundamentally supported by in-lab testing of handsets and software with a broader understanding of the political and social environment where these handsets are in use.

This section first provides a summary of the results for all the countries and then provides individual profiles for the individual countries. The purpose of the summary is to create a base reference point for a broader understanding of the individual countries.

The mobile communication market is a fast changing and highly volatile area. For example, in China, over 30 million additional subscribers were added to the mobile networks in the first three months of 2012 alone. This increase is larger than the absolute size of the Republic of Azerbaijan, Republic of Belarus, and Sultanate of Oman combined. During the evolution of this report one operator in Vietnam merged with a major mobile operator, and in Belarus a key plan to expand the market with a new player did not materialize.

In most markets there is a high dependence on mobile communication as the preferred strategy for both voice and data communication, and the fixed infrastructure is experiencing very low investment and growth. Only in one of the markets researched was mobile penetration less than 70% with only 4 markets less than 100% and there were 3 markets that achieved over 120% of penetration. The Kingdom of Saudi Arabia is remarkable for having almost achieved 200% penetration of the mobile market. It is clear that mobile communication is the preferred method of communication for all these markets.

ITU Country Statistics	Mobile cellular subscriptions	Market Penetration
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	73.6
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

The introduction of this report highlights the revenues in the mobile sector. The top 5 mobile operators generate revenues reaching over $300 billion and 1.7 billion subscribers. The markets researched in this report included almost 1.4 billion mobile service subscribers and 500 million of these were actively using mobile data services. Over 44 operators were included in the research for this report and the table below indicates that 9 of these operators were fully owned by the state with an overall subscriber base of over 1.1 billion subscribers.

Ownership	Number of Operators	Subscribers	Mobile Internet
State	9	1.12 b	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	1.38 b	534.74 m

Many of the operators were active in several countries and this provides a challenge for restricting the sale and use of dual-use technologies.

Country Overview

COMPARISON OF FIXED LINE TECHNOLOGIES WITH MOBILE TECHNOLOGIES

ITU Country Statistics	Fixed telephone subscrip-tions	Fixed broadband subscrip-tions	Mobile cellular subscrip-tions
Republic of Azerbaijan	1.51 m	0.46 m	9.1 m
Republic of Belarus	4.14 m	1.67 m	10.7 m
People's Republic of China	294.38 m	126.34 m	1.03 b
Arab Republic of Egypt	9.62 m	1.45 m	83.4 m
Islamic Republic of Iran (I.R.)	26.85 m	0.5 m	54.2 m
Libya	1.23 m	0.07 m	10.9 m
Sultanate of Oman	0.28 m	0.05 m	4.9 m
Kingdom of Saudi Arabia	4.17 m	1.5 m	56.1 m
Syrian Arab Republic	4.07 m	0.07 m	11.9 m
Tunisian Republic	1.29 m	0.48 m	12.5 m
Republic of Uzbekistan	1.86 m	0.09 m	24.3 m
Socialist Republic of Vietnam	16.4 m	3.63 m	119.0 m

ITU Statistics http://www.itu.int/ITU-D/ict/statistics/index.html

PRODUCT PRICING

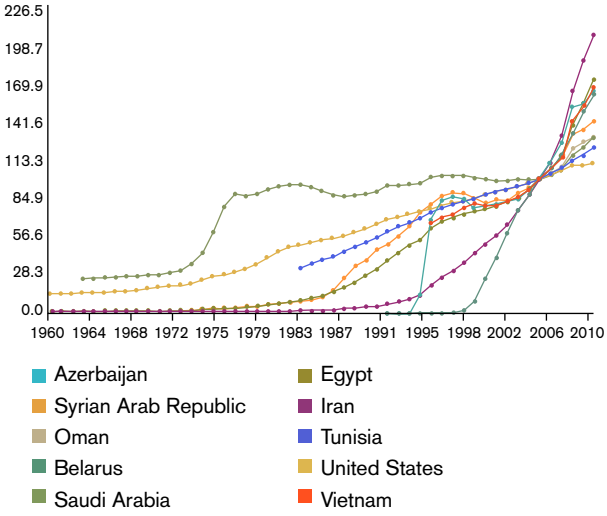
To compare the cost of services between countries is very challenging, and comparing cost of services between different mobile operators is an additional level of complexity because the cost of living is different and the maturity of the mobile markets varies widely. The World Bank maintains a very comprehensive analysis of the variations in the consumer price indices. The chart below describes these variations for the selected countries. An alternative method would be to use the Big Mac Index[32] outlined by The Economist.

CONSUMER PRICE INDEX (2005=100)

Consumer price index reflects changes in the cost to the average consumer of acquiring a basket of goods and services that may be fixed or changed at specified intervals, such as yearly.

http://www.indexmundi.com/facts/indicators/FP.CPI.TOTL/compare?country=sa#country=az:by:eg:ir:om:sa:sy:tn:us:uz:vn

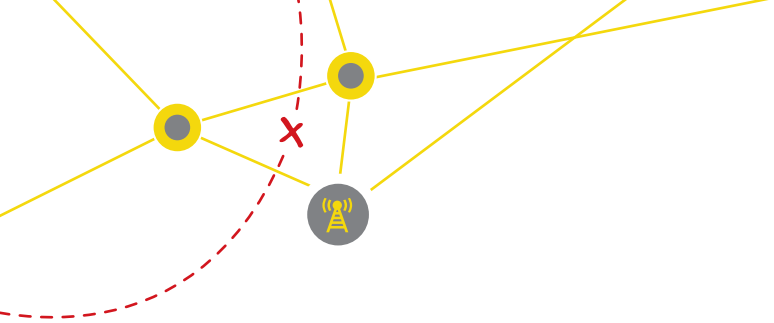
http://data.worldbank.org/data-catalog/world-development-indicators



Data Source: World Bank, World Development Indicators - Last updated March 2, 2011
See also: Thematic map

The cost of services from the 44 operators identified for this report was created from a sample of basic services identifying the different costs between pre-paid and post-paid services for voice, data, and text messaging. These charges were then converted into US$ for comparison. The type of service being marketed, the structure of the pre- and post-paid packages, and the range of handsets in use vary significantly between countries and between operators inside each country. This makes it difficult to create an easy table for comparison. However the intent of the table below is to indicate the level of maturity that the selected markets have achieved, and the results provide a helpful indication of the costs in each country for a user to have access to mobile communication and the differences between countries.

32 http://www.economist.com/search/apachesolr_search/big%20mac%20index



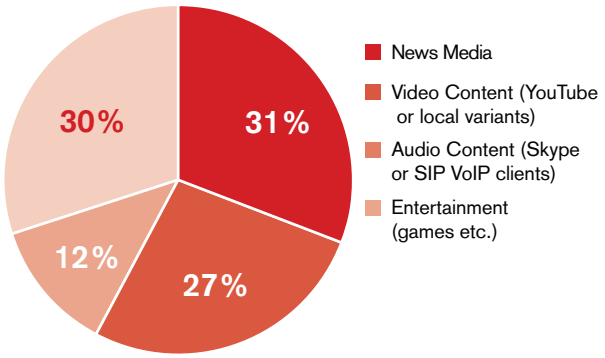
Pricing Analysis ($US)	Azerbaijan	Belarus	China	Egypt	Iran	Oman	Saudi Arabia	Syria	Tunisia	Uzbekistan	Vietnam
PRE-PAID Package Pricing											
Monthly Package Cost	-	-	-	-	-	28.15	24.00	-	-	0.30	-
Cost per Minute for National Call (First 3 Min)	0.09	0.04	0.04	0.06	0.07	0.27	0.43	0.13	0.14	0.03	0.06
Price for Data Traffic (Price per MB)	0.03	0.12	0.08	0.03	0.29	0.05	0.03	0.05	0.01	0.07	0.05
Price for One Text Message	0.04	0.02	0.02	0.06	0.01	0.02	0.07	0.13	0.03	0.02	0.02
POST-PAID Package Pricing	-	-	-	-	-	-	-	-	-	-	-
Monthly Package Cost	3.41		7.60	35.78	-	79.22	29.33	7.47	-	9.40	2.40
Cost per Minute for National Call (First 3 Min)	0.09		0.03	0.03	0.05	0.26	0.24	0.08	0.52	0.02	0.04
Price for Data Traffic (Price per MB)	0.29		0.08	0.03	0.45	0.01	0.03	0.05	0.01	0.09	0.01
Price for One Text Message	0.04		0.02	0.05	0.01	0.03	0.05	0.08	0.03	0.02	0.01

RANKING BY CHEAPEST	Azerbaijan	Belarus	China	Egypt	Iran	Oman	Saudi Arabia	Syria	Tunisia	Uzbekistan	Vietnam
PRE-PAID Package Pricing											
Monthly Package Cost						11	10			9	
Cost per Minute for National Call (first 3 min)	7	3	2	5	6	10	11	8	9	1	4
Price for Data Traffic (Price per MB)	2	10	9	3	11	6	4	7	1	8	5
Price for One Text Message	8	5	2	9	1	4	10	11	7	6	3
POST-PAID Package Pricing											
Monthly Package Cost	4	1	6	9	1	10	8	5	1	7	3
Cost per Minute for National Call (First 3 Min)	7		2	3	5	9	8	6	10	1	4
Price for Data Traffic (Price per MB)	9		7	4	10	2	5	6	3	8	1
Price for one text message	7		3	8	2	5	9	10	6	4	1

MARKET PROFILE

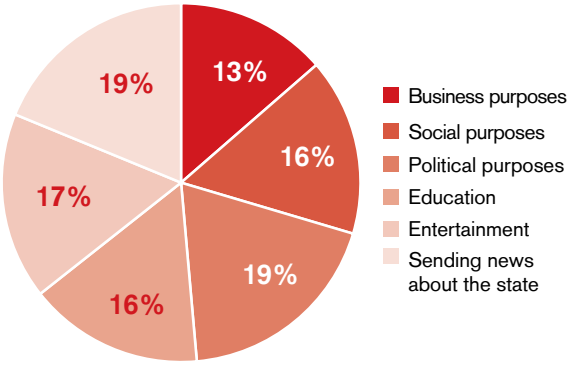
Fixed internet users use the internet for a wide range of activities, and this is no different for the mobile internet user. However, it is particularly important for the countries we have selected to identify the key activites of moblie internet use in those environments.

TYPES OF APPLICATIONS TYPICALLY USED BY MOBILE BROADBAND SUBSCRIBERS



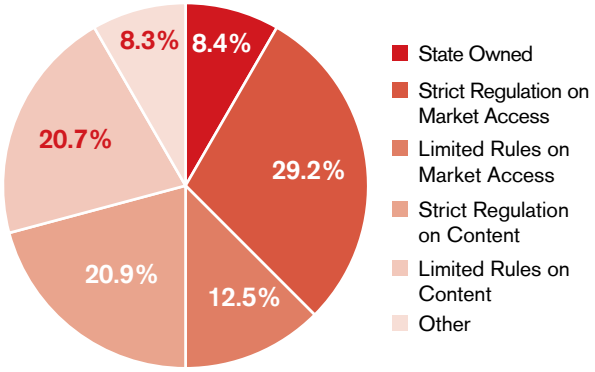
The focus of mobile internet users in these countries is on access to news content.
Second area of use is for entertainment.
Third, users are also interested in accessing video content from sources such as YouTube or the national variants of YouTube.

RATING THE IMPORTANCE OF UNFILTERED INTERNET ACCESS



Unsurprisingly, due to the scale of the mobile markets the need for access to an open and unfiltered internet is considered essential for all aspects of mobile internet use.

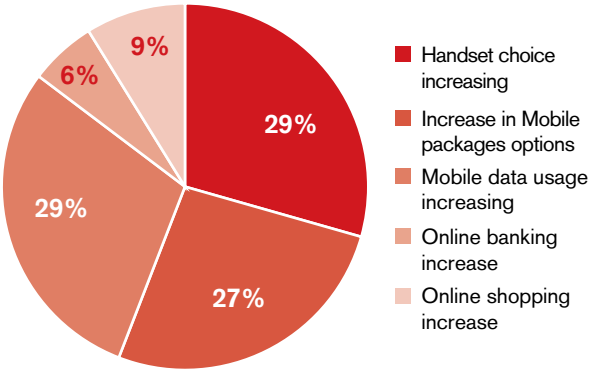
TELECOMMUNICATION MARKET REGULATION



Analysis of the markets selected for this report show a range of state strategies for ensuring efficient state oversight of mobile operators, both in terms of the market participants and in terms of the activites of the licensed market operators in operation.
The intention of state oversight is to support and encourage extensive investment and sector growth while ensuring varying levels of state control over operations.

MARKET TRENDS

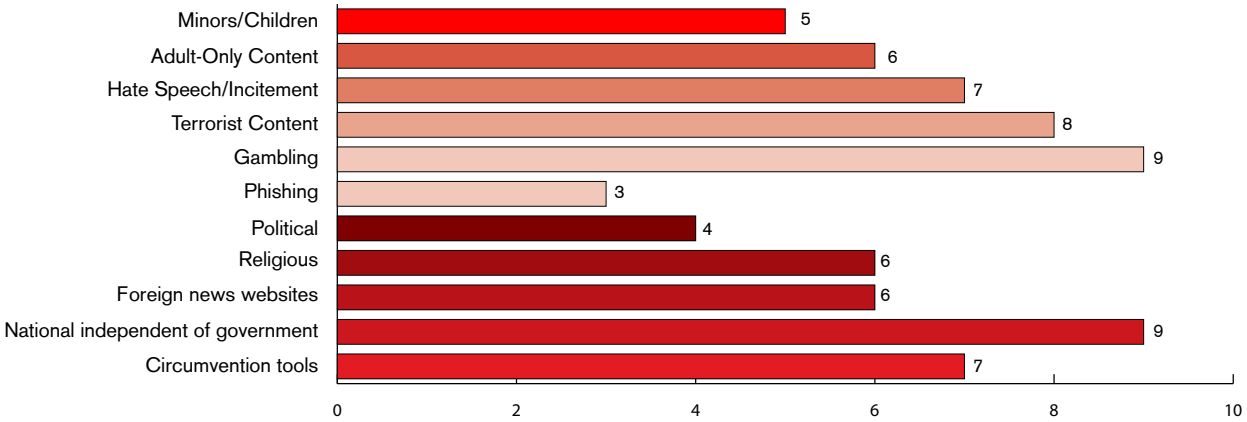
WHAT ARE THE CURRENT TRENDS IN THE MOBILE MARKETS



Handset choice is increasing in each market and new mobile packages are regularly made available. Mobile data usage is also increasing. All these suggest vibrant, competitive markets with strong demand in the future.

Note that a wide variety of handsets provides a challenge for state security agencies to have hardware options specifically designed for their market.

NUMBER OF COUNTRIES WHERE SPECIFIC CONTENT IS BLOCKED OR FILTERED



Mobile internet blocking occurs in a variety of ways. Many of the markets operate with direct blocking being required or implemented by government agencies, but there are many other ways that blocking is performed.

Note that public mobile internet, will at some point ,connect to the fixed line internet and incur the same blocking capabilities as fixed line.

A wide range of content is blocked in the countries of interest. Much of this content is considered illegal in countries across the world.

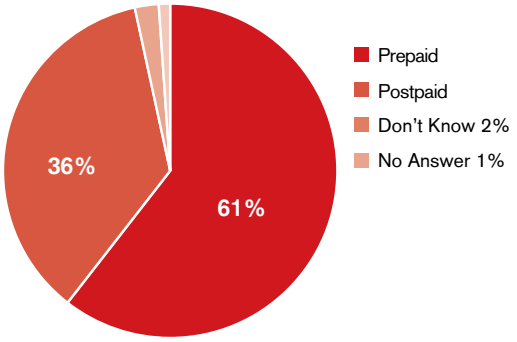
However, some of the content blocking, such as that of religious, foreign news, or national news sources, is a direct challenge to freedom of speech.

IN-COUNTRY MOBILE USERS

This is a summary of all the respondents received for all countries to provide an overview of the key results from the in-country surveys. 1,644 responses were analyzed with between 100-250 respondents per country, except for Libya and Egypt, which had a very low number of respondents.

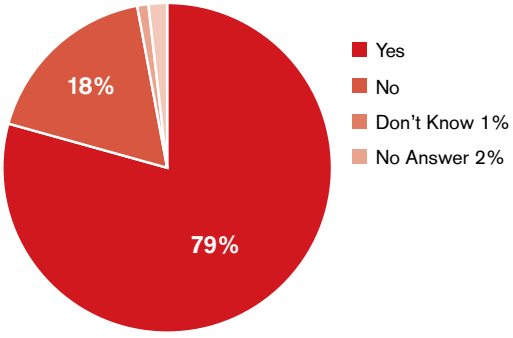
PROFILE OF RESPONDENTS

DO YOU USE PRE-PAID OR POST-PAID MOBILE SERVICE?



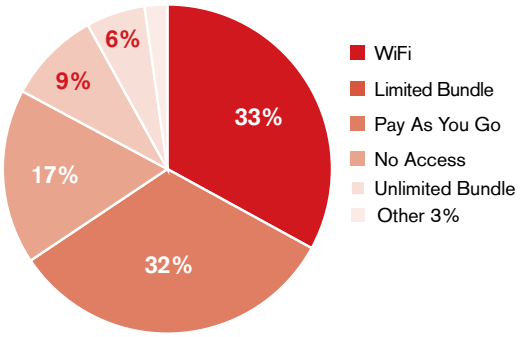
Over 60% of users were using pre-paid services with their mobile operator. Over 36% have a post-paid contract in place.

DO YOU HAVE ACCESS TO THE INTERNET USING MOBILE INTERNET SERVICES?



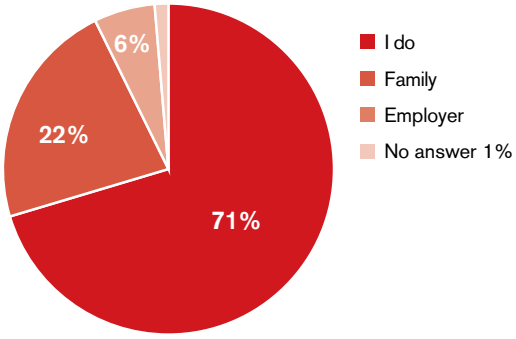
79% of mobile users have access to the internet using their mobile phone. Almost 18% did not have access to the internet.

HOW DO YOU HAVE ACCESS TO THE INTERNET ON YOUR MOBILE PHONE?



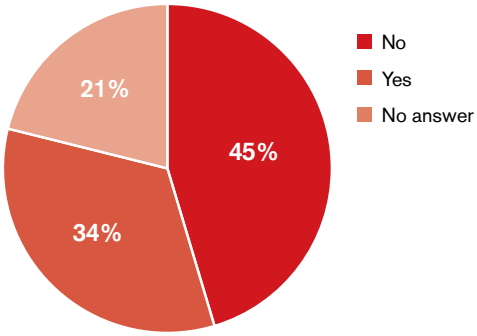
Almost 33% of users have access to the internet using a WiFi service. Access via a limited bundle (32%) and a pay-as-you-go service (17%) are the next most popular methods of connecting to the internet from a mobile handset.

WHO PAYS FOR YOUR MOBILE PHONE USE?



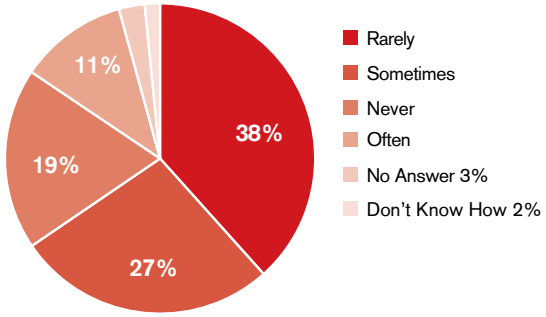
This unusual question is to determine who would know and understand the cost of the services, and who would have access to detailed billing records for analysis. Over 70% paid for their own phone services and 22% were paid by their family. This indicates who would have access to their billing information and usage. A high level of employers would indicate possibilities of third party access to billing information.

DO YOU RECEIVE DETAILED BILLS FOR YOUR MOBILE PHONE USAGE?



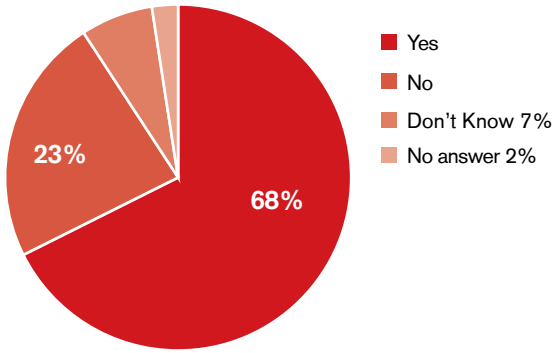
Detailed billing is an excellent method for users to gain greater knowledge and awareness of the range of data that is collected by a mobile operator and what data would be available to authorized state agencies to analyze.

HOW OFTEN DO YOU SHARE CONTENT USING BLUETOOTH ON YOUR MOBILE PHONE?



Over 57% said that they "rarely" or "never" share content using Bluetooth. Over 38% indicated that they share content "often" or "sometimes" – at least confirming they have the knowledge to share content. Sharing content using personal area networks (short distance) is more secure and harder to detect by investigators unless the Bluetooth network id (unique to each handset) is pre-stored by the handset retailer.

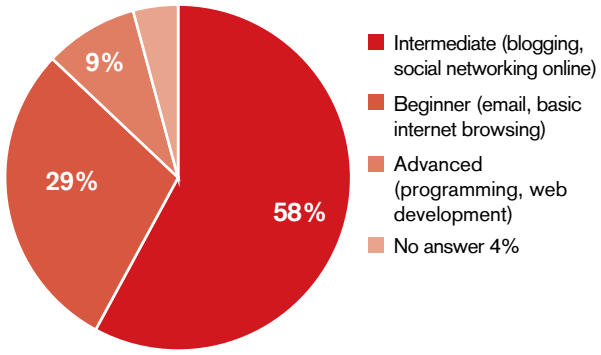
IS YOUR HANDSET A SMARTPHONE?



Over 68% of all respondents indicated that they did own smartphones, leaving a significant minority of 23% who did not have a smartphone, and a small grouping of 7% who did not know what a smartphone was. (It is reasonable to assume that they do not since the cost of a smartphone would need to be justified and explained to a prospective shopper).

PROFILE OF EQUIPMENT IN USE

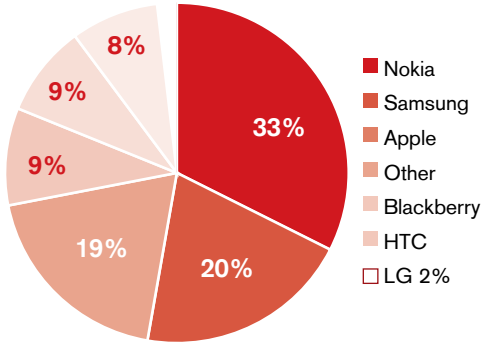
WHAT IS YOUR SKILL LEVEL AS A MOBILE INTERNET USER?



Over 58% of respondents indicated that they have an intermediate level of knowledge for internet use on mobile handsets.

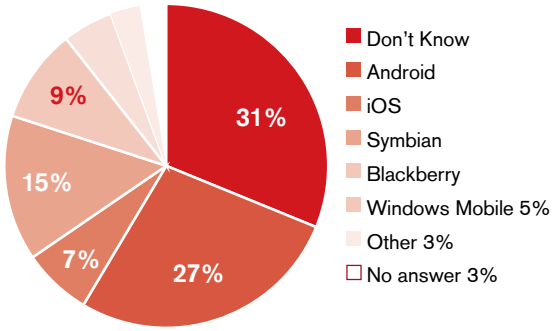
This suggests that these users would be able to implement reasonably complex instructions and guidelines for protecting their online activities.

WHO MANUFACTURED THE HANDSET YOU USE?



Handsets from Nokia (33%) are still the most prevalent. Samsung (20%) comes second, then Apple (19%). These three manufacturers share almost 72% of the whole market.

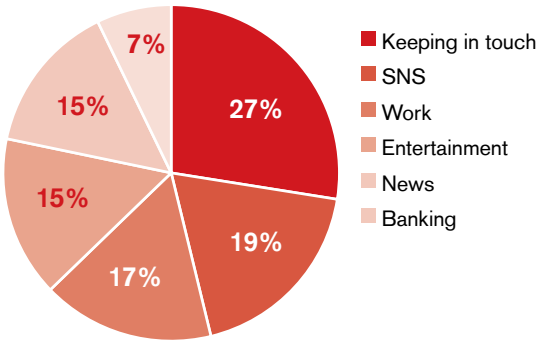
WHAT OPERATING SYSTEM DOES YOUR PHONE USE?



It is a challenge to offer security advice and tools if the end user does not know what type of operating system is installed on their handset. Basic risk and security advice would be needed for this category of users. The second most common platform is the Android operating system and Symbian is still very common.

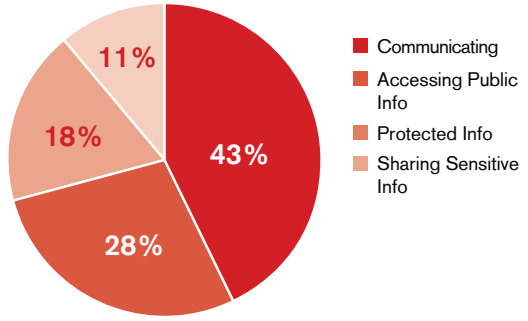
ACTIVITIES USING MOBILE HANDSETS AND MOBILE INTERNET

HOW DO YOU SPEND YOUR TIME USING YOUR MOBILE HANDSET?



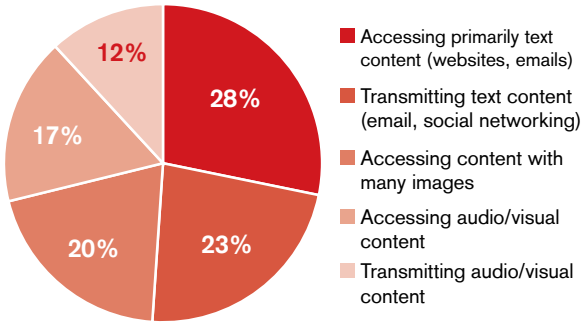
Most users spend their time on their mobile handset for the purpose the phone was created, which is keeping in touch with others. In the online environment it is used extensively for social networking services. The rest of the time is spent on work, entertainment, and news.

HOW DO YOU SPEND YOUR TIME ON MOBILE INTERNET?



One of the key risk issues is to determine the primary activity of users on the mobile internet. This will also help determine whether users want to bypass internet blocking measures to **read** content that is blocked, or want to **send** data to outside organizations. The answer will determine the level of security required with mobile apps.

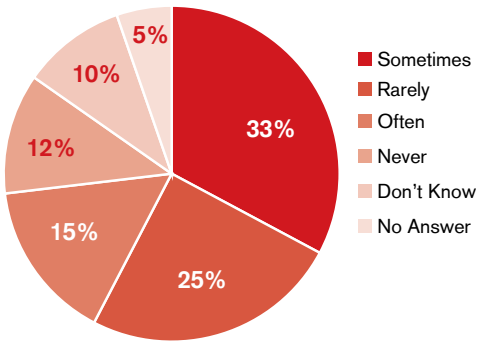
WHAT TYPE OF CONTENT DO YOU USUALLY ACCESS ON THE INTERNET?



There are different approaches to bypassing internet monitoring and blocking systems depending on whether the user wants to access content or to transmit content. Handling audio-visual content is an extra level of complexity, because it requires high-quality reliable network connections in conjunction with a trusted assignee who will remove any geo tagging on the audio/visual content.

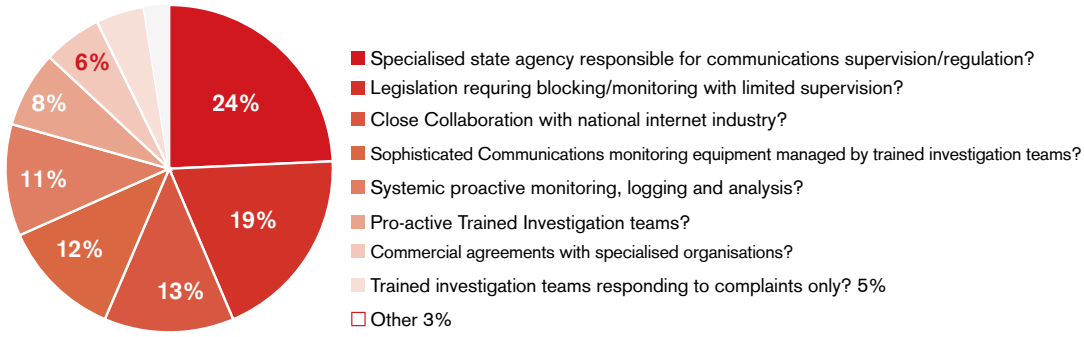
EXPERIENCES WITH ONLINE MOBILE CENSORSHIP AND CIRCUMVENTION

WHEN YOU USE THE MOBILE INTERNET, HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES?



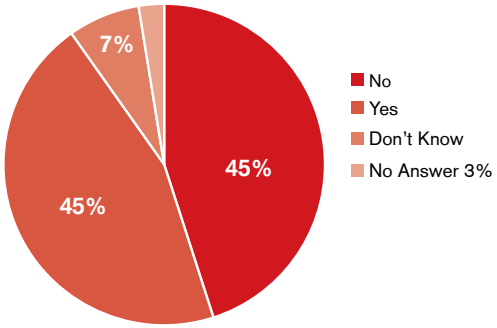
This provides a clear indication of the frequency of being prevented from accessing web content on mobile networks, and the level of awareness of users that blocking is being implemented.

IN YOUR OPINION HOW DOES YOUR COUNTRY FILTER OR MONITOR MOBILE INTERNET CONTENT?



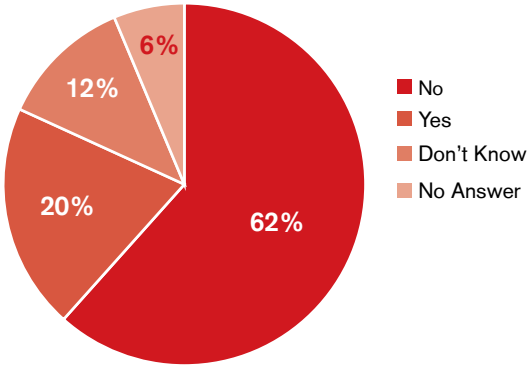
There are many ways for internet blocking and monitoring to be performed by a state. In most cases they will use a range of measures. This question seeks to determine the level of awareness among respondents about the capacities of their state to perform extensive monitoring, and therefore to increase awareness on the level of risk they incur in the use of their mobile handsets.

HAVE YOU EVER UPDATED THE FIRMWARE ON YOUR MOBILE PHONE?



The number of users who have upgraded their mobile phone provides a good indication of the level of understanding of the capabilities for the software to be updated/re-configured.

IS YOUR MOBILE PHONE 'JAILBROKEN'?



If a phone is "jailbroken" we can surmise that the user has significant competence with software and with performing upgrades and understands the possibilities of changing the core configuration of their handset. The number of persons who don't know is even more interesting, as it indicates that the number of users who do not understand what this question means.

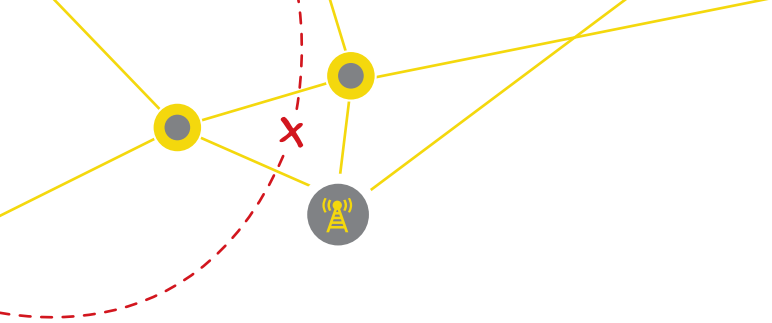
WHO DO YOU TRUST TO PROTECT THE PRIVACY OF YOUR MOBILE INTERNET COMMUNICATIONS?

Trusted Sources of Mobile Internet Communication — Includes Don't Knows

	Rank	Never (max = 5) Always
Government	11	1.1
State Agencies	10	1.2
ISP Inside	6	1.3
ISP Outside	1	1.5
NGO inside	7	1.3
NGO outside	9	1.3
CSP inside	8	1.3
CSP outside	5	1.3
Personal inside	2	1.5
Personal outside	3	1.4
Software Engineers	4	1.4
Other	12	0.7

It is very clear from the response to this question that there is very little trust for all stakeholders in this complex area. The main winners are ISPs outside of your national country (first place), personal friends and contacts inside of your country (second), and personal friends and contacts outside of your country (third).

Interestingly, national governments are treated with great distrust (last place) and are joined by state agencies (second to last place).



List of Countries

- Republic of Azerbaijan
- Republic of Belarus
- People's Republic of China
- Arab Republic of Egypt
- Islamic Republic of Iran
- Libya
- Sultanate of Oman
- Kingdom of Saudi Arabia
- Syrian Arab Republic
- Tunisian Republic
- Republic of Uzbekistan
- Socialist Republic of Vietnam

Republic of Azerbaijan

Mobile penetration is at an amazing 99% of population.

Indicator[33]	Measurement	Value
Computers	Per 100	5.7
Internet Users	Per 100	46
Fixed Lines	Per 100	16
Internet Broadband	Per 100	15
Mobile Subscriptions	Per 100	99
WiFi		
Mobile Broadband	% Internet Users	17.4
International Bandwidth	Per 100	4.6kb

At more than nine million, Azerbaijan is a mid-sized market for its three mobile networks. Government interference with internet content is observed by some users, although not all seem affected. The market is otherwise competitive with part-state and part-privately owned operators.

TELECOMMUNICATIONS MARKET

Azerbaijan exercises strict regulation on market access and limited rules on content. There are 3 GSM operators in Azerbaijan – Azercell (the largest), Bakcell (first operator in Azerbaijan), and Narmobile (Azerfon), which was the first to be awarded a 3G license.

In December 2011, Azercell[34] announced a project for the students of Nakhchivan State University where China's ZTE, which provides technological solutions, will enable 4G access for more than 4 thousand students. Azercell has tested 4G technology in 2 universities – Gafgaz and Nakhchivan State University in 2011.

Azerbaijan's three mobile operators are all privately owned. Some are largely in foreign private ownership, although some have ties with the state-owned Aztelekom and the Aliyev family (the family of the nation's current president, in the case of Azerfone) or western operators (Azercell is largely owned by the Swedish and Finnish firm of TeliaSonera)[35].

33 www.azstat.org

34 http://gun.az/hitech/22295

35 http://www.rferl.org/content/azerbaijan_president_aliyev_daughters_tied_to_telecoms_firm/24248340.html

QUICK FACTS –AZERBAIJAN

Land Area: 87,474 sq km *
Population: 9.077 million
GDI per capita, PPP $9,270 (WB, 2010)

TLD: .AZ
Fixed Telephones: 1.5 million (2010)
GSM Telephones: 9.1 million (2010)
Fixed Broadband: 0.5 million (2010)
Internet Hosts: 0.2 million (2010)
Internet Users: 4.2 million (2010)

Pricing Analysis ($US)	Azerbaijan	All countries surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute for National Call (First 3 Min)	0.09	6	0.09
Price for Data Traffic (Price per MB)	0.03	2	0.05
Price for One Text Message	0.04	8	0.02
POST-PAID Package Pricing			
Monthly Package Cost	3.41	5	7.47
Cost per Minute for National Call (first 3 min)	0.09	7	0.06
Price for Data Traffic (Price per MB)	0.29	9	0.04
Price for One Text Message	0.04	7	0.03

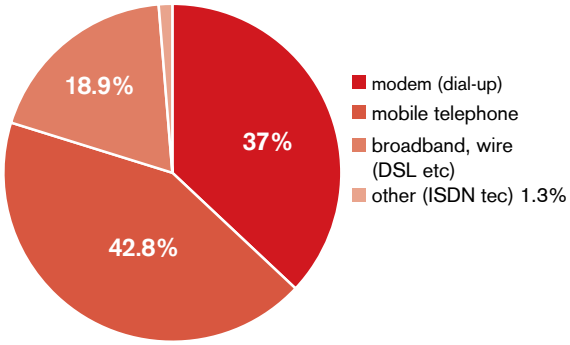
Azerbaijan was ranked 2nd cheapest country for access to mobile data.

Operator	Azercell	Bakcell	Azerfon MMC
Brands	Simsim, 3GMax	Cin, , Klass, Suret	Super Nar3G
Survey Respondents	37%	35%	28%
Subscribers	4,200,000	2,000,000	1,600,000
Mobile Internet Users	1,000,000	390,000	120,000
Ownership	Foreign	Foreign	National-Foreign

INTERNET ACCESS

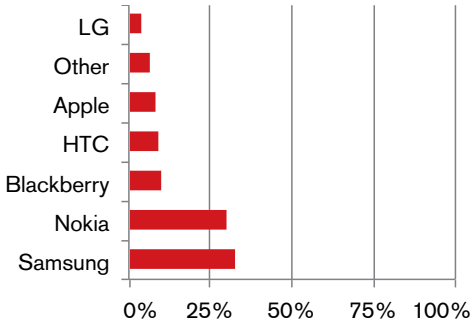
74% of respondents used mobile internet. Of these 50% used WiFi to access the internet with 18% paying for a limited volume of data with their subscription, and a further 17% paying for usage. There is still a significant number of internet users accessing the internet using dial up, but the greatest number of users access the internet via mobile broadband.

INTERNET CONNECTION TYPES 2010

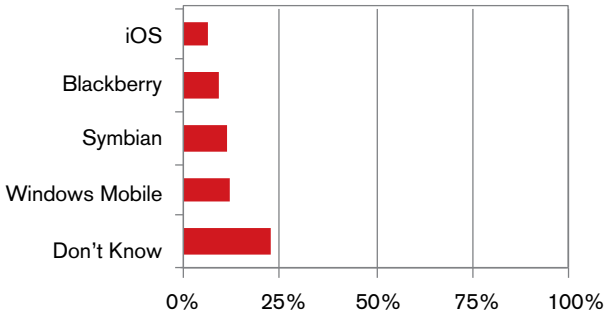


http://www.azstat.org

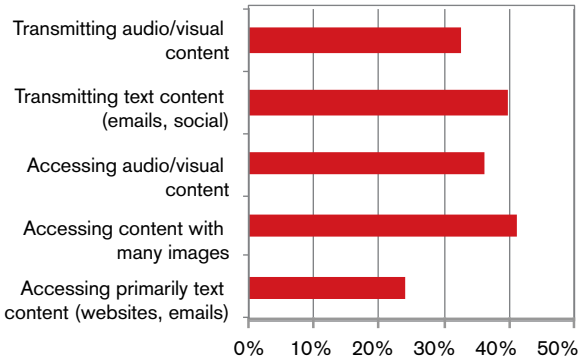
HANDSET MANUFACTURERS



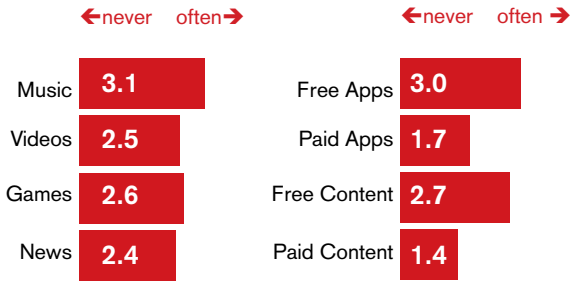
MOBILE OS IN USE



USE OF THE MOBILE INTERNET



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)



CENSORSHIP AND CIRCUMVENTION

In January 2012, Cabinet of Ministers introduced new regulations[36] that require every mobile phone to be registered with the state communications authority (the Ministry of Communications and Information Technology). All foreigners will also be required to register their phones, since non-registered phones will be cut from service.

In January 2012, the Azeri press[37] described plans to create the National Information Security Center within the Ministry of Communications and Information Technology. This center should be created in 2012, and its main duties will monitor the countries network infrastructure, announce information about new threats and measures against them, and help other organizations in case of emergencies concerning information security. Little information is available on the country's monitoring and blocking policies and equipment.

Less than 5% of responses believed that their country had systemic pro-active monitoring, logging, and analysis of communications. 23% believed that there was legislation requiring blocking and monitoring with limited supervision, 18% indicated that there were pro-active trained investigation teams, and 13% indicated that they were aware of specialized state agencies responsible for communications regulation and supervision. A further 13% of responses indicated that there were commercial agreements with specialized organizations.

On July 13th, 2011, Azerbaijani President Ilham Aliyev stated[38] that there were no restrictions on access to the internet in Azerbaijan because of the government's desire to promote media freedom, RFE/RL's Azerbaijani Service reported.

Only 20% of users indicated that they often encounter blocked websites.

Only 13% of users have jail-broken their phone and only 20% have ever updated the firmware on their phone.

36 http://www.eurasianet.org/node/64827

37 http://lent.az/xeber_85684_Az%C9%99rbaycanda_%C4%B0nformasiya_T%C9%99hl%C3%BCk%C9%99sizliyi_%C3%BCzr%C9%99_Milli_M%C9%99rk%C9%99z_yarad%C4%B1lacaq

38 http://www.rferl.org/content/president_praises_azerbaijan_internet_freedom/24264938.html

PHONE BRANDS[39]

Phone	E2152	E3	X2-01	Asha-200-Duos	X101-Duos
Manu	Samsung	Nokia	Nokia	Nokia	Nokia
Released	Sep 2010		Jan 2011	Feb 2012	
					
Data	GPRS/EDGE C10		GPRS/EDGE C32	GPRS/EDGE C12	No
Sensors	Dual-SIM			Dual-SIM	Dual-SIM
Internet	Yes	Email		No (lo-speed)	
GPS	No		No	No	No
Camera	1MP	5MP	1MP	2MP	No
WiFi	No	Yes	No	No	No

CONCLUSION

With relatively high mobile and regular internet access availability, Azerbaijan is an opportune market for actors in the mobile internet freedom area. Limited use of circumvention technology is observed despite a majority of participants reporting some form of government blocking and monitoring. The government is actively pursuing more control, as is evidenced by recent initiatives imposing stringent registration requirements on mobile phones using the countries network infrastructure.

FURTHER INFORMATION

Ministry of Communications - www.mincom.gov.az
State Statistical Committee - www.azstat.org
Bakcell – www.bakcell.com
Azercell – www.azercell.com
Azerfon - www.narmobile.az

39 Data and images from www.gsmarena.com

Republic of Belarus

With a mid-level income and a population of 9 million, Belarus presents a mid-sized market that has many characteristics of modern western telecommunications markets. Although some restrictive legislation is in place, especially where the sale of services is concerned, Belarus seems a promising, yet non-democratic marketplace where mobile internet access is concerned. Mobile penetration has reached over 108% of the population.

TELECOMMUNICATIONS MARKET

Indicator[42]	Measurement	Value
Computers	Per 100	26.0 (2007)
Internet Users	Per 100	32.1
Fixed Lines	Per 100	43.6
Internet Broadband	Per 100	17.55
Mobile Subscriptions	Per 100	108.9
Mobile Broadband	% internet users	17.4%
International Bandwidth	Per 100	4.76kb

There are 4 operators in Belarus - Velcom, offering voice/text/data and positioned as quality operator; MTS Belarus, offering voice/text/data and positioned as fair price operator; Life, offering voice/text/data, entered market later and is still behind other GSM operators in quality and coverage; Belcel (CDMA) is focused on data plans primarily, but also offers voice/text services and is positioned as a high-speed mobile internet provider rather than a traditional mobile operator. There was one additional potential operator called Yota, which planned to offer data only, using LTE standard. However, Yota recently announced that it intended instead to exit the Belarus market in order to focus on its Russian market. Yota.by was initially set up as a wimax carrier but never achieved the same market interest as in Russia.

ARPU (Average Revenue Per User) plummeted for all operators, because of devaluation of currency in 2011.

QUICK FACTS – BELARUS

Land Area:	207,600 sq km*
Population:	9.5 million
GDI per capita, PPP	$13,590 (WB, 2010)
TLD:	**.BY**
Fixed Telephones:	4.2 million (2011)
GSM Telephones:	10.7 million (2011)
Fixed Broadband:	1.7 million (2010)
Internet Hosts:	68,118 (2010
Internet Users:	6.8 million (2010)

Velcom implemented IPv6 on 6th June 2012 for the international IPv6 day and announced that the official website www.velcom.by would be permanently reachable in IPv6-protocol. According to Christian Ladstaetter, Head of the Velcom IT Division, they are now preparing their network to provide IPv6 services to subscribers in the future.

40 www.worldbank.org

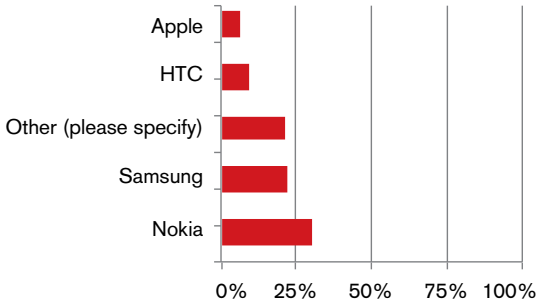
Pricing Analysis ($US)	Belarus	All countries surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute National Call (first 3 min)	0.04	2	0.09
Price for Data Traffic (Price per MB)	0.12	10	0.05
Price for One Text Message	0.02	5	0.02
POST-PAID Package Pricing			
Monthly Package Cost		1	7.53
Cost per Minute National Call (first 3 min)			0.06
Price for Data Traffic (Price per MB)			0.04
Price for One Text Message			0.03

Operator	Velcom	MTS	Life	Belcel
Brands				diALLOg
Survey Respondents	36%	42%	8%	28%
Subscribers	4,620,400	4,880,000	1,700,000	196,000
Mobile Internet Users	830,000	350,000	680,000	200,000
Ownership	Austria	Russia	Turkey/ Sweden	Netherlands

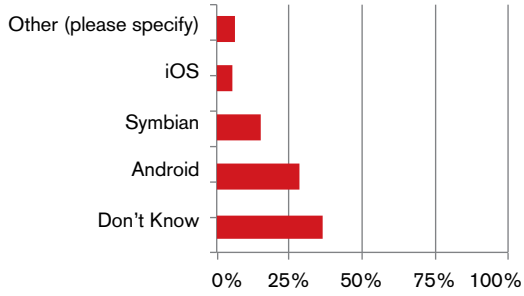
INTERNET ACCESS

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.

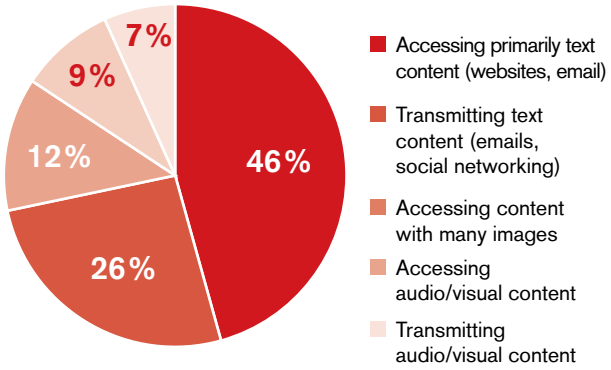
TOP 5 HANDSET MANUFACTURERS



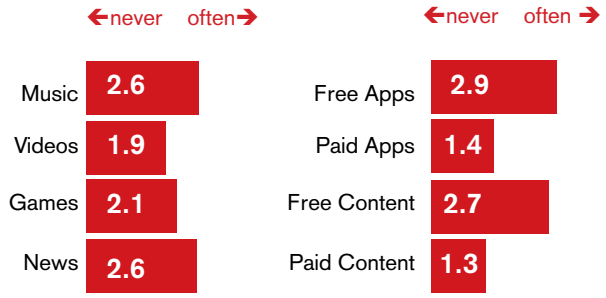
TOP 5 MOBILE OPERATING SYSTEMS



USE OF THE MOBILE INTERNET 2012



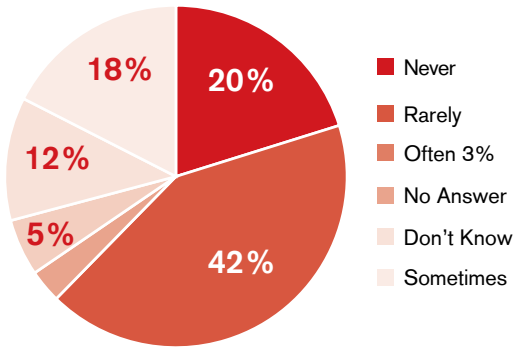
TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)



CENSORSHIP AND CIRCUMVENTION

Legislation introduced and refined in the period of 2010-2011[41] (Law № 317-3 of the Code of Administrative Offences) obliges internet providers (and mobile operators) to block certain websites if services are provided to state-owned entities, or by choice of a subscriber. This legislation also requires internet cafés and WiFi hotspot owners to register all users' IDs.

HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN-COUNTRY SURVEY)



Business entities engaged in the sale of goods and services that require the use of information networks (including systems and resources with an internet connection) and operating in the territory of Belarus must be registered in the manner prescribed by legislation. Of its own volition, Operator Life blocked several opposition websites, but later remote these blocks. There is widespread belief that internet traffic, text messages, and voice calls of oppositional activists are routinely monitored.

The OpenNet Initiative (ONI) report on Belarus[42] indicates that "Officially, internet filtering and monitoring of telecommunications networks are illegal in Belarus. However, authorities conduct surveillance of Internet activities under the pretext of protecting national security. In 2001, the president extended the concept of 'national security' to include the Internet as a potential threat to the information security of the country."

In 2007 and 2008, ONI tested seven main ISPs: Atlant, Aichyna, BASNET, Belinfonet, Belpak (Beltelecom), BN, and Solo. The testing confirmed blocking by almost all ISPs. Many Web sites tested on the academic network BASNET were inaccessible in Belarus, including position websites and local and global freedom of expression websites. International social networking, hosting, e-mail, P2P, and translation and multimedia Web sites were also filtered on BASNET, in addition to Web sites containing information on drug and alcohol consumption, as well as terrorist activities. Google transparency does not report any takedown requests from Belarus. Reporters Without Borders, reports[43] that in January 2011, Estonia stated that it was ready to put its cyber expertise to work on behalf of the Belarusian opposition to teach them "how to manage their internet websites and protect them against cyberattacks."

41 http://pravo.by/main.aspx?guid=71393

42 http://opennet.net/research/profiles/belarus

43 http://en.rsf.org/surveillance-belarus,39746.html

PHONE BRANDS[44]

Phone	S5830 Galaxy Ace	I9100 Galaxy II	iPhone 4	N7000 Galaxy Note	S5660 Galaxy Gio
Manu	Samsung	Samsung	Apple	Samsung	Samsung
Released	February 2011	April 2011	June 2010	October 2011	March 2011
					
Data	GPRS/EDGE C10	GPRS/EDGE C10	GPRS/EDGE C10	GPRS/EDGE C12	GPRS/EDGE
Bluetooth	V2.1 vA2DP	v3.0+HS	v2.1 with A2DP	v3.0 with A2DP	v2.1 with A2DP
Sensors	Accelerometer, Proximity, Compass	Accelerometer, Gyro, Proximity, Compass	Accelerometer, Gyro, Proximity, Compass	Accelerometer, Gyro, Proximity, Compass, Barometer	Accelerometer, Proximity, Compass
Internet	Yes	Yes	Yes	Yes	Yes
OS	Android 2.3	Android 4x	IOS 5.1	Android 4x	Android 2.3
GPS	Yes (A)	Yes (A)	Yes (A)	Yes (A+Glonass)	Yes (A)
Camera	5MP	8MP	5MP	8MP	3.15MP
WiFi	b,g,n	a,b,g,n	b,g,n	a,b,g,n	b,g,n

There are no official statistics on handset use and it is noted that there is a significant black market for imported handsets.

CONCLUSION

Although the mobile penetration is over 100%, the market in Belarus has strong competition. There is a lot of activity in the apps markets and the handset options are from a range of recent smartphones.

FURTHER INFORMATION

Ministry of Communications and Information of the Republic of Belarus - http://www.mpt.gov.by/en/
National State Statistical Committee of the Republic of Belarus - belstat.gov.by
Velcom – www.velcom.by
MTS - www.mts.by
Life – www.life.com.by
Belcel – www.belcel.by

44 Data and images from www.gsmarena.com

People's Republic of China

The size of the Chinese mobile market is truly staggering. In Q1 2012, mobile operators gained an additional 30 million users to mobile networks. Mobile penetration has reached 74% and continues to grow. The mobile operator China Mobile is the largest telecom company in the world.

TELECOMMUNICATIONS MARKET

Indicator[45]	Measurement	Value
Computers in Households	Per 100	38.4
Internet Users	Per 100	34.4
Fixed Lines	Per 100	21.3
Fixed Broadband	Per 100	9.44
Mobile Subscriptions	Per 100	73.6
Mobile Broadband	Per 100	11.9
International Bandwidth	Per 100	n/a

On March 30th, 2012, the country's Ministry of Industry and Information Technology confirmed that, as of the end of February, there were more than a billion mobile subscribers in the country (1.01 billion, to be specific). As the AFP notes, that refers to individual subscriptions, including users with more than one phone, but any way you slice it that is a whole lot of cellphone users. Of those, 143.92 million are on 3G networks, which is fully double the number from April of 2011. Fixed line phones have dropped to 284.3 million.

Internet use also continues to be on the upswing, with more than half a billion people having internet access of some sort, and 154.96 million having broadband access (up nearly five million during those same two months).[46]

Statistics produced on the May 23rd, 2012[47], show mobile phone subscriptions increased to 1.030 billion, with 158.97 million using 3G.

QUICK FACTS CHINA

Land Area: 9,327,480 sq km
Population: 1.338 billion (2010)
Urban Population: 43% of total population
GNI per capita, PPP: $7,640 (WB, 2010)

TLD: .cn
Fixed Telephones: 283.7 million (2012)
GSM Telephones: 1.030 billion (2012)
Fixed Broadband: 159.3 million (2012)
Internet Users: 389 million (2009

45 www.worldbank.org

46 www.google.com/hostednews/afp/article/ALeqM5jhpFZrHwD9qqSZ2pfh9WxJuDwE8A?docId=CNG.df05140bd848fd4930151160f19892b6.501

47 http://www.miit.gov.cn/n11293472/n11293832/n11294132/n12858447/14621263.html

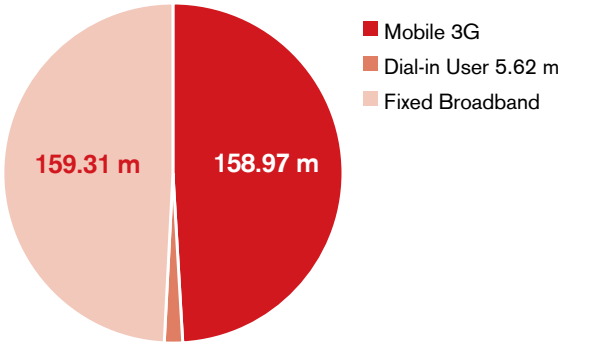
Pricing Analysis ($US)	China	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost	-		-
Cost per Minute National Call (First 3 Min)	0.04	2	0.07
Price for Data Traffic (Price per MB)	0.08	9	0.05
Price for One Text Message	0.02	2	0.02
POST-PAID Package Pricing			
Monthly Package Cost	7.60	6	7.53
Cost per Minute National Call (First 3 Min)	0.03	2	0.06
Price for Data Traffic (Price per MB)	0.08	7	0.04
Price for One Text Message	0.02	3	0.03

Operator	China Mobile	China Unicom	China Telecom
Brands	CMCC		
Survey Respondents	53%	39%	
Subscribers	672.5 m	212.7 m	138.5 m
Mobile Internet Users	300.0 m (61.9m 3G)	100.0 m (51.8m 3G)	50.0 m (45.6m 3G)
Ownership	State	State	State

INTERNET ACCESS

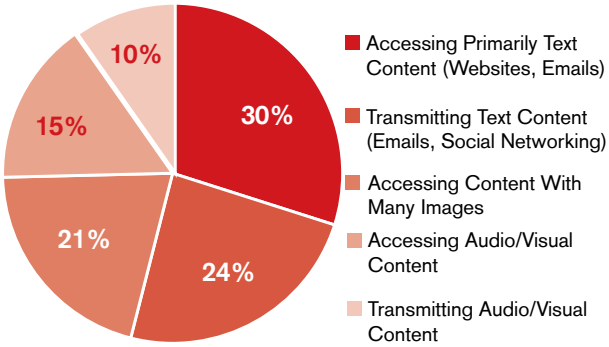
Over 93% of respondents used mobile internet and less than 6% do not use mobile internet. 79% of these mobile internet users pay for a limited bundle, almost 20% use WiFi and less than 0.5% have no access. Almost 96% owned a smartphone and almost 36% had "jailbroken" their phone but over 62% had updated the firmware on their phone.

INTERNET CONNECTION TYPES AS OF 23 MAY 2012 (MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY)



ROLE OF MOBILE DEVICES

USE OF THE INTERNET 2012 (IN COUNTRY SURVEY)



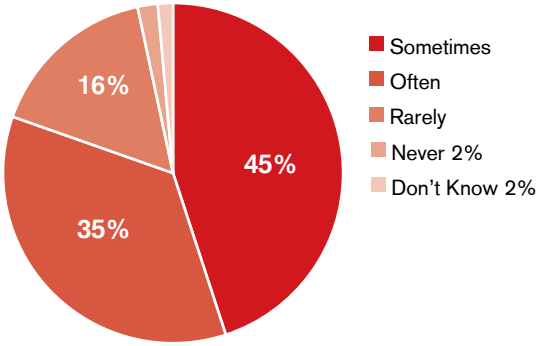
CENSORSHIP AND CIRCUMVENTION

China operates the largest internet monitoring and censorship system in the world. Many documents have been written, and extensive research conducted, on the best methods of circumventing the blocking system in operation.

On June 4th, 2012, the UK's Guardian newspaper reported that China's censors blocked internet access to search terms "six four," "23," "candle," and "never forget," therefore broadening already extensive efforts to silence talk about the 23rd anniversary of the June 4th

crackdown on pro-democracy protesters in Tiananmen Square. These terms have also been blocked on Sina Weibo, the most popular of China's Twitter-like microblogging platforms.

HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN-COUNTRY SURVEY)



On May 31st, 2012, Alan Eustace, Senior Vice President for Knowledge at Google wrote on his blog[48] about a new service Google will provide to users suffering from internet blocking. Google "has had a lot of feedback that Google Search from mainland China can be inconsistent and unreliable. It depends on the search query and browser, but users are regularly getting error messages like 'This webpage is not available' or 'The connection was reset.' And when that happens, people typically cannot use Google again for a minute or more." These interruptions are closely correlated with searches for a particular subset of queries. Google will now notify users in mainland China when they enter a keyword that may cause connection issues. By prompting users to revise their queries, Google hopes to reduce the disruptions and improve user experience – particularly from mainland China. It has been suggested that users can then edit their query using pinyin, the system used to transliterate Chinese characters into Latin script.

48 http://insidesearch.blogspot.ie/2012/05/better-search-in-mainland-china.html

CONCLUSION

The Chinese mobile market is huge and continues to grow. Mobile subscriptions are still at less than 75%, so there is a lot of room for growth. This market is also one of the least competitive considering the size of the market; it is also the most tightly regulated and controlled. Internet censorship is major state activity.

FURTHER INFORMATION

Ministry of Industry and Information Technology – www.miit.gov.cn
China Internet Network Information Center – www.cnnic.net.cn/en/
China Mobile - www.chinamobileltd.com
China Unicom - chinaunicom.com.hk
China Telecom - chinatelecom-h.com

Arab Republic of Egypt

There was very little data received from the in-country user survey, and most of the data has been collected from the in-country expert. This is due to the complex political situation in the country, with the new Egyptian President inaugurated in late June 2012.

TELECOMMUNICATIONS MARKET

There has been no recent change in the number of operators, although 3G is increasingly utilized via pre-paid and post-paid contracts. Apps are increasingly used on mobile phones to access the internet and communicate via data connections, rather than standard SMS/voice connections. Egypt mandated a change in all Egyptian mobile phone numbers to increase the number of digits from 10 to 11 digits by end of March 2012. Some citizens are concerned that the mobile phone number change is also intended to create a more accurate database of user identities.

Indicator[50]	measurement	Value
Computers in Households	Per 100	44.3
Internet Users	Per 100	35.7
Fixed Lines	Per 100	10.9
Fixed Broadband	Per 100	2.3
Mobile Subscriptions	Per 100	119
Mobile Broadband	Per 100	13.2
International Bandwidth	Per 100	229 kb

In 2012, the Egyptian Mobile market penetration has reached 119% (calculated based on figures from the Central Agency for Public Mobilization and Statistics "CAPMAS," and the operators' official published releases) as a result of the multi-SIM phenomenon. The growth potential lies in the penetration of rural areas and new demographic segments, in the growth of higher-value contract customers, and in the wider availability of mobile broadband services.
Mobile broadband/3G connections are becoming increasingly desired, and there is increased usage of mobile phones to connect to the internet at WiFi-enabled cafes, with a corresponding increasing number of cafes which offer WiFi access to customers.
There is also an increasing desire for wider choice in smartphone handsets, not only iPhone and BlackBerry, but Android OS-based hardware. Mobile phone usage grew approximately 22% in 2011 There is increasing evidence that iPads may outgrow iPhones as a tool for mobile browsing/mobile internet across Middle-East. Egypt was 4th in 2011 in a study of the volume of geo-located tweets on the African continent[50] in Q4 2011.

QUICK FACTS EGYPT

Land Area:	1,009,450 sq km
Population:	81.1 million (2010)
GNI per capita, PPP	$6.060 (WB, 2010)
TLD:	**.eg**
Fixed Telephones:	9.3 million (2010)
GSM Telephones:	83.4 million (2011)
Fixed Broadband:	4.3 million (2011)
Internet Users:	25.9 million (2011)

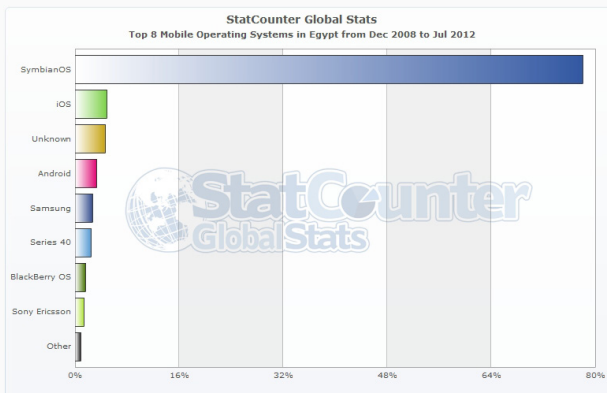
49 www.worldbank.org and www.capmas.gov.eg and www.mcit.gov.eg

50 www.portland-communications.com/Twitter_in_Africa_PPT.pdf

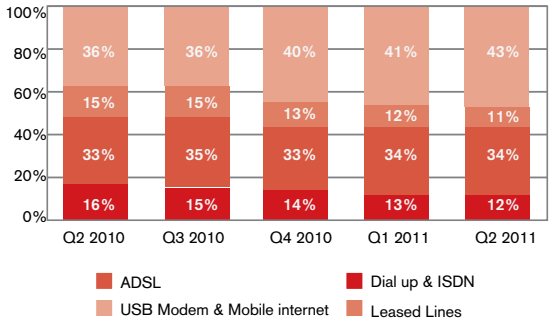
Pricing Analysis ($US)	Egypt	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute National Call (first 3 min)	0.06	4	0.09
Price for Data Traffic (Price per MB)	0.03	3	0.05
Price for One Text Message	0.06	9	0.02
POST-PAID Package Pricing			
Monthly Package Cost	35.78	9	7.53
Cost per Minute National Call (First 3 Min)	0.03	3	0.06
Price for Data Traffic (Price per MB)	0.03	4	0.04
Price for One Text Message	0.05	8	0.03

Operator	Etisalat Misr	Mobinil	Vodafone
Brands			Vodafone Egypt Click GSM Sarmady
Survey Respondents	n/a	n/a	n/a
Subscribers	12.4m	30.3m	34.2m
Mobile Internet Users	n/a	n/a	n/a
Ownership	National	France Orange	Vodafone Group

INTERNET ACCESS
MOBILE OS USAGE AS SEEN BY STATCOUNTER

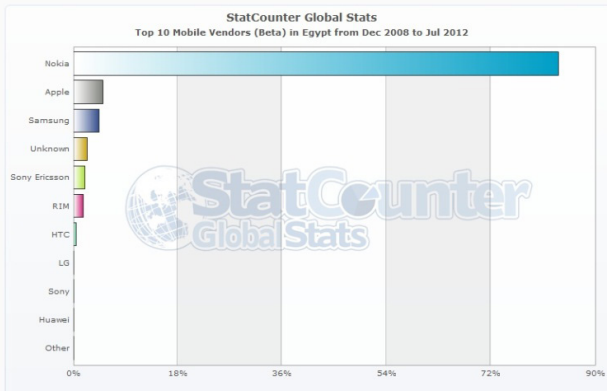


INTERNET CONNECTION TYPES
Q2 2010 TO Q2 2011



Sources: Ministry of Communications and information Technology, National Telecom Regulatory Authority

HANDSET MANUFACTURER AS SEEN BY STATSCOUNTER



CENSORSHIP AND CIRCUMVENTION

There is increasing state concern about on-going protests.

Citizens are concerned that the renumbering of Egyptian mobiles is part of a program to establish a more accurate database for monitoring user habits connected to a more accurate identity.

In 2011, the state clearly demonstrated its willingness to completely cut the internet in Egypt off from the outside world. The state blocks primarily on "moral" grounds, i.e., pornography sites, but citizens are increasingly concerned that Egypt may look to broader blocking authority due to ongoing unrest.

PHONE BRANDS[51]

Phone	iPhone 4S	BlackBerry Bold 9780	BlackBerry Curve 9360	BlackBerry Torch 9800
Manufacturer	Apple	RIM	RIM	RIM
Released	October 2011	November 2010	August 2011	August 2010
				
Data	GPRS/EDGE C10	GPRS/EDGE	GPRS/EDGE	GPRS/EDGE C10
Bluetooth	V4.0 with A2DP	V2.1 with A2DP	v2.1 with A2DP	v2.0 with A2DP
Sensors	Accelerometer, Gyro, Proximity, Compass			Proximity
Internet	Yes	Yes	Yes	Yes
OS	IOS 5.1	BlackBerry OS 6.0	BlackBerry OS 7.0	BlackBerry OS 6.0
GPS	GPS-A and Glonass	GPS-A	GPS-A	GPS-A
Camera	8MP (gps)	5 MP	5 MP	5 MP
WiFi	b/g/n/hotspot	b/g/UMA	b/g/n/UMA	b/g/n/UMA

51 Data and images from www.gsmarena.com

CONCLUSION

Mobile penetration is over 100%, and there is good competition in the market.

FURTHER INFORMATION

Central Agency for Public Mobilization and Statistics (CAPMAS) www.capmas.gov.eg
Ministry of Communications and Information Technology - www.mcit.gov.eg
National Telecommunications Regulatory Authority (NTRA) - www.tra.gov.eg/english
Eqypt ICT indicators - www.egyptictindicators.gov.eg/en
Internet Egypt - www.interneteqypt.com

Etisalat – www.etisalat.com.eg
Mobinil – www.mobinil.com
Vodafone Eqypt – www.vodafone.com.eg

Islamic Republic of Iran

The Islamic Republic of Iran has one of the smaller mobile penetration markets in the region at 72.3% with only the Syrian Arabic Republic at 57.7% being smaller. However, there are still over 54 million mobile subscribers in the country. Fixed broadband has amazingly low penetration with only 0.7% of the population and an absolute volume of 1.7 million.

TELECOMMUNICATIONS MARKET

In February 2004, Ministry of Communications and Information Technology (MCIT) announced that the Irancell consortium was the winner of the tender for the second mobile operator. Irancell network was officially launched on October 21st, 2006 in Tehran, Tabriz, and Mashhad. Since launching, Irancell has sold about 60m sim-cards.

Indicator[52]	Measurement	Value
Computers in Households	Per 100	n/a
Internet Users	Per 100	37.2
Fixed Lines	Per 100	36.3
Fixed Broadband	Per 100	0.7
Mobile Subscriptions	Per 100	72.3
Mobile Broadband	Per 100	n/a
International Bandwidth	Per 100	n/a

In November 2011, the FARS news agency reported[53] that the Iranian government awarded a third license to Tamin Telecom in October 2009. However, the operator did not start service until late 2011. This operator announced plans to cover 60 % of the population with its 2G network and 40 % with its 3G network by 2014. Rightel only started its activities in late 2011 because of international sanctions, and it is the first operator in Iran to provide 3G technology. Rightel started its pre-sell of 3G SIM-cards from February 8th, 2012, in Tehran.

52 www.worldbank.org & http://en.cra.ir/portal/File/ShowFile.aspx?ID=ae0bc516-e389-48a5-9c51-094d667c3f86

53 http://english.farsnews.com/newstext.php?nn=9007274839 (accessed 11 June 2012)

QUICK FACTS IRAN

Land Area:	1,628,550 sq km
Population:	74.0 million (2010)
GNI per capita, PPP	$11,490 (WB, 2009)
TLD:	.ir
Fixed Telephones:	26.4 million (2011)
GSM Telephones:	54.2 million (2011)
Fixed Broadband:	1.7 million (2011)
Internet Users:	27.5 million (2010)

A fourth operator (based on 4G) will start its activities as soon (Hamrah Aval (First and the biggest operator in Iran) decided to buy Spadan and Talyia Operators's stocks - According to some gossips and a SMS from Irancell in some days ago, it has sold about 68 million SIM-cards

IRNA (Islamic Republic News Agency) says 61.7% of Iranians use mobiles and 37% have access to internet Fars News Agency has reported that only 9% of Iranian's use mobile internet, whereas there are more than 100 million SMS sent per day.

ZTE Corp, China's second-largest telecommunications equipment maker, stated that it will "curtail" its business in Iran following a report indicating that it had sold Iran's largest telecom firm a powerful surveillance system capable of monitoring telephone and internet

communications. Reuters reported March 2012[54] that Shenzhen-based ZTE had signed a €98.6 million contract with the Telecommunication Co of Iran in December 2010 that included the surveillance system. ZTE is publicly traded, but its largest shareholder is a Chinese state-owned enterprise. It says it sells equipment in more than 140 countries and reported annual revenue of $10.6 billion in 2010. In May 2012, Reuters further reported that Department of Commerce started investigating Chinese telecommunications equipment maker ZTE Corp for allegedly selling embargoed U.S. computer products to Iran.

Operator	Mobile Communication Company of Iran (MCI)	Irancell Telecommunication Services	Tamin Shams Novin Telecommunication Co.	Taliya	Isfahan Mobile Share	Kish Mobile
Brands						
Survey Respondents						
Subscribers	34.6m	20.18m	n/a	0.2m	0.03m	0.02
Mobile Internet Users	9.5m	n/a	n/a	n/a	n/a	n/a
Ownership	Iran	51% Iran/49% MTN South Africa		Iran	Malaysia/Iran	

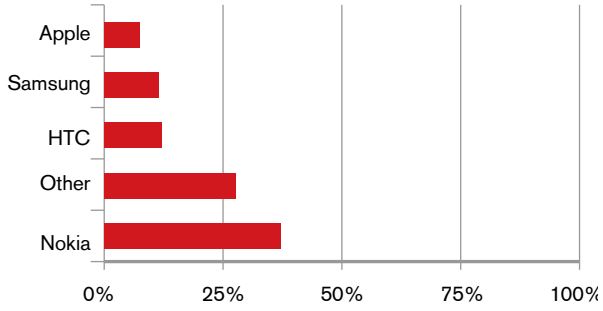
Pricing Analysis ($US)	**Iran**	**All Countries Surveyed**	
		Rank by Cheapest	**Median Price**
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute National Call (First 3 Min)	0.07	5	0.09
Price for Data Traffic (Price per MB)	0.29	11	0.05
Price for One Text Message	0.01	1	0.02
POST-PAID Package Pricing			
Monthly Package Cost		1	7.53
Cost per Minute National Call (first 3 min)	0.05	5	0.06
Price for Data Traffic (Price per MB)	0.45	10	0.04
Price for One Text Message	0.01	2	0.03

54 http://www.reuters.com/article/2012/03/23/iran-telecoms-zte-idUSL3E8EN53W20120323 (accessed 11 June 2012)

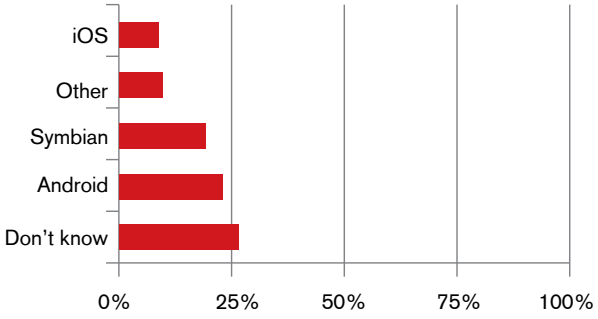
INTERNET ACCESS

Over 55% of respondents used mobile internet and over 39% do not use mobile internet. 33% of these mobile internet users used WiFi to access the internet with 27% paying for a limited volume of data with their subscription and a further 18% paying for usage. Almost 19% indicated they had no access to the internet using their mobile handsets. Almost 42% owned a smartphone and only 6% had "jailbroken" their phone but over 30% had updated the firmware on their phone.

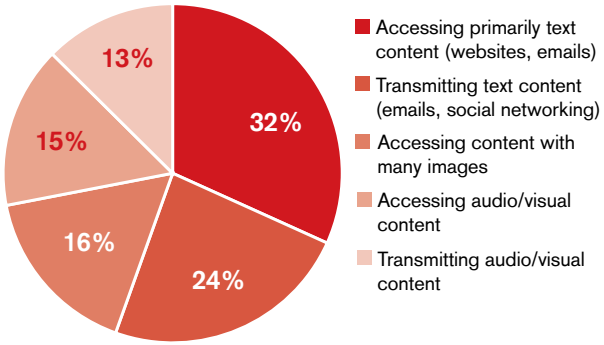
TOP 5 HANDSET MANUFACTURER



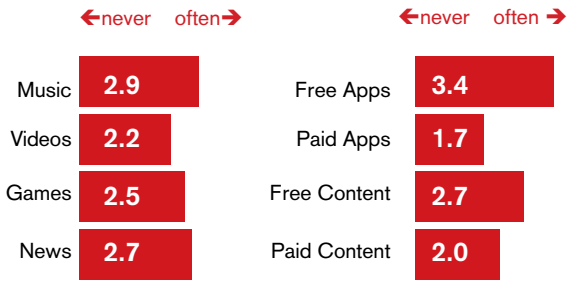
TOP 5 MOBILE OPERATING SYSTEM IN USE



USE OF THE INTERNET 2012 (IN COUNTRY SURVEY)



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)

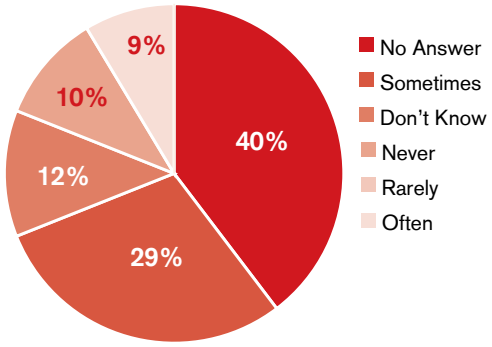


CENSORSHIP AND CIRCUMVENTION

At a news conference[55] on December 28, 2011–the day for registering candidates for the March 2012 parliamentary elections–Abdosamad Khoramabadi, the Prosecutor-General's legal adviser, unveiled "a list of 25 election-related internet crimes." Among the contents deemed "criminal" were calling for an election boycott and the publication of counter-revolutionary or opposition logos or website contents.

55 http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf Pg25 (last accessed 11 June 2012)

HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN COUNTRY SURVEY)



Under the new 20-point regulations for cybercafés, published by the Iranian internet Police on December 28, 2011, clients are required to produce an ID. Managers must install cameras on the premises and keep the camera recordings, along with all the details of their clients and a list of the websites they visited. The use of software to circumvent content filtering, Virtual Private Networks (VPNs), and USB flash drives is banned. After raiding 43 cybercafés in Birjand (in the southern province of Khorasan), the police closed six of them for "non-compliance with security measures and the use of censorship circumvention software."

Reza Rahimi (Iranian Parliament member) stated that Irancell's SIM-Cards were the main cause of post-election protests, because those active without submitting any form of ID. Protesters used them to inform others about the time and location of strike & protest. - Mostafa Tabatabaei Nejad (Iranian Parliament member) said: "Operators must use a system for tracing who called 'Prank Calls.' "He went on to say that this usually occurred among Irancell's subscribers. Taghipour (the Iranian minister of communication) said that all Iranian data centers should transfer their servers from overseas to Iran.

According to this law, the Committee in Charge of Determining Unauthorized Websites is legally empowered to identify sites that carry forbidden content and report that information to TCI and other major ISPs for blocking[56]. The committee is headed by the prosecutor general and operates under the supervision of that office.

56 http://www.freedomhouse.org/sites/default/files/inline_images/Iran_FOTN2011.pdf pg 4(last accessed 11June 2012)

SAMPLE PHONE BRANDS IN USE[57]

Phone	C7	701	Xperia ray	Sensation	Xperia Arc
Manu	Nokia	Nokia	Sony Ericsson	HTC	Sony Ericsson
Released	October 2010	September 2011	August 2011	May 2011	March 2011
					
Data	GPRS/EDGE C32	GPRS/EDGE C33	GPRS/EDGE	GPRS/EDGE	GPRS/EDGE
Bluetooth	V3.0 with A2DP	V3.0 with A2DP	V2.1 with A2DP	V3.0 with A2DP	v2.1 with A2DP
Features	Accelerometer, Proximity, Compass	Accelerometer, Proximity, Compass	Accelerometer, Proximity, Compass	Accelerometer, Gyro, Proximity, Compass	Accelerometer, Proximity, Compass
Internet	Yes	Yes	Yes	Yes	Yes
OS	Symbian 3 OS upg to Nokia Belle OS	Symbian Belle upg Belle FP1	Android OS 2.3 – upg to v4.0	Android v2.3.4 upg to v4.x	Android 2.3 upg v4.0
GPS	GPS-A	GPS-A	GPS-A	GPS-A	GPS-A
Camera	8MP (gps)	8MP (gps)	8 MP	8 MP	8 MP
WiFi	b/g/n	b/g/n	b/g/n/DLNA/hotspot	b/g/n/DLNA/hotspot	b/g/n/DLNA/hotspot

CONCLUSION

Regulation of the Iranian mobile market is very sophisticated and there is significant state ownership of the mobile operators, with external involvement from organizations in South Africa and Malaysia. Market penetration has not kept pace with other countries in the region but there is still a relatively large number of subscribers.

FURTHER INFORMATION

Islamic Republic News Agency (irna) - www.irna.ir
Statistical Center of Iran 2006 - amar.sci.org.ir/index_e.aspx
Ministry of Information and Communication Technology (MICT) - No accessible website
Communications Regulatory Authority (CRA) www.cra.ir
Iranian Research and Academic Network – www.iranet.ir
IRAN-GRID Certificate Authority – cagrid.ipm.ac.ir

Iran Telecommunication Company – www.mci.ir
Irancell Telecommunication Services – www.irancell.ir
Tamin Shams Novin Telecommunication Co. - www.rightel.ir
Taliya - www.taliya.ir
Isfahan Mobile Share – www.mtce.ir
Kish Mobile - www.tkckish.ir

57 Data and images from www.gsmarena.com

Libya

Due to ongoing political turmoil it was difficult to solicit cooperation on the ground in Libya for the research in this project. A number of contacts, when requested to complete the expert survey and to implement the user survey, declined to participate. The following information is, therefore, based on desk research.[58]

TELECOMMUNICATIONS MARKET

Indicator[57]	measurement	Value
Computers	Per 100	n/a
Internet Users	Per 100	14.0
Fixed Lines	Per 100	19.3
Internet Broadband	Per 100	1.2
Mobile Subscriptions	Per 100	171.5
Mobile Broadband	Per 100	n/a
International Bandwidth	Per 100	n/a

It is widely believed that Libiya's telecommunications infrastructure suffered significant damages during the recent ousting of the Gadhafi regime. It does, however, have a history of having one of the most advanced mobile network infrastructures in the whole of Africa, and one of the highest broadband penetration rates on the continent. Due to the lack of data, one can only make assumptions about the current state of the infrastructure.

Two networks were present under the Gadhafi regime: since Al-Madar and Libyana. The latter is believed to be the major catalyst towards bringing Libya a very high mobile penetration rate[59]. The Gadhafi regime had also invested heavily in other African countries' mobile networks. To facilitate eavesdropping and maximum control most international links were routed through Tripoli, the nation's capital, and the seat of the regime and it's security services.

58 http://www.worldbank.com

59 http://www.businesswire.com/news/home/20120531006052/en/Research-Markets-Libya---Telecoms-Mobile-Broadband

LIBYA

During the course of the recent civil war the Ghadafi regime severed most interconnecting to phone networks in the country and cut off international access for networks serving the east and the rebel held town of Benghazi. Mobile service by Libyana remained in the air, there, however, and restoration efforts appear to be underway. Backed, in large part, by U.A.E and Qatar based firms, presumably hoping to make their way into the newly formed Libyan market, Libyana restored service in the east and went on to provide free service, for the duration of the conflict[60]. Due to the lack of the original HLR, the communication on this free network could not be encrypted.[61]

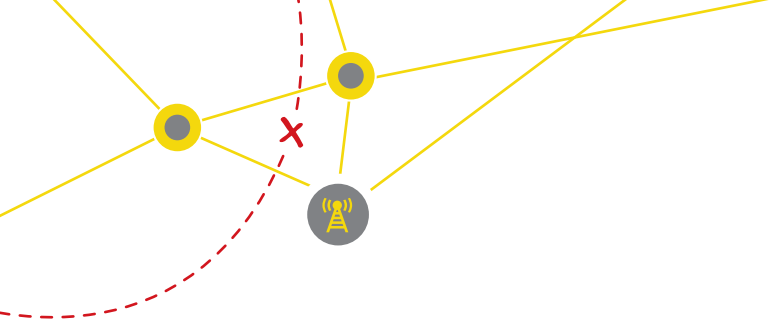
Both operators' websites remained inaccessible throughout the writing of his report.

INTERNET ACCESS

Internet access in Libya was also severed during the

60 "How 'rebel' phone network evaded shutdown " Al Jazeera: http://www.aljazeera.com/indepth/features/2011/04/20114233530919767.html (last accessed July 7 2012)
Wall street journal: http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html
Qataris looking to buy into Libyana mobile network, Libya Herald: http://www.libyaherald.com/qataris-looking-to-buy-into-libyana-mobile-network/ (Last accessed July 7 2012)

61 The Register, Free Libyana: networkjacker speaks: http://www.theregister.co.uk/2011/04/14/free_libyana/page2.html (Last accessed July 7 2012)



2011 uprising. A report by Akamai, monitoring internet access from Libya, noted Libya as the country with the slowest internet speeds in the world.[62]

LTT, the country's only internet provider, has clearly not succeeded in bringing service levels back to what they were before the conflict. Recent rumors of a new, privately owned ISP could not be confirmed during the writing of this report.

Recent data or intelligence on mobile internet access was unavailable.

In terms of Mobile traffic emanating from Libya, 75% appears to originate from a Nokia (Symbian or Series 40) devices, according to statcounter statistics.

CENSORSHIP AND CIRCUMVENTION

The ousting of the Gadhafi regime brought to light a number of western firms that supplied advanced monitoring and blocking infrastructure to the Libyan regime. Libya was known to block Skype, censor YouTube, and blocked circumvention tools and proxies that would allow its citizens unfettered internet access.[63]

In more recent news Libya's interim government is said to be using the same equipment from the Gadhafi era to monitor calls and internet traffic of Gadhafi supporters.

CONCLUSION

Libya could not be adequately surveyed for this report. Ample anecdotal evidence suggests its telecommunications market is slowly getting back to its feet, although worries remain, especially around the use of Gadhafi-era monitoring equipment.

62 Kifah Libya, "Beyond LTT" http://www.kifahlibya.com/2012/05/20/tech-beyond-ltt-the-state-of-libyas-internet/

63 Wall street journal, Firms aided Libyan spies, http://online.wsj.co/article/SB10001424053111904199404576538721260166388.html (Last accessed july 7 2012)

Sultanate of Oman

Mobile penetration has almost reached 180% of the population and continues to grow. In comparison, there are 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 will be over mobile networks.

TELECOMMUNICATIONS MARKET

The total penetration of mobile phone users in Oman is about 173% (there are more mobile phone subscriptions than the total population). The total number of mobile services subscribers in Oman is 4,809,248. – The market is dominated by two main operators (Omantel and Nawras) who own 90% of the market with almost equal shares. There are a number of reseller operators (or MVNOs) that offer only prepaid services and collectively own a 10% share of the market. The market share of these MVNO has slowly increased incrementally through the year 2011. These resellers are Friendi, Renna, Apna/Hala, and Samatel.

Indicator[63]	measurement	Value
Computers	Per 100	n/a
Internet Users	Per 100	62.0
Fixed Lines	Per 100	10.6
Internet Broadband	Per 100	3.5
Mobile Subscriptions	Per 100	177.6
Mobile Broadband	Per 100	44.2
International Bandwidth	Per 100	834 kb

There is a good competition between Omantel and Nawras (who both also provide fixed internet services) in providing greater options for mobile data packages for both post-paid and pre-paid subscribers. It is becoming more common for people to have data plans on their phones, especially after Omantel introduced a bundle package that includes unlimited SMS and phone calls in addition to a number of GBs of data along with it. The reduction in the cost of the lowest available mobile data plan has also helped in spreading the subscription of such services.

QUICK FACTS – SULTANATE OF OMAN

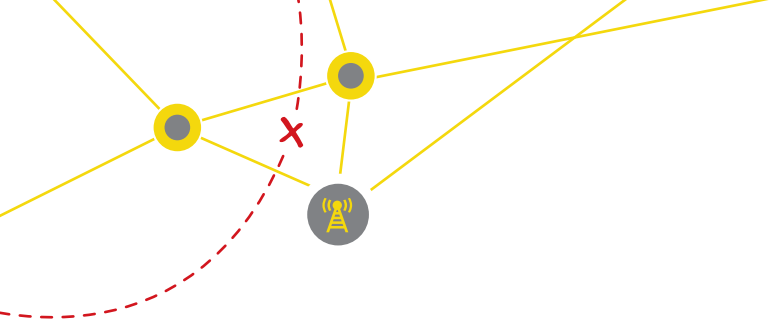
Land Area:	309,500 sq km
Population:	2.7 million
GDI per capita, PPP	$25,190 (WB, 2009)
TLD:	**.om**
Fixed Telephones:	0.3 million (2012)
GSM Telephones:	4.9 million (2012)
Fixed Broadband:	0.088 million (2012)
Internet Hosts:	9,114 (2010)
Internet Users:	2.5 million (2012)

The total number of active mobile broadband subscribers[65] in Oman is 1,226,442, which is approximately 25% of all mobile phone subscribers in the country. Samsung smartphones are becoming increasingly popular, as is the iPhone, which in February 2012 was still not being sold officially by any service provider in Oman, but was freely available as an import. Most recent official reports state that the total number of SMS messages sent in Q4 of 2011 was 1,448 billion, and that number continues to grow. The total number of MMS sent in Q4 of 2011 was 7.77 billion, and that MMS usage is decreasing. Internet-based messaging services such as WhatsApp are becoming increasingly popular.

In 2010, Nawras launched VoIP service in conjunction

64 http://www.tra.gov.om/newsite1/sectorIndicatorsQ12012.aspx?Lang=1

65 As per ITU definition



with the Nawras fixed service products for both business and residential consumers. The fixed VoIP service provides the opportunity for Nawras' customers to make low cost, lower quality international calls using Nawras' fixed products via the prefix 0902. In June 2010, the Telecommunications Regulatory Authority (TRA)[66] issued new labelling guidelines aimed at combating the flood of unauthorized mobile phone handsets and other types of telecom equipment entering the Omani consumer market,

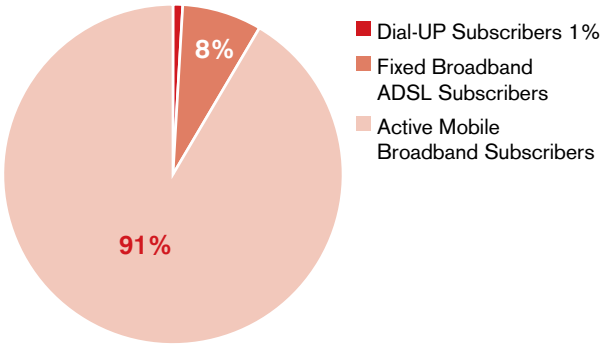
Pricing Analysis ($US)	Oman	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost	28.15		
Cost per Minute National Call (first 3 min)	0.27	9	0.09
Price for Data Traffic (Price per MB)	0.05	6	0.05
Price for One Text Message	0.02	4	0.02
POST-PAID Package Pricing			
Monthly Package Cost	79.22	10	7.53
Cost per Minute National Call (First 3 Min)	0.26	9	0.06
Price for Data Traffic (Price per MB)	0.01	2	0.04
Price for One Text Message	0.03	5	0.03

Operator	Omantel	Nawras	FRiENDiMobile	Majan TeleCommunication	International Telecommunications	Sama Communications
Brands	Oman Mobile Omantel	Nawras		Renna	Apna Moible Hala	Samatel
Survey Respondents	40%	33%				
Subscribers	2.28m	1.93m	0.15m	0.15m	0.15m	0.15m
Mobile Internet Users	1.76m	1.49m	0.12m	0.12m	0.12m	0.12m
Ownership	Oman	Qatar/Oman	Mixed	Oman	Oman-UAE	Oman

66 http://www.tra.gov.om/newsite1/NewsDetails.aspx?newsid=208

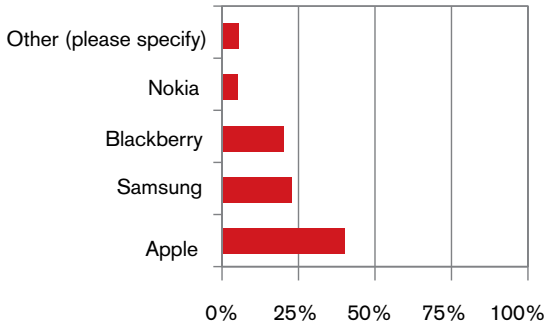
INTERNET ACCESS

INTERNET CONNECTION TYPES, 2010

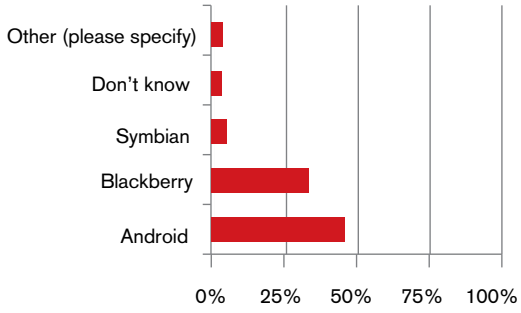


91% of respondents used mobile internet. Of these, 40% used WiFi to access the internet, with 48% paying for a limited volume of data with their subscription, and a further 9% paying for usage.

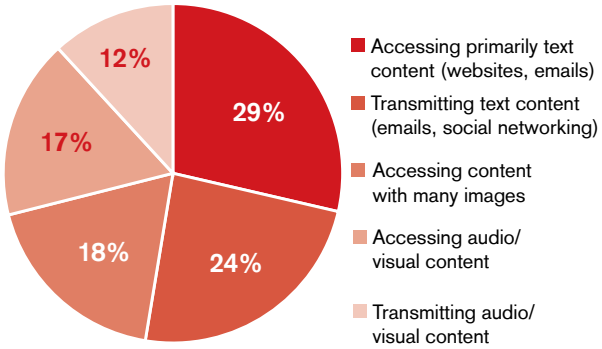
TOP 5 MOBILE HANDSET MANUFACTURERS



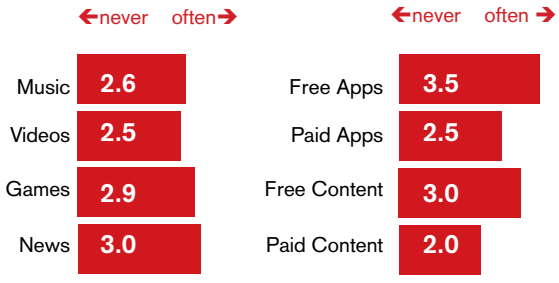
TOP 5 MOBILE OS IN USE



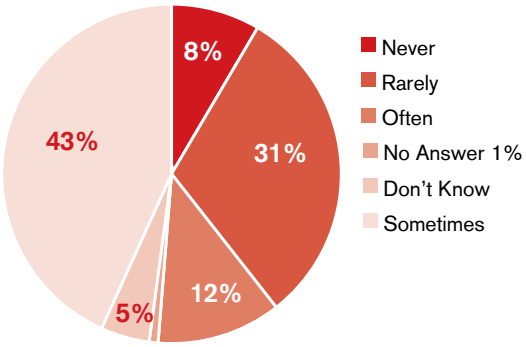
USE OF THE INTERNET 2012



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)

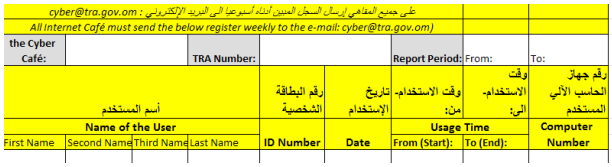


HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN COUNTRY SURVEY)



CENSORSHIP AND CIRCUMVENTION

The biggest legislative issue in Oman in relation to communication is the ban of VoIP services, which are not licensed by the Telecommunication Regulation Authority in Oman. Services such as Skype are blocked and cannot be used by subscribers in Oman without relying on circumvention tools. It is believed that the primary reason for this is the government's concern that VoIP services will affect the profits of Omantel (the oldest telecommunication company in the country, in which the government is the majority shareholder).



cyber@tra.gov.om : على جميع المقاهي إرسال السجل المبين أدناه أسبوعيا الى البريد الإلكتروني							
All Internet Café must send the below register weekly to the e-mail: cyber@tra.gov.om)							
the Cyber Café:		TRA Number:			Report Period:	From:	To:
أسم المستخدم				رقم البطاقة الشخصية	تاريخ الإستخدام	وقت الاستخدام- من:	وقت الاستخدام- الى:	رقم جهاز الحاسب الآلي المستخدم
Name of the User						Usage Time		Computer
First Name	Second Name	Third Name	Last Name	ID Number	Date	From (Start):	To (End):	Number

Freedom House reports[67] that libel is treated as a criminal offense and journalists can be fined or imprisoned for up to two years for voicing criticisms of the sultan, or for printing material that leads to "public discord, violates the security of the state, or abuses a person's dignity or rights."

Recent amendments to the publication law and the criminal law that affect freedom of expression have been passed and have a direct implication on what kind of communications people have over mobile internet. It is not usual, by the government and by private individuals, to take legal action against people who post defamatory material on the internet.

Freedom House reports that the state Internet Service Manual stipulates a lengthy list of prohibited content, including defamation of the ruling family and false data or rumours. The government routinely blocks websites deemed sexually offensive or politically controversial. Private communications such as mobile telephone calls, e-mail, and exchanges in internet chat rooms are monitored.

In October 2010, the Telecommunications Regulatory Authority (TRA) identified 15 shops which were found to be in breach of the Telecommunications Regulatory Act, of which five were illegally offering VoIP without being licensed to provide this service. Those offenders were directly referred to public prosecution. The other ten shops seized were internet cafés that were in breach of TRA Resolution No. 166/2007 for the reselling of internet service without obtaining a Certificate of Registration from TRA. Resolution No 11/2011[68] regarding cyber cafés requires cafés to ensure the registration of personal details of users and visitors (see picture) and send these details to TRA email address cyber@tra.gov.om.

67 http://www.freedomhouse.org/report/freedom-press/2011/oman

68 http://www.tra .gov.om/newsite1/Portal/Upload/Documents/467_11-2011Ar.pdf

PHONE BRANDS[69]

Phone	S5570 Galaxy Mini	I9000 Galaxy S	iPhone 4	Bold 9780	Curve 8520
Manu	Samsung	Samsung	Apple	RIM	RIM
Released	February 2011	June 2010	June 2010	November 2010	August 2009
					
Data	GPRS/EDGE C12	GPRS/EDGE C12	GPRS/EDGE C10	GPRS/EDGE	GPRS/EDGE C10
Bluetooth	V2.1 vA2DP	v3.0 with A2DP	v2.1 with A2DP	V2.1 with A2DP	v2.0 with A2DP
Sensors	Accelerometer, Proximity, Compass	Accelerometer, Proximity, Compass	Accelerometer, Gyro, Proximity, Compass		
Internet	Yes	Yes	Yes	Yes	Yes
OS	Android 2.3	Android 2.3	IOS 5.1	BlackBerry OS 6.0	BlackBerry OS 5.0
GPS	GPS-A	GPS-A	GPS-A	GPS-A	No
Camera	3.15 MP (gps)	5 MP(gps)	5MP (gps)	5 MP	2 MP
WiFi	b/g/n	b/g/n/dlna/hotspot	b/g/n	b/g	b/g

CONCLUSION

The Sultanate of Oman is a very vibrant mobile market with over 177% penetration on mobile usage. There is active regulation and enforcement of the market regulations, and high levels of supervision of mobile and internet operators. Almost 92% owned a smartphone and there is widespread use of the latest smartphone handsets, and almost 82% of the respondents indicated they had intermediate level skills with mobile technologies.

FURTHER INFORMATION

Telecommunications Regulatory Authority (TRA) - http://www.tra.gov.om
Sultanate of Oman - Ministry of National Economy - http://www.moneoman.gov.om
Ministry of Transport & Communication - http://www.motc.gov.om

Omantel - www.omantel.om
Nawras - www.navras.om
FRiENDiMobile – www.friendimobile.om
Majan TeleCommunication - www.rennamobile.com
International Telecommunications - www.apnamobile.om
Sama Communications - www.samatel.om
The ITU's Arab Regional Office - www.ituarabic.org
The ITU's Arab Centre of Excellence - www.ituarabic.org/ceo

69 Data and images from www.gsmarena.com

Kingdom of Saudi Arabia

Saudi Arabia is impressive at almost 200% mobile penetration, and even more interesting due to the low penetration of fixed broadband (5.5%)

TELECOMMUNICATIONS MARKET

The mobile market in KSA was originally dominated by a government-owned company called STC. The market has been liberated over the years as additional licenses were given to two additional operators, called Mobily and Zain. STC now owns about 43.2% of the market share, while Mobily owns 40%, and Zain owns 16.4%. There have not been any new entrants to the mobile market except recently for a Push-To-Talk operator called Bravo that focuses on businesses.

Indicator[68]	Measurement	Value
Computers	Per 100	n/a
Internet Users	Per 100	46.0
Fixed Lines	Per 100	15.9
Fixed Broadband	Per 100	5.5
Mobile Subscriptions	Per 100	198.0
Mobile Broadband	Per 100	40.5
International Bandwidth	TOTAL	950MB

Key reasons for this growth are increased competition and the mass market availability of smart phones, which enable customers to access a variety of data packages. At the same time, mobile networks are also being upgraded as 3.5G (HSPA) continues to be widely deployed and more advanced wireless broadband technologies (4G) emerge. Data-only SIM cards have reached up to 7.8 million of the total number of mobile broadband subscriptions.

On January 7th, 2010, Saudi Arabia operator Mobily announced[71] it had one million mobile broadband subscribers. Registering 264 % growth, Mobily closed

70 http://www.worldbank.org & http://www.citc.gov.sa/English/MediaCenter/CITCinthemedia/Pages/PR_MED_094.aspx

71 http://www.itu.int/ITU-D/ict/newslog/Mobily+Announces+1+Mln+Mobile+Broadband+Subscribers+Saudi+Arabia.aspx

QUICK FACTS SAUDI ARABIA

Quick Facts	Saudi Arabia
Land Area:	2,149,690 sq km
Population:	27.5 million
GDI per capita: (ppp)	$22,750 (2009)
TLD:	**.sa**
Fixed Telephones:	4.5 million (2010)
GSM Telephones:	56.1 million (2011)
Fixed Broadband:	2.2 million (2012)
Internet Users:	13.0 million (2011)

2008 with 266,000 mobile broadband subscribers in its three high-volume bundles, prompting the GSM World Association to describe Mobily as having the busiest mobile date network on the face of the planet. Monthly traffic, upload and downloaded by customers, has grown more than 10 times from December 2007 to the time this report was written, and stood at over 50 TB for December 2009.

In June 2009 Mobily reported an active mobile broadband subscriber base of 600,000 customers. Three months later, when Mobily released its third quarter financials, the company announced it had 800,000 customers.

Fixed Broadband subscriptions, including DSL, Fixed Wireless (WiMax), and other fixed line subscriptions, grew to around 2.13 million at the end of Q3 2011.

The Fixed Broadband penetration rate stood at around 30.6 % of households at the end of Q3 2011[72]. Mobile broadband subscriptions reached 11.5 million at the end of Q3 2011, representing a penetration of 40.5% of the population.

Pricing Analysis ($US)	Saudi Arabia	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost	24.00		
Cost per Minute National Call (first 3 min)	0.43	10	0.09
Price for Data Traffic (Price per MB)	0.03	4	0.05
Price for One Text Message	0.07	10	0.02
POST-PAID Package Pricing			
Monthly Package Cost	29.33	8	7.53
Cost per Minute National Call (first 3 min)	0.24	8	0.06
Price for Data Traffic (Price per MB)	0.03	5	0.04
Price for One Text Message	0.05	9	0.03

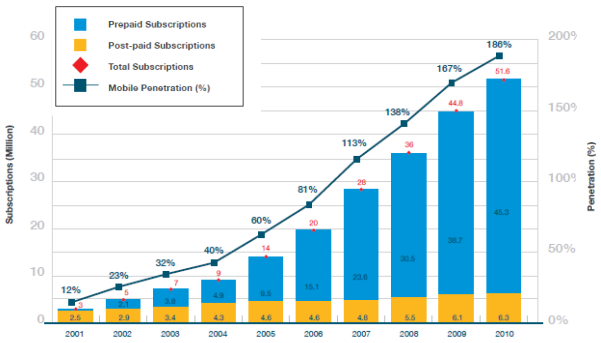
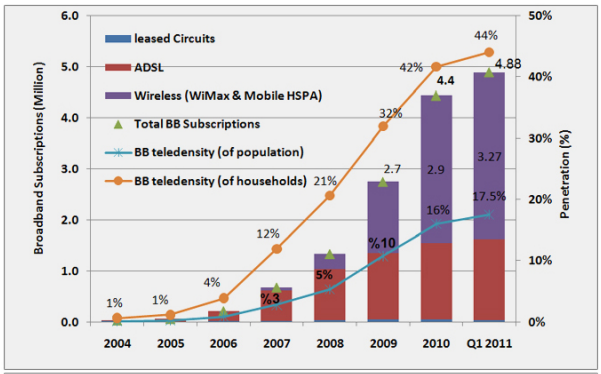


Figure (1): Mobile Service Market Growth - Total Subscriptions (2001-2010) Source: Based on numbers reported by mobile service providers [73]

Operator	Saudi Telecommunications Group	Etihad Etisalat Company	Mobile Telecommunications Company Saudi Arabia
Brands	STC	Mobility	Zain
Survey Respondents	45%	26%	2%
Subscribers	24.3m	22.5m	9.2m
Mobile Internet Users	9.8m	9.1m	3.7m
Ownership	KSA	UAE/KSA	Kuwait/KSA

INTERNET ACCESS

INTERNET CONNECTION TYPES 2010



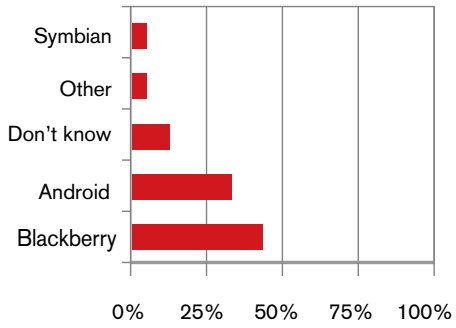
Broadband Market Evolution (2004 - Q1 2011)

Almost 88% of respondents used mobile internet, while 9% do not use mobile internet. 54% of mobile internet users used WiFi to access the internet with 36% paying for a limited volume of data with their subscription and a further 9% paying for usage. No one indicated that they lacked access to the internet using their mobile handsets. Almost 92% owned a smartphone and almost 23% had "jailbroken" their phone. Almost 72% had updated the firmware on their phone.

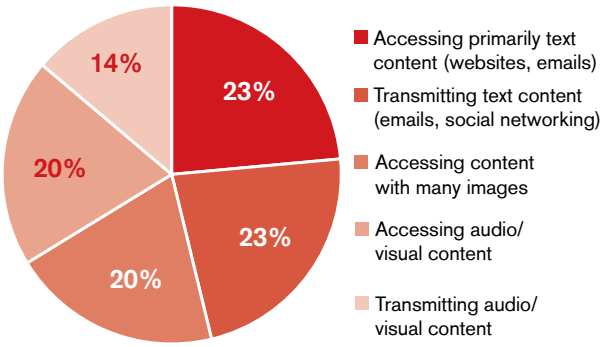
72 http://www.citc.gov.sa/English/MediaCenter/CITCinthemedia/Pages/PR_MED_098.aspx

73 http://www.citc.gov.sa/English/MediaCenter/Annualreport/Documents/PR_REP_006E.pdf

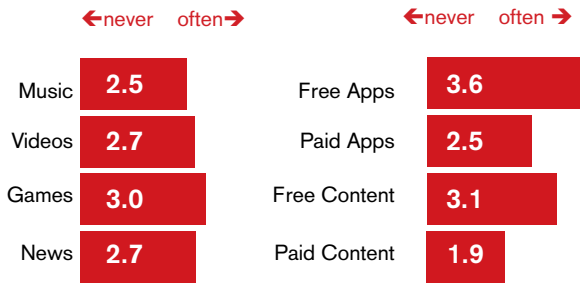
TOP 5 MOBILE OS IN USE



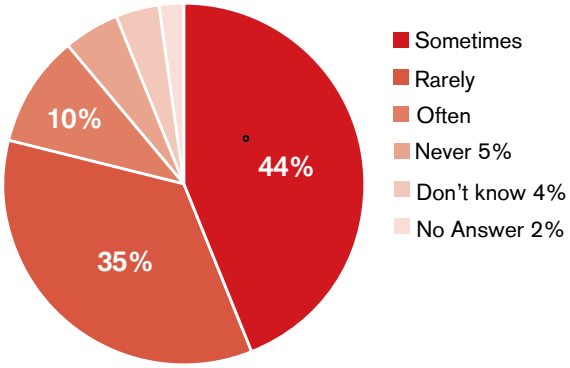
USE OF THE INTERNET 2012 (IN-COUNTRY SURVEY)



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)



HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN COUNTRY SURVEY)



CENSORSHIP AND CIRCUMVENTION

KSA continues to censor the internet to a great extent. It is very open about its internet censorship policies and provides a dedicated web page for reporting any additional content that users feel the need to have blocked. The KSA regularly censors pornographic content, and dissenting political or religious content, along with websites focused on human rights issues.

It is common knowledge that KSA monitors internet usage. In 2009 the government made orders to install hidden cameras in internet cafes and to record the names of all its users.

Censorship in the KSA is done through a proxy farm in the King Abdulaziz City for Science and Technology. This system blocks content on the basis of two lists, one for "immoral content" and the second for content to be blocked by direction of a special security committee run by the Ministry of the Interior. Recently, websites created in the aftermath of the demonstrations in Tunisia and Egypt were blocked. The website of the NGO Amnesty International was blocked after its publication of a draft anti-terrorist law that could have the result of repressing criticism.

PHONE BRANDS[74]

Phone	iPhone 4S	S5570 Galaxy Mini	I9000 Galaxy S	Bold 9780	Curve 8520
Manu	Apple	Samsung	Samsung	RIM	RIM
Released	October 2011	February 2011	June 2010	November 2010	August 2009
					
Data	GPRS/EDGE C10	GPRS/EDGE C12	GPRS/EDGE C12	GPRS/EDGE	GPRS/EDGE C10
Bluetooth	V4.0 with A2DP	V2.1 vA2DP	v3.0 with A2DP	V2.1 with A2DP	v2.0 with A2DP
Sensors	Accelerometer, Gyro, Proximity, Compass	Accelerometer, Proximity, Compass	Accelerometer, Proximity, Compass		
Internet	Yes	Yes	Yes	Yes	Yes
OS	IOS 5.1	Android 2.3	Android 2.3	BlackBerry OS 6.0	BlackBerry OS 5.0
GPS	GPS-A and Glonass	GPS-A	GPS-A	GPS-A	No
Camera	8MP (gps)	3.15 MP (gps)	5 MP(gps)	5 MP	2 MP
WiFi	b/g/n/hotspot	b/g/n	b/g/n/dlna/hotspot	b/g	b/g

CONCLUSION

Market regulation is strong and market competition is very healthy. Almost 82% of users consider themselves intermediate users of mobile handsets and almost 92% of the mobile users in our survey have a range of the most recently manufactured smartphones.

FURTHER INFORMATION

Saudi Communications and Information Technology Commission (CITC) - www.citc.gov.sa
Ministry of Communications & Information Technology - www.mcit.gov.sa
Network Security Center - www.netsec.org.sa
Internet Services Unit - www.kacst.edu.sa
Saudi Telecommunications Group - www.stc.com.sa
Etihad Etisalat Company - www.mobily.com.sa
Mobile Telecommunications Company Saudi Arabia - www.sa.zain.com

74 Data and images from www.gsmarena.com

Syrian Arab Republic

The Syrian Arab Republic has the lowest level of mobile penetration in the region, and among the lowest number of phones in use at 11.9 million subscribers. There are only two mobile operators active in the market and operators give a share of their profits to the state.

TELECOMMUNICATIONS MARKET

In 2001, Syrian Telecom launched the Network of Mobile Operators – BOT (building, operation, transfer) to cover Syrian territories – and in 2002, the Market of Mobile Communications in Syria began, which was restricted to two companies – Syria Tel and 94 Areeba (which in 2007 merged with MTN).

Indicator[73]	Measurement	Value
Computers in Households	Per 100	30.0
Internet Users	Per 100	20.7
Fixed Lines	Per 100	19.9
Fixed Broadband	Per 100	0.33
Mobile Subscriptions	Per 100	57.7
Mobile Broadband	Per 100	n/a
International Bandwidth	Per 100	n/a

Rami Makhlouf, a cousin of the Syrian President, has the largest stake in Syria Tel, and MTN-Syria is owned by MTN group in South Africa. MTN Syria is controlled by some influential people in Syria - including Rami Makhlouf.

There is inadequate competition between both companies; all prices and special offers are always identical.

The public sector's profit share is uncertain. When the contracts were signed, the public sector's profit share was agreed as 30% for the first 3 years from the start of the contract, 40% for the second 3 years, 50% for the next 9 years, and 60% if they renew the contract.

QUICK FACTS SYRIAN ARAB REPUBLIC

Quick facts	Syrla
Land Area:	183,630 sq km
Population:	20.5 million (2010)
GNI per capita, PPP	$5,120 (WB, 2010)
TLD:	**.sy**
Fixed Telephones:	4.1 million (2010)
GSM Telephones:	11.9 million (2011)
Fixed Broadband:	0.07 million (2010)
Internet Hosts:	n/a
Internet Users:	4.2 million (2010)

In 2011, the revenue of SyriaTel during the first half of year amounted to SYP 25.832 billion. The share of Syrian telecom was about SYP 12.306 billion, while the total net profit was about SYP 5 billion.

For MTN, the financial statements confirmed that its revenues during the same period amounted to SYP 20.747 billion. Syria Telecom's share was about SYP 9.862 billion, and the net profit reached SYP 3.119 billion.

Since the start there have been no new entrants into the market, although Syria's Ministry of Communication and Technology has issued a prequalification call for a third mobile network license in September 2010. Qatar Telecom and Saudi Telecom Co. (STC) were the only companies bidding for the mobile license after a number

75 www.worldbank.org and www.mtn.com.sy and www.moct.gov.sy and http://www.syria-today.com/index.php/component/content/article/978-business-news/18979-profits-fall-at-syriatel-and-rise-at-mtn-

of competing firms abandoned their bids amid concerns over the Syrian government's revenue sharing plan[76].

	Number of Clients	Coverage of Residential Areas	Geographical Coverage	Number of Employees	Service Centers
Syria Tel	6,135,000	99%	90%	2,000	55
MTN	5,632,000	99.5%	80%	1,335	63

Customers are currently very frustrated. At the beginning of the revolution, there were a corruption charges against the mobile operators. The fact that prices are identical suggests that products are being offered with a prior agreement between the two companies; this destroys any potential competition in the market to fire up supply and demand. High taxes indicate the limited options in both companies, because they return more than half of their profit to the government.

Pricing Analysis ($US)	Syria	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute National Call (First 3 Min)	0.13	7	0.09
Price for Data Traffic (Price per MB)	0.05	7	0.05
Price for One Text Message	0.13	11	0.02
POST-PAID Package Pricing			
Monthly Package Cost	7.47	5	7.53
Cost per Minute National Call (first 3 min)	0.08	6	0.06
Price for Data Traffic (Price per MB)	0.05	6	0.04
Price for One Text Message	0.08	10	0.03

In June 2001, Syriatel, which runs one of the two 3G networks along with rival MTN, charged SYP 3,000 (US$ 63) a month for "medium" usage of 3 gigabytes. (Fixed-line broadband is also expensive, costing at least SYP 1,000 (US$ 21) a month for speeds of 256 kilobytes per second).

People are using internet for text chat, Skype, live video streaming and web browsing. The number of mobile internet users is approximately 20% of all mobile users.

In terms of handsets, Nokia has the largest proportion of the market handset share (55%); LG, Sony Ericsson, Samsung, Siemens, Chinese Brands and other non-smart phones have 28.5% market share; then Android Mobile Phone (HTC, Samsung, Sony Ericsson) with 15% share, and iPhone at <1,5%. An average monthly subscription fee for the line is SYP 400.

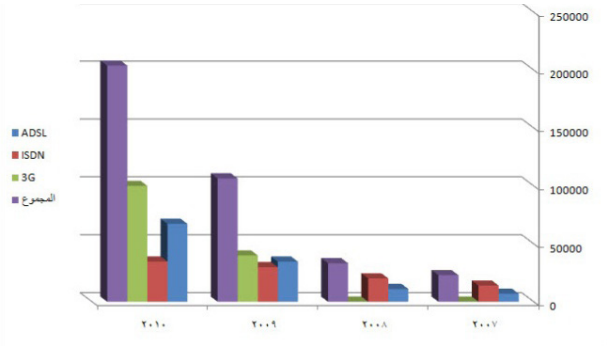
Operator	Syria Tel	MTN
Brands		
Survey Respondents	53%	39%
Subscribers	6.1m	5.6m
Mobile Internet Users	0.5mm	0.33m
Ownership	National	MTN South Africa

INTERNET ACCESS

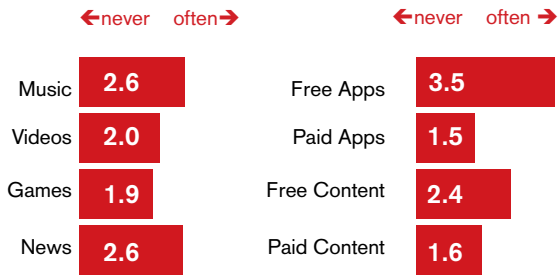
Over 90% of respondents used mobile internet and less than 7% do not use mobile internet. 52% of these mobile internet users pay for usage of mobile internet with 21% paying for a limited volume of data with their subscription and a further 19% using WiFi. Almost 4% indicated they had no access to the internet using their mobile handsets. Over 73% owned a smartphone and almost 12% had "jailbroken" their phone. Over 34% had updated the firmware on their phone.

76 http://www.syria-today.com/index.php/may-2011/793-business-news/14931-mobile-licence-bidders-cut-to-two-

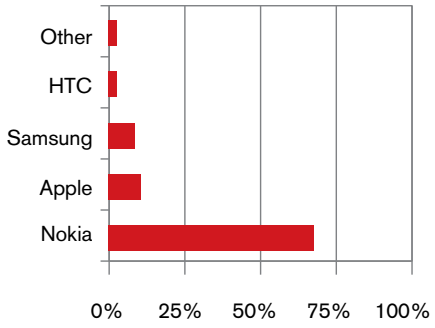
INTERNET CONNECTION TYPES, 2010 (MINISTRY COMMUNICATIONS AND TECHNOLOGY)



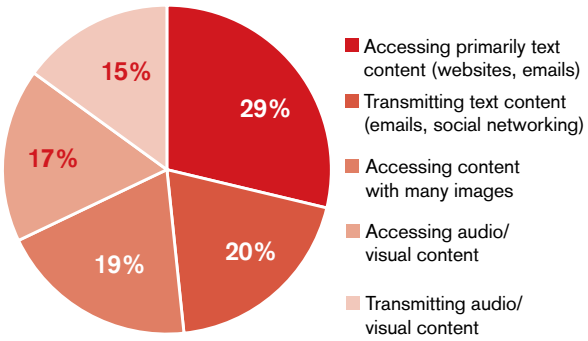
TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)



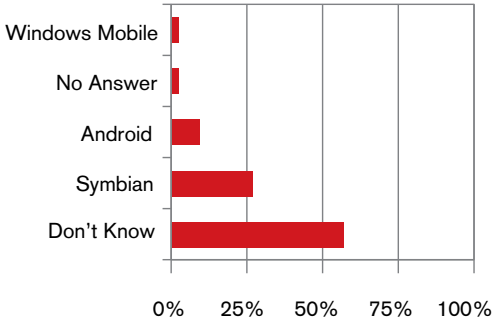
TOP 5 MOBILE HANDSET MANUFACTURERS



USE OF THE INTERNET 2012 (IN COUNTRY SURVEY)



TOP 5 MOBILE OS IN USE



CENSORSHIP AND CIRCUMVENTION

Many activists had been arrested through the use of the GSM tracking systems. Syria is using Sony Ericsson technology to trace the GSM handsets of activists. The operators now block many words being sent over SMS (e.g. freedom, demonstration, group, revolution, etc.).

Syria uses Blue Coat Technology (Blue Coat SG8100 Series) to filter mobile internet and fixed line ISPs. Internet activists from Telecomix released 54 GB of log files created by the Syrian government between July 22nd and August 5th, 2011. According to the 2012 Enemies of the Internet Report[77] by Reporters Without Borders, mobile phones are used to create video and send that video straight to video-streaming websites. Sometimes events are recorded with video cameras and the video files are copied onto USB flash drives and then passed from hand to hand until they can finally be posted online. Skype and Mumble are used quite often for this purpose[78]. Syrians who live the near border use Lebanese or Turkish servers to access the internet or mobile phone networks, thereby escaping surveillance.

In an attempt to limit the size of the protests, and the transmission of photos and videos, the authorities often temporarily suspend internet and mobile phone services in the localities where protests are taking place.

77 http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf (last accessed 12 June 2012)

78 http://mumble.sourceforge.net/ (last accessed 12 June 2012)

SAMPLE PHONE BRANDS IN USE[79]

Phone	E72	5530	Xperia ray (tbc)	Titan	Xperia Arc (tbc)
Manu	Nokia	Nokia	Sony Ericsson	HTC	Sony Ericsson
Released	October 2009	August 2009	August 2011	October 2011	March 2011
					
Data	GPRS/EDGE C32	GPRS/EDGE C32	GPRS/EDGE	GPRS/EDGE C32	GPRS/EDGE
Bluetooth	V2.0 with A2DP	V2.0 with A2DP	V2.1 with A2DP	V2.1 with A2DP, EDR	v2.1 with A2DP
Sensors	Accelerometer, Compass	Accelerometer, Proximity	Accelerometer, Proximity, Compass	Accelerometer, Gyro, Proximity, Compass	Accelerometer, Proximity, Compass
Internet	Yes	Yes	Yes	Yes	Yes
OS	Symbian 9.3 Series 60 v3.2 UI	Symbian OS v9.4, Series 60 rel. 5	Android OS 2.3 – upg to v4.0	Microsoft Windows Phone 7.5 Mango	Android 2.3 upg v4.0
GPS	GPS-A	GPS-A	GPS-A	GPS-A	GPS-A
Camera	5MP (gps)	3.15MP (gps)	8 MP	8 MP	8 MP
WiFi	b/g Nokia VoIP 3	b/g	b/g/n/DLNA/hotspot	b/g/n/DLNA	b/g/n/DLNA/hotspot

CONCLUSION

With only two operators, the Syrian market does not have significant competition. The market is tightly controlled by organizations that are closely aligned with the government. The government receives significant annual revenues from the mobile operators, as specified in their contracts. Mobile penetration has lagged behind other countries in the region.

FURTHER INFORMATION

Ministry of Communications and Technology – www.moct.gov.sy
National Agency for Network Services – www.nans.gov.sy
Syria Tel – www.syriatel.sy
MTN - www.mtn.com.sy

79 Data and images from www.gsmarena.com

Tunisian Republic

Mobile penetration in the Tunisian Republic is reaching 117% of the population. In November 2011, the Tunisian government set up a national holding company called CDC (Caisse des Dépôts et Consignation) to manage it's shareholdings in the country's two mobile operators, Tunisiana and Orange. An independent subcommittee has also been assigned to monitor corruption, approve the general policies of the funds and evaluate the investments. The CDC manages 25% of Tunisiana, 51% of Orange and the Zitouna bank, which was seized from the former ruling family.

TELECOMMUNICATIONS MARKET

The total penetration of mobile phone users in Tunisia is almost 117% (there are more mobile phone subscriptions than the total population). The total number of mobile services subscribers in Tunisia is 12,533,369. The market is dominated by two main operators (Tunisia and Tunisie Télécom) who own 90% of the market with 54% and 36% share of the market, respectively.

Indicator[77]	Measurement	Value
Computers	Per 100	15.0
Internet Users	Per 100	33.4
Fixed Lines	Per 100	10.7
Internet Broadband	Per 100	5.2
Mobile Subscriptions	Per 100	116.6
Mobile Broadband	Per 100	3.4
International Bandwidth	Per 100	568 kb

Until mid-2012, only two operators could afford 3G, Tunisie Télécom and Orange Tunisie. In early 2010, France Telecom's Orange launched a 3G network in the country, in cooperation with Investec, a Tunisian subsidiary of the Mabrouk group. In September

80 http://www.intt.tn/upload/files/Tableau%20de%20Bord%20Mobile%20-%20Mars2012.pdf and http://www.mincom.tn/index.php?id=315&L=2

QUICK FACTS TUNISIAN REPUBLIC

Land Area:	163,610 sq km
Population:	10.55 million
GNI per capita, PPP	$9,060 (WB, 2010)
TLD:	**.tn**
Fixed Telephones:	1.15 million (2012)
GSM Telephones:	12.5 million (2012)
Fixed Broadband:	0.6 million (2012)
Internet Hosts:	12,684 (2012)
Internet Users:	3.5 million (2009)

2010, Tunisie Telecom was awarded a 3G license at a cost of US$ 80.2 million. In May 2012, Qatar Telecom (Qtel) announced that its subsidiary Tunisiana was awarded licenses to launch and operate a 3G network and a fixed-line network by the Tunisian Ministry of Information Technologies and Communication. The licences were purchased for approximately US $135 million. In line with regulatory guidelines, the 3G network will be launched in July 2012, with fixed-line services launching at the beginning of 2013. Tunisiana has also signed an agreement with Huawei to deploy a 3G network in the internal regions within the country.

In June 2012, ZTE from China, which is the world's fourth-largest mobile phone producer[81], announced that

81 http://allafrica.com/stories/201206200071.html - ZTE's Marketing Director, Jasmine Xu, told Xinhua that ZTE employs 85,000 people and ZTE's turnover estimated at US$ 13.6 bn in 2011

it had entered the Tunisian market. Following a test launch in 2011, ZTE opted for Tunisia in its bid to enter the African market. The Chinese company's Tunisian partner, Rayencom, will benefit from the exclusive distribution of a wide range of ZTE products. ZTE will commercialize five products, including two smartphones and a tablet running on Android 2.3.

In February 2012, the Tunisian Internet Agency, in partnership with the company Landolsi L2T Telecom Technology, launched the first multi-store operators to host and download Android applications in Tunisian and international Yasmine Market.

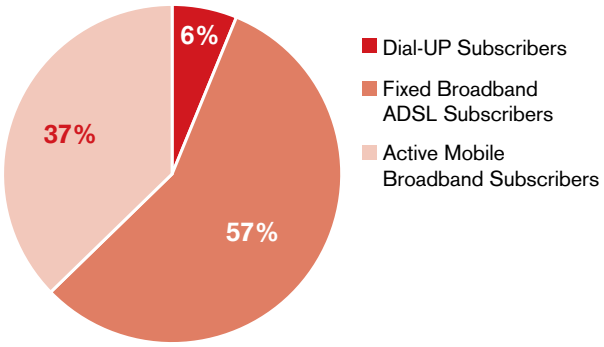
Pricing Analysis ($US)	Tunisia	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute National Call (First 3 Min)	0.14	8	0.09
Price for Data Traffic (Price per MB)	0.01	1	0.05
Price for One Text Message	0.03	7	0.02
POST-PAID Package Pricing			
Monthly Package Cost		1	7.53
Cost per Minute National Call (first 3 min)	0.52	10	0.06
Price for Data Traffic (Price per MB)	0.01	3	0.04
Price for One Text Message	0.03	6	0.03

Operator	Tunisiana	Tunisie Télécom	Orange
Brands			
Survey Respondents	78%	11%	7%
Subscribers	6.8m	4.5m	1.2m
Mobile Internet Users	0.0m	0.0m	0.0m
Ownership	Qatar (Qtel)	UAE	Mixed

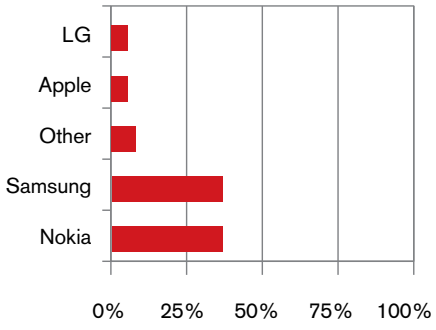
INTERNET ACCESS

45% of respondents said they used mobile internet, with 48% saying they did not. 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.

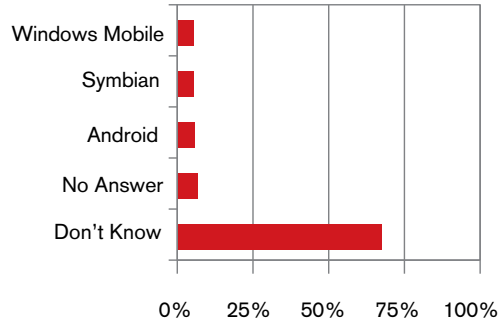
INTERNET CONNECTION TYPES 2010



TOP 5 MOBILE HANDSET MANUFACTURERS

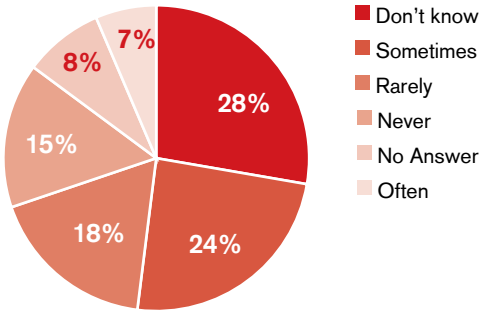


TOP 5 MOBILE OS IN USE



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)

HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN COUNTRY SURVEY)



CENSORSHIP AND CIRCUMVENTION

Before the revolution the government was filtering every call especially for politicians, journalists and artists. It is believed that there is no calls interception after the revolution. In January 2011, the Secretary of State for Information and Communication Technologies stated[82] that access to all websites in Tunisia is free, except for sites with indecent content, comprising violent elements, or inciting hatred. An email address (contact@web-liberte.tn) is made available for citizens and civil society components for any claim in relation to freedom of expression on the internet.

On February 22nd, 2012, the Supreme Court (Cour de Cassation) accepted the appeal of the ATI, the Tunisian Internet Agency, and sent it back to the Court of Appeal. ATI was appealing a decision by a judge issuing an order to requiring ATI to censor pornographic websites. In June 2011, ATI had implemented the filtering of pornographic site addresses listed by Smartfilter®.

CONCLUSION

The market in Tunisia has become more transparent since the Arab Spring movement changed the political landscape. There are three major players and market penetration exceeds 100%.

FURTHER INFORMATION

Instance Nationale des Télécommunications - www.intt.tn
Ministry of Information and Communications Technologies - www.minicom.tn
Tunisian Internet Agency - www.ati.tn
Tunisiana - www.tunisiana.com
Tunisie Télécom - www.tunisietelecom.tn
Orange - www.orange.tn
www.yasminemarket.com
Arab Information and Communications Technologies Organization - www.aicto.org
The ITU's Arab Regional Office - www.ituarabic.org
The ITU's Arab Centre of Excellence - www.ituarabic.org/ceo

82 http://www.mincom.tn/index.php?id=291&L=2&tx_ttnews[tt_news]=784&tx_ttnews[backPid]=11&cHash=c49c057e6f

Republic of Uzbekistan

The telecommunications market of Uzbekistan is in the process of saturation and is one of the fastest growing sectors of the economy. Uzbekistan has the highest rate of growth in the number of mobile subscribers in the CIS. The growth rate of revenues from mobile services lags behind the pace of growth in the number of mobile subscribers. There were 24.3 million mobile subscribers to the end of 2011.[83]

TELECOMMUNICATIONS MARKET

Indicator[80]	Measurement	Value
Computers	Per 100	n/a
Internet Users	Per 100	31.2
Fixed Lines	Per 100	6.6
Internet Broadband	Per 100	0.3
Mobile Subscriptions	Per 100	84.0
Mobile Broadband	Per 100	19.9 (est)
International Bandwidth	Per 100	17.2 kb

There have been no changes in number of operators in the last 3 years: "MTS" brand from "Uzdunrobita" (established June 1991) GSM/UMTS; "Beeline" brand from "Unitel" (established in April 1996) GSM/UMTS; "Ucell" brand from "COSCOM" (established in April 1996) GSM/UMTS; "Perfectum Mobile" brand from "Rubicon Wireless Communication" (established in November 1996) CDMA 2001X; "UzMoble" brand from JSC "Uzbektelecom" (established in August 2000) CDMA-450.

Three major players of the market (MTS, Beeline, and Ucell make up the "Big Three") own more than 98% of the total subscriber base; the "Big Three" operators provide services at GSM, UMTS, and LTE standards. Over 90% of mobile phone handsets are purchased on the black market, because the devices are delivered without any certification that significantly reduces their price.

83 http://www.worldbank.org

QUICK FACTS UZBEKISTAN

Land Area: 425, 400 sq km
Population: 28.2 million
GNI per capita, PPP $3,110 (WB, 2010)

TLD: .uz
Fixed Telephones: 1.9 million (2010)
GSM Telephones: 24.3 million (2011)
Fixed Broadband: 0.15 million (2010)
Internet Users: 8.8 million (2012)

In August 2011, all mobile operators in Uzbekistan suspended internet and messaging services[84] for the duration of university entrance exams in an attempt to prevent cheating. Five national mobile operators shut down mobile internet, text, and picture messaging for four hours from 9 am local time, citing "urgent maintenance work on telecommunications networks." Voice services were not affected but the restrictions affected not just those taking tests, but all of the country's estimated 19 million mobile phone users. In March 2011, Russia's RBC Daily[85] reported that Uzbek regulators had demanded mobile operators notify the government about mass distributions of SMS messages with "suspicious content." A source at the Uzbek Agency for Communications and Information, which regulates the wireless market, told RBC Daily

84 http://www.news.com.au/breaking-news/uzbekistan-halts-mobile-internet-sms/story-e6frfku0-1226107023386

85 http://www.rbcdaily.ru/2011/03/15/media/562949979862486

that mobile operators would also have to switch their internet networks off whenever authorities wish. In addition, operators who control access to the internet, were asked to monitor activity in social networks and the internet as a whole.

In February 2010, TeliaSonera increased its ownership in UCell from 74% to 94% by acquiring 20% of the shares in the jointly-owned TeliaSonera Uzbek Telecom Holding from Takilant for US$ 220 million.

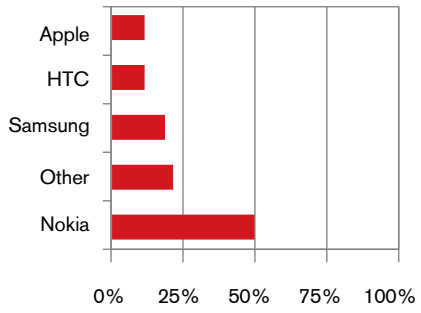
Pricing Analysis ($US)	Uzbekistan	All countries surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost	0.30		
Cost per Minute National Call (First 3 Min)	0.03	1	0.09
Price for Data Traffic (Price per MB)	0.07	8	0.05
Price for One Text Message	0.02	6	0.02
POST-PAID Package Pricing			
Monthly Package Cost	9.40	7	7.53
Cost per Minute National Call (First 3 Min)	0.02	1	0.06
Price for Data Traffic (Price per MB)	0.09	8	0.04
Price for One Text Message	0.02	4	0.03

Operator	MTS (Uzdunrobita)	Beeline	Ucell	Perfectum Mobile	UZMOBILE
Brands					UZTELECOM
Survey Respondents	33.7%	42.2%	12.0%	1.2%	
Subscribers	9.0m	6.9m	8.0m	0.3m	0.17m
Mobile Internet Users	2.2m	1.4m	2.0m	0.02m	0.01m
Ownership	MTS-Russia	Vimpel-Com-Russia	Telia-Sonera Finland	Rubicon Wireless	Uzbek Telecom

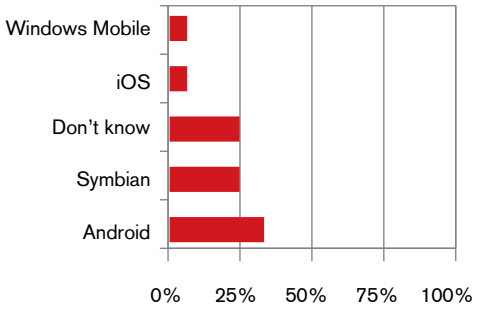
INTERNET ACCESS

87% of respondents used mobile internet and 11% do not use mobile internet. 18% of mobile internet users used WiFi to access the internet with 41% paying for a limited volume of data with their subscription and a further 29% paying for usage. Almost 9% indicated they had no access to the internet while using their mobile handsets. Almost 70% owned a smartphone but only 12% had "jailbroken" their phone. Only 35% had ever updated the firmware on their phones.

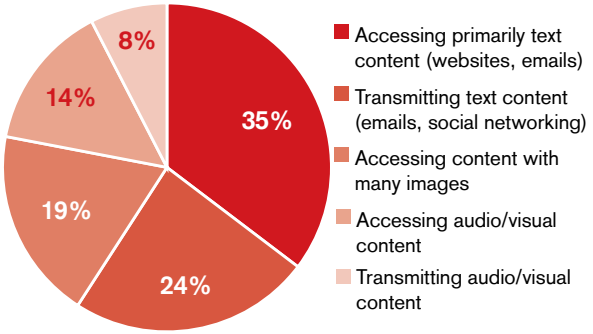
TOP 5 MOBILE HANDSET MANUFACTURERS



TOP 5 MOBILE OS IN USE

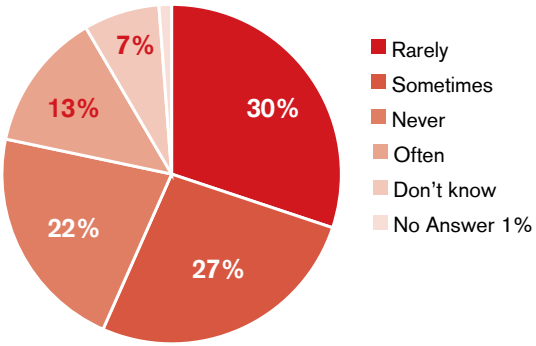


USE OF THE INTERNET 2012 (IN COUNTRY SURVEY)



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)

HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN-COUNTRY SURVEY)



CENSORSHIP AND CIRCUMVENTION

The Uzbek Agency of Communication and Information (UzACI) acts as the main control center in communication and information relations. This administrative structure is authorized to develop and implement state policy in the communication and information technologies sector. According to the decree of the president, there is only one Tier-1 ISP, which is Uzbek telecom– a joint-stock company. All incoming and outgoing internet data passes through the Uzbek telecom switching equipment.

It is rumored that the government can request any information from ISP about their users (name, home address, IP, history logs, etc.) even if there is no crime committed. Most internet users, therefore prefer to use public internet cafes, proxies, and anonymizers to access the internet. It is also understood that the government can easily request any information from mobile carriers about a subscriber (name, address, call logs, and SMS content) even if there is no crime committed.

Several news websites and online newspapers are permanently blocked (although available through proxies and anonymizers). Articles and news criticizing the state, the government, or the president, may be blocked (again, available through proxies and anonymizers). Websites propagating racism, religious beliefs, terrorism, or with adult and pornographic content are restricted.

In some cases, the government can impose a partial/temporary ban on the provision of services: every year on August 1, all mobile carriers turn off extra services such as SMS, MMS, and data for 3-6 hours. This is a day of national university examinations.

The government requires all mobile operators to send informative and warning SMS messages to users. Some activities of mobile operators, such as marketing campaigns or entertainment programs may be blocked by the state. For example, the state ordered all mobile operators and ISPs to not provide any special support on St. Valentines day.

PHONE BRANDS[86]

Phone	1280	6300	E1252	5530	U1280
Manu	Nokia	Nokia	Samsung	Nokia	Huawei
Released	March 2010	January 2007	October 2010	August 2009	July 2009
					
Data	No	GPRS/EDGE C10	No	GPRS/EDGE C32	GPRS/EDGE C10
Bluetooth	No	V2.0	No	v2.0 with A2DP	v2.0 with A2DP
Sensors	n/a	n/a	Dual SIM	n/a	n/a
Internet	No	No	Yes	Yes	n/a
OS	Nokia	Symbian Series 40	Samsung	Symbian OS v9.4 S60r5	n/a
GPS	No	No	No	No	No
Camera	No	2 MP	No	3.15 MP	2 MP
WiFi	No	No	No	b/g	No

CONCLUSION

There is a large black market for mobile handsets. Competition in the market is very good and latest 3G and 4G services are being rolled out. A major concern is the level of state control on mobile operators and the legislative environment they operate in.

FURTHER INFORMATION

Communications and Information Agency of Uzbekistan - www.aci.uz/en
The Governmental Portal of Republic of Uzbekistan - www.gov.uz/en/

MTS (Uzdunrobita) - www.mts.uz
Beeline - www.beeline.uz
Ucell - www.ucell.uz
Perfectum Mobile - www.cdma.uz
UZMOBILE - www.uzmobile.uz/ru/

86 Data and images from www.gsmarena.com

Socialist Republic of Vietnam

The mobile market in Vietnam has been growing very fast. The mobile penetration has reached 137% of population over 9 years. Currently there are over 119 million subscribers. They are also one of the few countries that is making significant progress in the transition to IPV6 internet addressing technologies on the mobile networks. Already a significant amount of Vietnamese mobile broadband users access video content on their mobile phone.

TELECOMMUNICATIONS MARKET

Vietnam is a highly competitive and extremely lucrative telecommunication market for mobile phones. The number of mobile phone users has increased from 2 million in 2004 to 34 million in 2010. Based on data from the census bureau, by January 2012, the number of users in the Vietnam mobile market reached 119 million for a country of 88 million people. The total gross value for the telecommunication market in January 2012 alone is approximately US $500 million.

Indicator[83]	measurement	Value
Computers	Per 100	6.1
Internet Users	Per 100	35.33
Fixed Lines	Per 100	18.9
Internet Broadband	Per 100	5.0
Mobile Subscriptions	Per 100	136.9
Mobile Broadband	Per 100	14.7
International Bandwidth	Per 100	354.9 kb

There are six mobile phone companies operating on the market: MobiFone (41%), Viettel (36%), Vinafone (20%), S phone (3%), Vietnam Mobile, and Beeline. The first four are major players and take up almost the entire domestic telecommunications market.

The last two, Vietnam Mobile and Beeline, only take up a very small market percentage. One, EVN went bankrupt in March 2012 and was taken over by Viettel.

The number of mobile phone users has kept increasing exponentially in the past 7 years, which gives rise to a highly robust and profitable mobile phone market and service industry. Smart phones have become popular ever since Apple iPhone's introduction to Vietnam. Vietnam indicated in its Whitebook 2011[88] that almost 47 million IPv6 addresses had already been allocated for use.

With nearly 90% of the market in the hands of three main players (Mobifone, Viettel, and Vinafone) there is sufficient competition in the market, regardless of

QUICK FACTS SOCIALIST REPUBLIC OF VIETNAM

Land Area:	310,070 sq km
Population:	86.9 million
GNI per capita, PPP	$3,070 (WB, 2010)
TLD:	**.vn**
Fixed Telephones:	16.4 million (2010)
GSM Telephones:	119.0 million (2012)
Fixed Broadband:	4.3 million (2012)
Internet Hosts:	0.8m (2012)
Internet Users:	30.9 million (2012)

87 http://www.worldbank.org & http://www.thongkeinternet.vn/jsp/trangchu/index.jsp

88 http://mic.gov.vn/Attach%20file/sachtrang/sachtrang2011.pdf

the public ownership that underlies the three main operators. Investment levels and profit appear to remain high[89], despite the economic downturn, with various operators announcing investment in mobile broadband[90].

Recent developments include a plan to merge the third largest operator, Vinaphone, with Mobifone, further enhancing the latters dominant position[91]. Most Vietnamese cannot afford iPhones from authorized sales agents. They ask their friends or relatives from overseas to buy "unlocked" iPhones. As a result, they cannot access official Apple iStore applications, but use the non-Apple apps. They find that the fees for Apple apps are out of their reach. They also find Apple apps not very useful in Vietnam, so the use of the is low.

Pricing Analysis ($US)	Vietnam	All Countries Surveyed	
		Rank by Cheapest	Median Price
PRE-PAID Package Pricing			
Monthly Package Cost			
Cost per Minute National Call (First 3 Min)	0.06	3	0.09
Price for Data Traffic (Price per MB)	0.05	5	0.05
Price for One Text Message	0.02	3	0.02
POST-PAID Package Pricing			
Monthly Package Cost	2.40	3	7.53
Cost per Minute National Call (First 3 Min)	0.04	4	0.06
Price for Data Traffic (Price per MB)	0.01	1	0.04
Price for One Text Message	0.01	1	0.03

89 http://www.vinafone.com.vn/61-0-2-1952-Viettel-records-high-profit-in-2011.html

90 http://www.vir.com.vn/news/business/mobifone-to-upgrade-network-by-50-per-cent.html

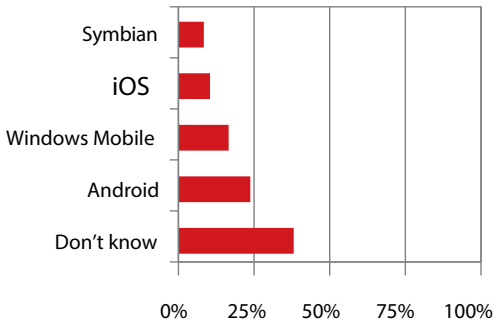
91 http://businesstimes.com.vn/mobifone-vinaphone-to-merge/

Operator	Mobifone	VIETTEL	VINAPHONE	Vietnam Mobile	CDMA-S Telecom	Beeline Vietnam
Brands						
Survey Respondents	57%	20%	21%	2%		
Subscribers	68.4m	29.6m	36.0m	1.2m	1.1m	0.12m
Mobile Internet Users	18.0m	8.9m	10.8m	0.4m	0.8m	0.04m
Ownership	National - VMS and VNPT	National Military Comms	National VNPT	Hanoi Telecom and Hutchinson Asia	Saignon Post and LG DongA Telecom	GTEL and Russia

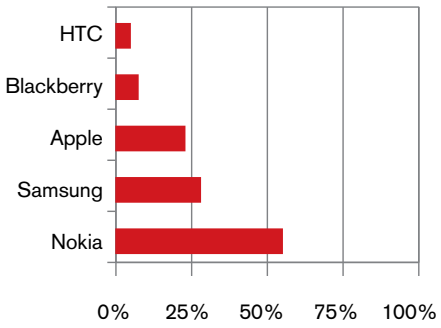
INTERNET ACCESS

91% of respondents used mobile internet and 9% do not use mobile internet. 53% of mobile internet users used WiFi to access the internet with 14% paying for a limited volume of data with their subscription and a further 23% paying for usage. Almost 8% indicated they had no access to the internet using their mobile handsets. Almost 62% owned a smartphone and an amazing 74% had 'jailbroken' their phone and 61% had updated the firmware on their phone.

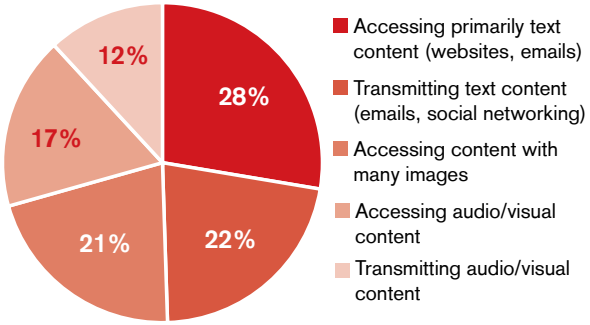
TOP 5 MOBILE OS IN USE



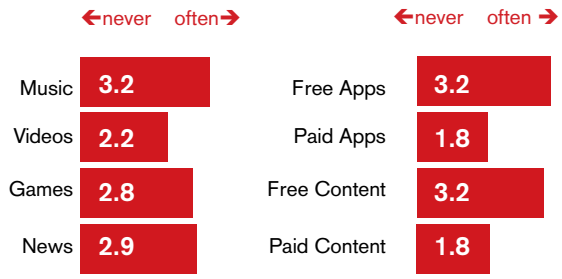
TOP 5 MOBILE HANDSET MANUFACTURERS



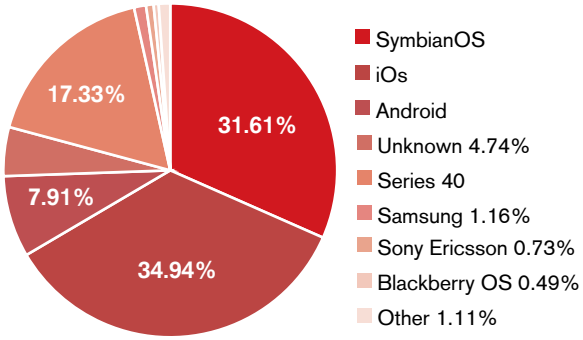
USE OF THE INTERNET 2012 (IN COUNTRY SURVEY)



TYPES OF MOBILE DOWNLOADS INCLUDING CONTENT (LEFT) AND TYPES OF APPS (RIGHT)



MOBILE OS DISTRIBUTION (STATCOUNTER)



ROLE OF MOBILE DEVICES

A significant amount of Vietnamese mobile broadband users access video content on their mobile phone. This is further evidence of Vietnams advanced state of mobile internet access, and corresponds to figures and newsreels seen elsewhere.

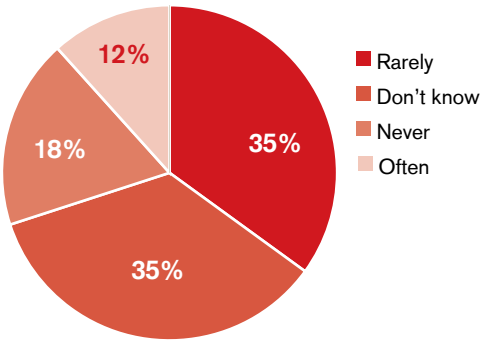
Mobile OS figures also show Vietnam in the forefront, with iOS leading the way after Nokia's Symbian. It should be noted that the user survey produced different phone ownership statistics, especially regarding BlackBerry, which may havee more presence than shows in the statcounter[92] figures.

92 http://statcounter.com/

CENSORSHIP AND CIRCUMVENTION

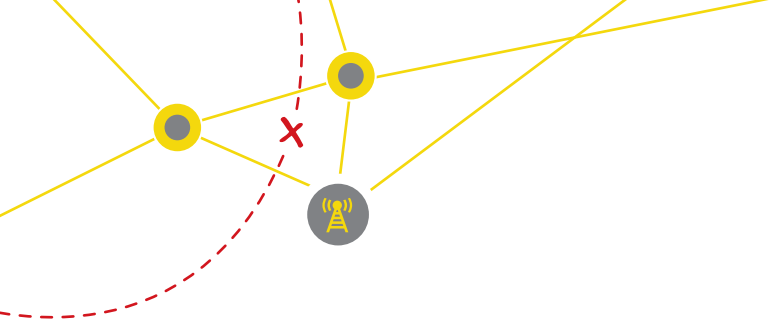
With state ownership of the mobile networks in Vietnam, little, if anything is known about the blocking and monitoring practices of the country. Most evidence is anecdotal, although some can be corroborated using various in-country sources. The state uses firewall technologies to block access to certain sites. They also listen to conversations and trace calls from those on their blacklist. These people are usually high profile "activists" or well-known members of certain targeted organizations. They sometimes disconnect mobile phone service of those who are actively engaged in activities that are deemed "reactionary."

HOW OFTEN DO YOU ENCOUNTER BLOCKED WEBSITES? (IN COUNTRY SURVEY)



Monitoring appears to be regular practice in Vietnam. The recent uproar surrounding China's claim over the Eastern Sea (part of the South Chinese Sea) saw the Vietnamese government reigning in many of the most vocal activists, stirring sentiments against China in an apparent attempt to appease Vietnamese-Chinese relationships. According to the expert survey, conducted many "leaders" in these discussions were confronted with monitored calls and SMS messages.

With as many as 18 bloggers and internet users imprisoned over the past few years, according to Reporters without Borders, Vietnam seems a fertile market for advanced monitoring technology for mobile devices.



Blocking also seems a pervasive practice, especially for political purposes. Social networks such as Facebook, however, also appear to be blocked, even if "unofficially." Although the Vietnamese government denies this, on-going "technical problems" in reaching Facebook's vast US and EU data centers cannot easily be explained other than through blocking – a fact corroborated by many rumours appearing to stem from local Telecom workers who indicate that blocking is taking place at the behest of the Vietnamese government.[93] Still, only a limited number of respondents appear to be hindered by such blocking: only 11% often encounters blocked content.

An expert responder rated the blocking effort much more pervasive, which seems to be confirmed by data from the OpenNet initiative.[94]

93 Stories about randpom blocking of Facebook taking place go back as far as 2009: http://news.bbc.co.uk/2/hi/8370762.stm

94 http://opennet.net/research/profiles/vietnam

PHONE BRANDS[95]

Phone	1280	Galaxy S3 I9300	S5570 Galaxy Mini	IPhone 3	B168
Manu	Nokia	Samsung	Samsung	Apple	Gionee
Released	March 2010	July 2010	February 2011	July 2008 (discontinued)	Yamaha
					
Data	No	GPRS/ EDGE C12	GPRS/EDGE C12	GPRS/EDGE	n/a
Bluetooth	No	v3.0 with A2DP	V2.1 vA2DP	v2.0 with A2DP	n/a
Sensors	n/a	Accelerometer, Gyro, Proximity, Compass, Barometer	Accelerometer, Proximity, Compass	Accelerometer, Proximity	Dual SIM
Internet	No	Yes	Yes	Yes	No
OS	Nokia	Android OS, v4.0.4	Android 2.3	iPhone iOS 4.2.1	Yamaha
GPS	No	A-GPS + Glonass	GPS-A	A-GPS	No
Camera	No	8 MP Rear GPS	3.15 MP (gps)	2 MP	No
WiFi	No	a/b/g/n, DLNA, Direct, hotspot	b/g/n	b/g	n/a

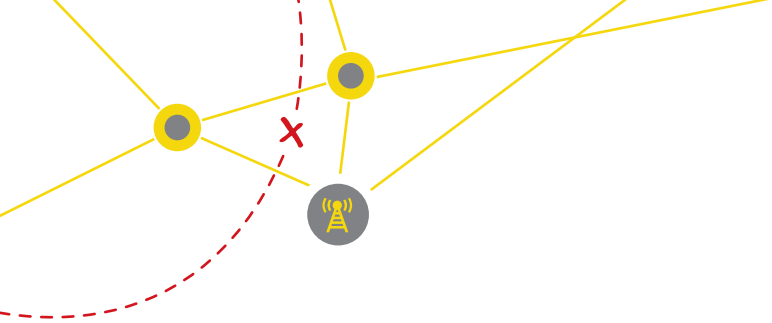
CONCLUSION

Vietnam is one the fastest growing mobile networks in the world. There is pro-active state interest in monitoring and blocking access. Almost 62% owned a smartphone and, different from other countries in the report, an amazing 74% of respondents had "jailbroken" their phone. 61% had updated the firmware on their phone.

FURTHER INFORMATION

Ministry of Information and Communications – english.mic.gov.vn
Vietnam Internet Network Information Center (VNNIC)- www.vnnic.vn
General Statistics Office of Vietnam - www.gso.gov.vn
MTS (Uzdunrobita) - www.mts.uz
Beeline - www.beeline.uz
Ucell - www.ucell.uz
Perfectum Mobile - www.cdma.uz
UZMOBILE - www.uzmobile.uz/ru/

95 Data and images from www.gsmarena.com



Conclusions

Creating the expert surveys, the user surveys and collecting data from public sources has been a complicated activity. Sometimes the need to ensure the safety of the persons who were administering the surveys in country had higher priority than insisting on complete and more detailed feedback and information about the day-to-day experiences using mobile handsets and networks. In some countries such as Vietnam, it is illegal to conduct a survey without a license.

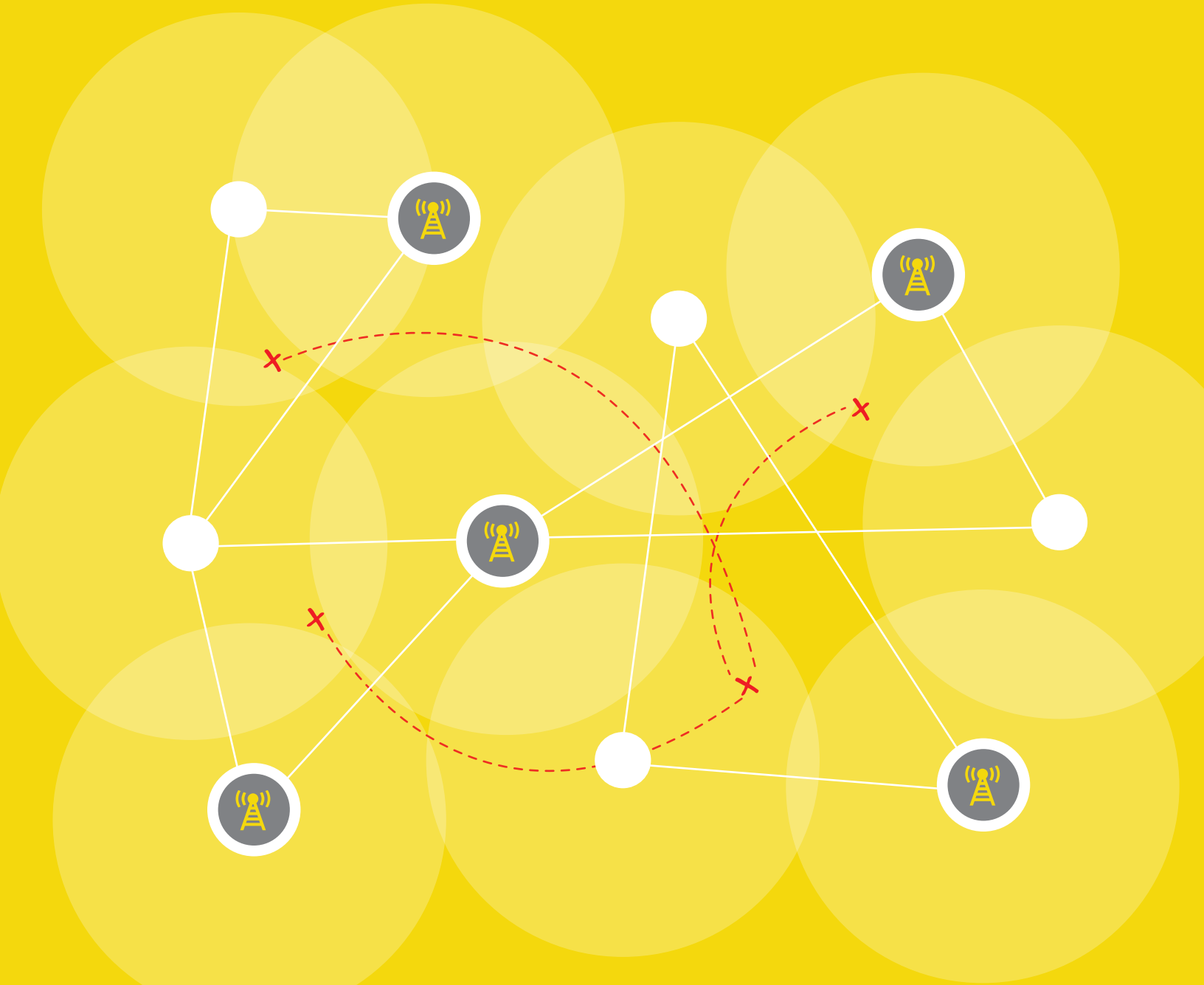
Against a backdrop of ongoing volatility in the regions being analyzed, specific major political upheavals and social unrest in several countries occurred during the period of the work on this report and especially in Egypt and Libya. Whereas it was possible to collect some information about the mobile markets in Egypt it has not been possible to collect adequate levels of data about Libya.

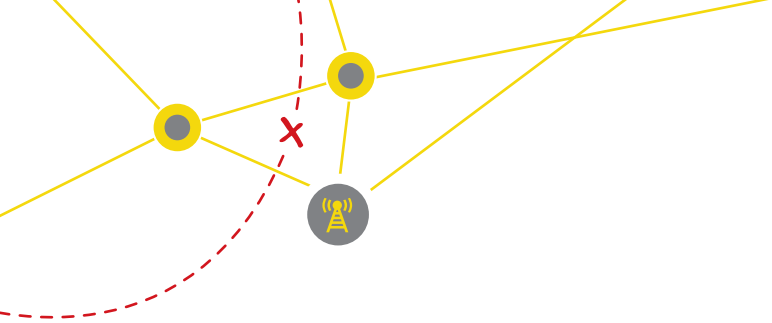
The mobile markets in these countries highlight a number of interesting characteristics.

- Due to the nature of mobile communication where spectrum is a scarce resources requiring direct regulation and management by the state there are easy opportunities to increase mandatory reguirements to include monitoring and surveillance capabilities.
- The size of the mobile markets in all the markets is huge with large levels of mobile penetration. China is the largest at 1,030 million subscriptions and the Sultanate of Oman is the smallest with 4.9 million subscriptions.
- The penetration of mobile subscribion in the population of every country is huge. The Syrian Arabic Republic has the lowest penetration at almost 58%. The Kingdom of Saudi Arabia has the highest penetration at 198%.
- Revenues from the mobile market are significant for both the mobile operator and the government - both in terms of taxes and in terms of license fees.
- The investment in fixed line infrastructure is low in most of the countries in the survey.
- In several countries such as Belarus and 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 would not have been be installed with specific software configured by the state or mobile operator. In several countries such as Sultanate of Oman a handset labeling requirement for authorized handsets has been implemented and spot audits have performed on retail outlets selling handsets to ensure compliance.

Since many mobile operators are multi-national in nature and operate either wholly-owned or part-owned subsidiaries in many markets it will be difficult to control the sale and distribution of surveillance and monitoring technologies or dual use technologies. Due to the global nature of the internet, either the equipment will find its way to the undesirable country or the data can be moved to the location of the equipment for analysis.

Chapter 7:
Conclusions





Conclusions

This project started in November 2011 and was completed in July 2012. The strategy was created at the beginning and each phase of the project was implemented with minor schedule variations.

It became apparent in the early months that this was an area where there was a lot of data and information on the mobile markets and operators, but data on the use of mobile networks and handsets by democratic activists was very sparse. The focus on handset use, and the particular interest on smarthphone apps, was a particular challenge. During the first weeks of the study a literature review highlighted the shortage of material in this area of interest. There was also a dearth of information available on smartphone security.

However, it was also an area that was generating increased interest and attention from many different sources. There was growing attention to mobile malware by the anti-virus companies, and a number of excellent reports were released providing up-to-date information on specific risks for mobile handsets. At the same time, the issue of mobile risk was being regularly discussed in the media and on the relevant security mailing lists. Many of the mobile manufacturers and government agencies released reports describing the security models inside the operating systems (e.g., Apple iOS) and the approach to implement mobile security in the enterprise (e.g., Department of Defence in Australia, NSA in USA).

It became very clear in the early weeks of the technical testing and the public source research that there were enormous, almost unavoidable, risks to security, privacy and, therefore, safety for any person using a mobile network in regions of the world that have a poor history of respect for human rights. It was very obvious that there were many risks at number of levels that would make it a major challenge to identify any relatively secure methods for using mobile phone handsets and networks. It remains true that it would be difficult for an individual to safely use mobile handsets in these countries if they are already a focus of interest for state security.

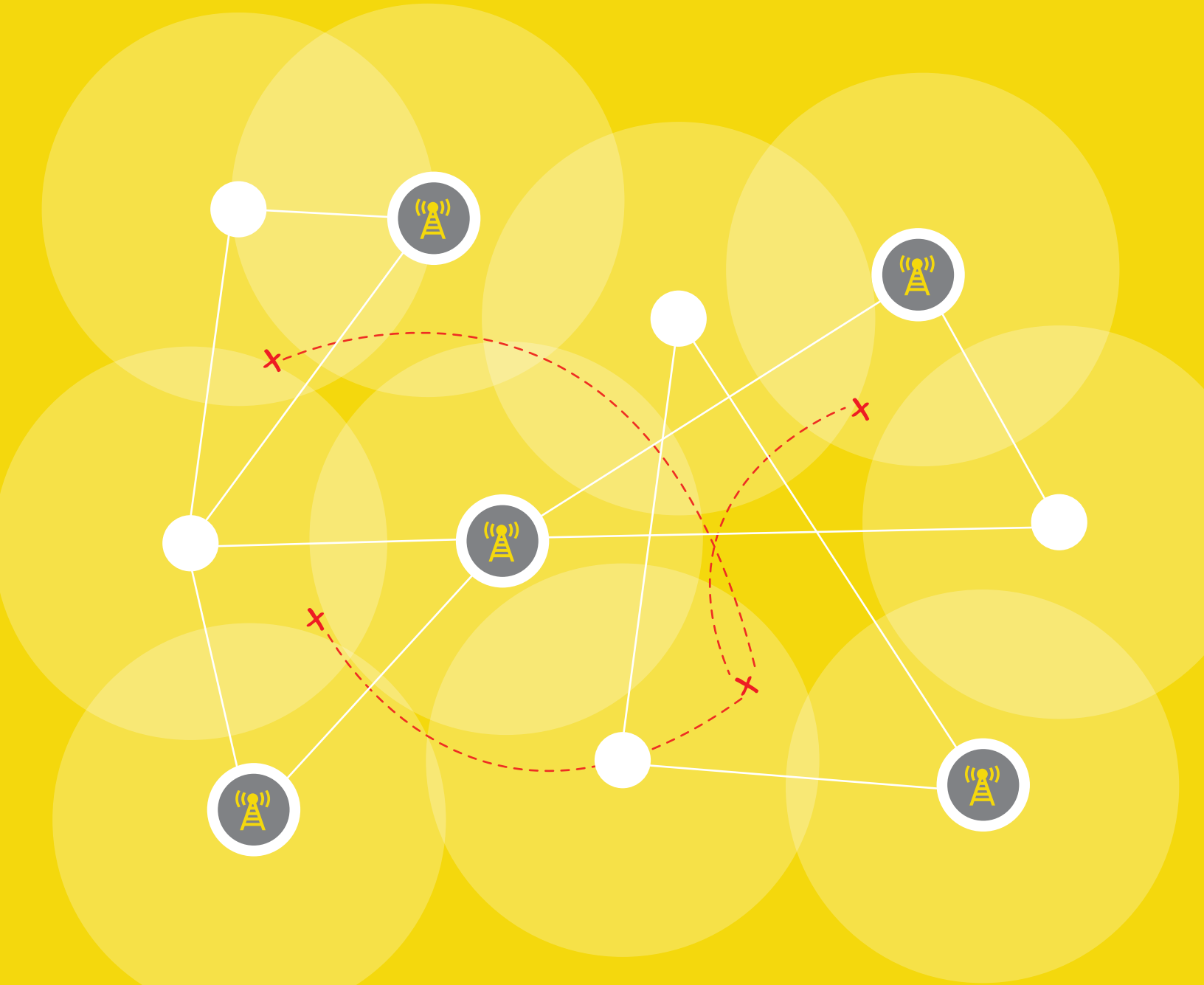
Security of a computer system starts with the creation of a physical level of security for the hardware itself. This is the same for the mobile handset. However, this physical security is already weakened since the mobile handset is created remotely to the specification designed by the state regulatory bodies, are setup and configured by the mobile operator, and during most of their life remain strictly controlled and managed by the mobile operator. In summary, the physical security has already been breached before the owner takes possession of the handset. The solution to this is an independently developed mobile operating system that can be installed on any handset, which will transfer back knowledge and control to the end user.

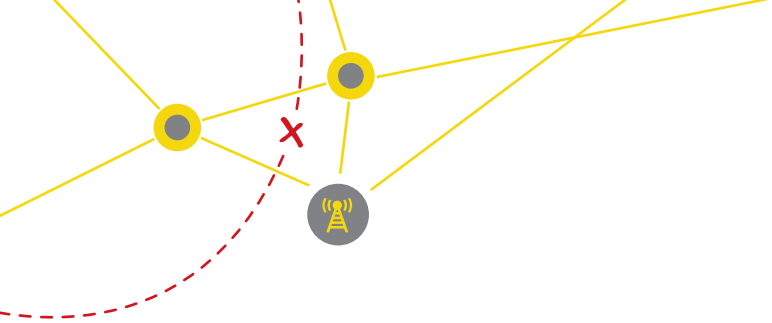
There is an indisputable need to conduct regular, and in-depth reviews of mobile apps in terms of privacy and security. This review must reflect the current level of security built into the hardware and the mobile operating system by the manufacturers. The review needs to acknowledge the lack of expert knowledge of users who still need higher levels of security and provide clear recommendations.

It is clear from the markets that are analyzed in this report that there is a phenomenally high level of penetration of mobile handsets in almost all areas. It is also clear that these markets generate a high level of revenue for the mobile operators, and a high level of license fee revenues for the states in which they operate. As a result of the widespread adoption of mobile phones, the demand for new services will continue and the mobile handset will become a communication tool with no serious competition for many years to come. It is a powerful tool for activists to record incidents of human rights abuse, and via the design of the networks which they connect to, they will also be the best method for states to monitor the activities of their citizens.

The bad news is that there are significant risks at the hardware level, the mobile operating system level, the

Chapter 8:
Reccomendations





regulatory level, the mobile network level, the apps level, and at the end user level. In addition, there are significant risks from malware.

Recommendations

This study has highlighted several issues that exist in the current landscape of applications and services available for circumvention of state censorship in oppressive regimes. It has become clear that it will be impossible for any single actor acting in isolation to change this situation, since both platform security developments at the OS level, as well as application development stakeholders have, so far, left users in these regimes outside their mainstream development goals. Only niche stakeholders have taken the responsibility and have developed true and purpose-built tools for circumvention on mobile devices.

As a first recommendation, these developers deserve support from U.S. government entities working in this space, because they both help the landscape of these initiatives toward the next professional level. They also have the unique opportunity to provide leadership toward a more robust and secure censorship-circumvention landscape. Government entities working on internet censorship issues should also foster the development of new tools, insofar as they provide new and innovative ways of opposing state censorship and monitoring.

It is recommended that efforts be made to bring together the major application developers in this area on a more regular basis, not only to share knowledge and understanding of best practices, but also with a view to developing a number of short term goals that should include:

- Working to bring true circumvention tools to the major platforms used in oppressive regimes – in the near term this will, primarily, require application developers to build these applications themselves.
- Working on better support of VPN services for circumvention scenarios on all major operating systems, with special attention for Symbian (which has a large legacy user base) and support of IPv6.

At the same time, it has become apparent that there are many factors and players that are relevant for this development. Although a narrowly focused group, as indicated above, could probably deliver most results in a short period of time, for the longer term, we suggest more focus on creating a beneficial environment by sharing these goals and efforts with a broader set of actors.

Mobile operating systems, for instance, focus largely on the needs of western consumers, and build applications, security features and platform security models on the basis of a certain amount of trust being placed in network operators and their respective states of operation. This is not a safe assumption to make in the case of the countries we studied. Most operators are firmly controlled, either directly or indirectly, by the regime they operate in.

These states also use or allow many US and European suppliers to deliver enhanced mobile coverage and connectivity to their citizens. Out of all mobile OSs, not one is written primarily in a regime we studied. A large portion of the mobile hardware used by end users is also designed by western companies. Although we note that China, in this area, is rapidly becoming a world class player.

At the same time, the research done for this report makes it clear that a larger pool of expertise is required to develop and test applications in greater depth, and in a timely manner. It would be fitting and appropriate for government entities to bring relevant actors together and ask them to focus more attention (in a real development effort) to the needs of citizens in these new, and rapidly expanding telecommunications markets. Many actors in this area are dependent on each other and yet do not seem to be in regular contact. The actors that could benefit from such efforts include major application

developers, major circumvention application developers, major OS developers, major hardware manufacturers, major security solution providers, major NGOs working in oppressive regimes, major government agencies, foreign counterparts working in the field of communications security and foreign relations, and a selection of activists and bloggers with specific experience in the field.

Together, these actors, in a safe and vetted environment, could then work together on developing strategies, development goals, and best practices to help foster unfettered access to the Internet on mobile devices.

With specific skills and access in the broadcasting arena, awareness raising, through both new and traditional media, about the risks and best practices for using mobile devices could be taken up.

At the same time the role of individual actors cannot be ignored. This report will first highlight the recommendations in the field of awareness raising and then move on to recommendations for other areas.

AWARENESS RAISING

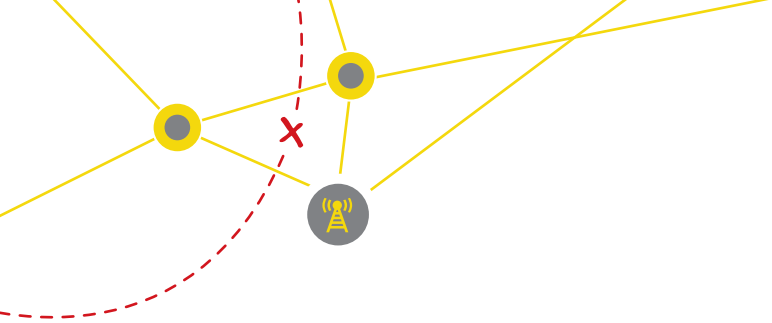
- The level of influence that handset manufacturers have on the safety and security of handsets is significant.
- The complex environments in which mobile operators operate creates challenges for government, industry, and mobile users in order to strike the appropriate balance between current trends in sharing significant amounts of data online while protecting that data from inappropriate abuse.
- In a tightly regulated market with a limited number of operators, and with a highly regulated telecommunications infrastructure, governments can easily dictate mobile policies with respect for, or a total disregard for, international human rights and implement policies that can have devastating effects on democratic principles.
- The modern handset is a complex computer with a vast range of sensors and capabilities. Users need greater knowledge of, and training on, the capabilities of handsets today.
- There is a need to understand the safety and security challenges that users who live in restrictive regimes face on a daily basis. Some circumvention strategies work to bypass blocking and filtering systems but do not offer anonymity or security for the user. This can be dangerous for users who can be identified by the state. Alternative systems offer both circumvention capabilities and high levels of security, which strive to prevent any forensic evidence from being collected by state agencies, which could be used as evidence in a court of law. However, even these systems can be dangerous to users. This is because state agencies in these restrictive regimes are often not searching for high levels of forensic evidence, but only for a simpler system to reduce the high number of potential suspects to a smaller number of suspects for dedicated higher levels of monitoring and interrogation. Using complex secure tools, which cannot be decrypted or hacked by the state can be, in itself, a dangerous identifying criteria.

HANDSET MANUFACTURERS

- Security and privacy architecture by design in hardware and firmware (including the ability to disable remote control of camera, microphone, GPS, radio transmission, etc., and to ensure the ability to securely turn off camera, microphone, GPS, radio transmission, WiFi, etc. Disabling unauthorized remote software updates and reconfiguration without the owners knowledge/permission would be helpful.)
- Secure data encryption in hardware is a key necessity and secure communication using encrypted SMS, voice, data is important.
- Need for openness and transparency.

OS DEVELOPERS

- Security and privacy architecture by design in operating systems.
- Better networking and routing APIs that enable



circumvention tools to operate without "rooting" or "jailbreaking."
- More support for security enhancements to their platform, either through dedicated APIs or through adoption of such enhancing technologies into mainstream operating systems.
- Openness and transparency about their dealings with states that have a direct effect on freedom of speech.
- Support for good practice security.
- Fostering non-western security threat models that encompass non-trustworthiness of state-controlled operators.

APPS DEVELOPERS

- Create more circumvention and anonymity tools to complete the landscape.
- Use security features of the OS as much as possible.
- Make an effort to develop circumvention applications for all platforms rather than focusing on only one.
- Think about how apps could enhance OS security.
- Privacy statements.
- Transparency of purpose, intention and implementation.

IN COUNTRY ACTORS (REPORTERS, INTERNATIONAL AGENCIES, ACTIVISTS)

- Basic and intermediate training on risk assessment and risk mitigation. Attention to high risk environments and activities, especially when risks, and the resultant consequences, cannot be eliminated.
- Regular formal risk assessment (for security, privacy, safety) of each country, government, handset in use, OS, app, mobile operator, and individual.
- Clear, concise, consistent, constructive, and complete advice that is easy to understand.

FUTURE WORK

- The survey of each country needs to be repeated in these countries on an annual basis. There is a need for more engagement with local experts in this area.
- The speed of change in all aspects of the mobile environment is astounding. The focus of this report needs to be repeated at regular intervals to stay up-to-date and relevant.
- Detailed, independent and transparent test. procedures and a laboratory manual need to be created, which would permit regular, repeatable analysis of apps that are specifically developed and coded for circumvention. These apps could be tested on request of the developers, or could be independently tested on request of the end users.

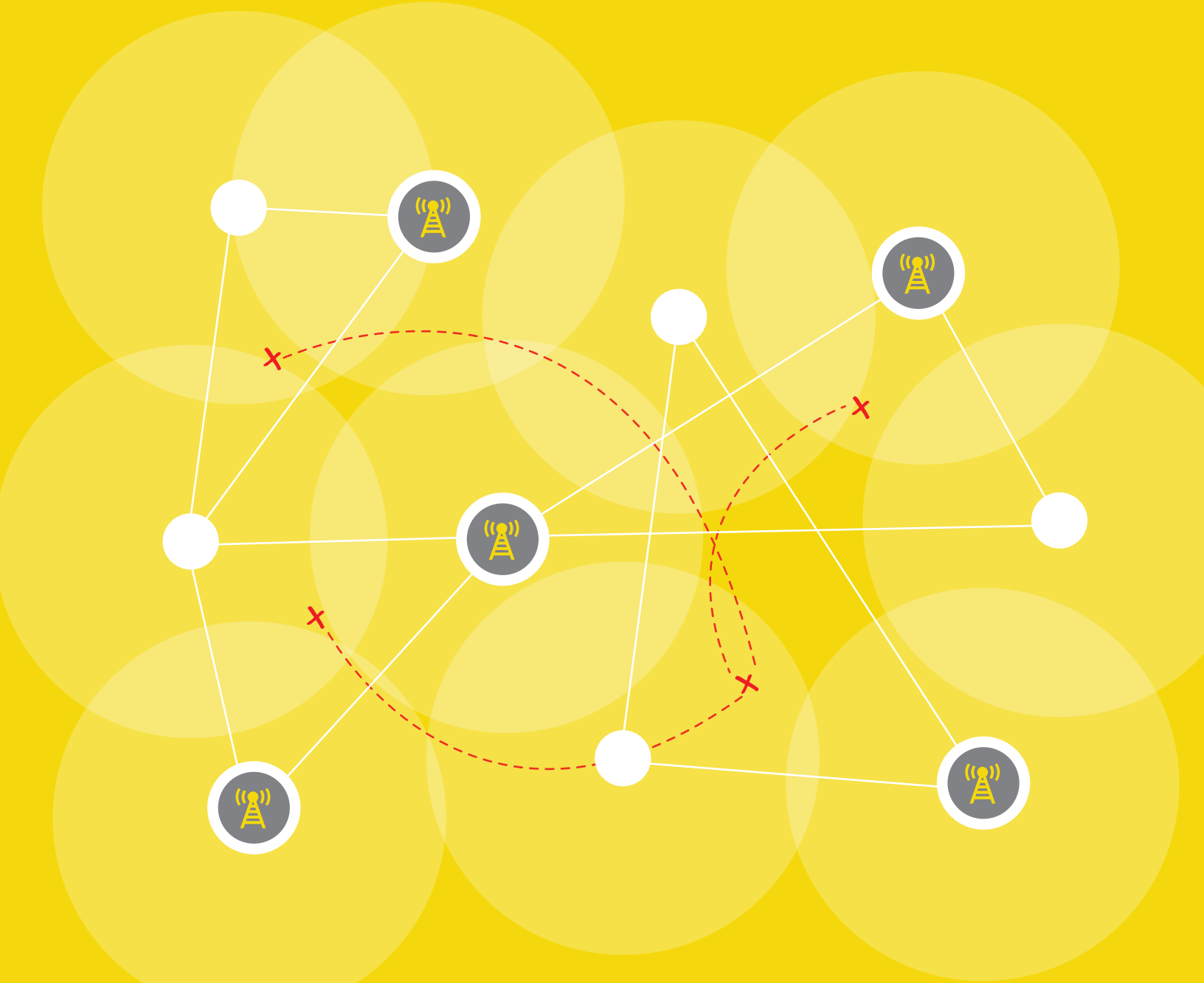
Appendices:

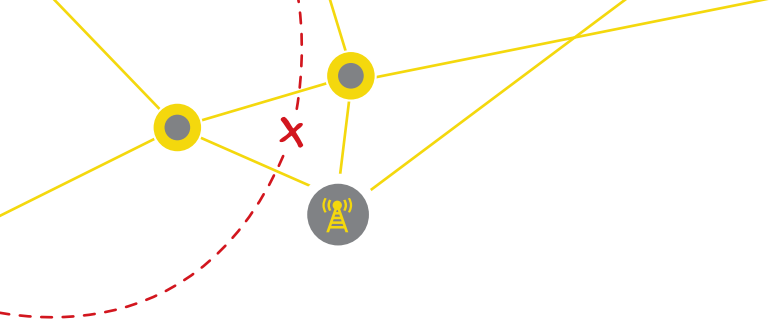
Methodology

Broadcasting Board of Governors Broadcasting Principles

Glossary of Terms

Information Sources





Appendix I
Methodology

The project plan is to work with technology developers and local partners to analyze secure mobile technologies in repressive environments and recommend improved IT security practices in the mobile area.

Rather than focus on a single technology, this analyzed multiple mobile technologies including operating systems, applications, and mobile protocols to determine how they may work to combat censorship and surveillance. Throughout the in-country analysis, the protection of mobile phone users is of paramount importance.

This project was started in October 2011 and completed in July 2012.

Data collection was managed by Freedom House, an independent nongovernmental organization that supports democratic change, monitors freedom, and advocates for democracy and human rights around the world. Financial support was provided by the Broadcasting Board of Governors, an independent federal government agency that oversees all U.S. civilian international broadcasting. Mr. Cormac Callanan, CEO of Aconite Internet Solutions, Dublin, Ireland and Mr. Hein Dries Ziekenheiner, CEO of Vigilo Consulting, Leiden, Netherlands, were responsible for data analysis and for developing the report. Final report design and layout was performed by Catalysto, Dublin, Ireland.

The project consisted of five phases:

- Phase 1 was the creation of a survey collecting detailed information about the mobile market in each country, which was completed by a single identified expert in each country who would collect the relevant information from public sources and in the local language.
- This phase of data collection involved a rigorous assessment of the current mobile markets of 12 countries predetermined by the BBG. The countries selected were Azerbaijan, Belarus, China, Egypt, Iran, Oman, Libya, Saudi Arabia, Syria, Tunisia, Uzbekistan, and Vietnam. Freedom House worked with local partners and staff to identify a key lead researcher in each target country. These individuals were contracted by Freedom House for their time and services. Payment was tied to delivery of data. For their personal safety, their identity is only known by Freedom House.

The survey questions collected information on the current state of the mobile market, including the market size, the size of the mobile operators, the range of phone handsets in regular use and the cost of mobile services for end users. It also dealt with issues around internet blocking and blocking circumvention.

Each research lead was asked to fill out a five-part English language questionnaire about their target country's telecommunications market. If the research lead was not fully knowledgeable, he or she was asked to identify an informed industry expert who could provide the needed information. When circumstances required it, the research lead administered the questionnaire personally to the expert in the local language. Data collected in phase one was entered in an online survey tool in English. Information sought in the expert questionnaire included details about public or private ownership of mobile providers, the pricing structure of the market; incumbent and newcomer mobile providers vying for customers; broadband and WiFi growth; determinants for mobile phone use; mobile hardware and operating systems used; pending infrastructure improvements; new media trends and technologies accessible via mobile devices; filtering and monitoring technologies; accessibility of filtered information on mobile devices; new media technologies accessible via mobile device; and circumvention tools used via mobile.

- Phase 2 was the creation of a user survey collecting views of users on how they used their mobile phones and what knowledge they exhibited about their own capabilities to understand the risks and the security choices available to them to mitigate identified risks.

  This involved a 23-question survey to determine mobile user habits among activists, human rights experts and NGO officials in the 12 predetermined countries. Each research lead identified a sample of key stakeholders. A target of over 200 respondents was sought per country, however this benchmark was only reached in Belarus, China, Oman, Syria, and Tunisia. Only two countries (Egypt and Libya) had less than 100+ due to the serious political upheavals in progress in those countries during the time when the survey was administered.

  The total user survey sample was 1,644.
  The questionnaire was translated into national language(s) and the survey was promoted and distributed by the in-country lead identified by Freedom House. The survey was administered using online survey sites and, in some countries, it was performed on paper and the answers submitted online.

  Once the online responses were collected, the surveys were converted back into English and the survey results analyzed. These survey results provided the in-country knowledge and permitted cross-country analysis as well.

  Incomplete responses were eliminated. Answers from a country, which was not about that country, (some answers were from international locations and were not relevant to the analysis being conducted) were removed from the analysis.

  Information sought in the survey included access and use of mobile service; operating system and the device used; skill level accessing the internet via mobile; applications used; content sharing, jailbreaking and firmware update habits; and attitudes about privacy, content filtering, and government monitoring on mobile.

  The user survey was available in multiple native languages on the online survey tool. Translations and localization of the instrument were carried out by Freedom House language experts. Back translations of responses from local language to English were also managed by Freedom House. If respondents could not access the internet or their connection was insecure, the research lead in-country personally administered the instrument and entered responses into the survey tool. All data curated in phase one and two of this study was exported from the survey tool into Excel where it was cleaned of missing values for analysis. The data is not weighted to represent the general population given the focused nature of the sample.

  The identities of the respondents in Phase 1 and Phase 2 of this project were kept confidential via coding. In addition, respondent names will be excluded in the final analysis and upon completion of the research project. Collected data will be kept in private files at Freedom House. The participants were not misinformed about the true nature of the project.

  An introductory document outlining the objectives of the research and involvement of Freedom House and the BBG was circulated to each in-country research lead. Any anticipated physical, psychological, social, or legal risks to the respondents were minimized. Each in-country research lead was discrete in their recruitment of participants and in operationalization of the survey instrument.

- Phase 3 was a lab technical analysis of the major phone platforms and performing forensic analysis on network data exchanged. This phase of the project involved a “hands-on” technical assessment of specific mobile handsets including Apple iPhone 4 8GB, Nokia N8, HTC Radar, BlackBerry Curve 8520, HTC Desire S.

Phone	iPhone 4 8GB	Curve 8520	Radar	Desire S	N8
Manu	Apple	BlackBerry	HTC	HTC	Nokia
Released	June 2010	August 2009	October 2011	March 2011	October 2010
					
Data	GPRS C10 48kbps EDGE C10 236kbps	GPRS C10 48kbps EDGE C10 236kbps	GPRS 80 kbps EDGE (236kbps)	GPRS 114 kbps EDGE 560 kbps	GPRS Class 33 EDGE Class 33
Bluetooth	V2.1 with A2DP	V2.0 with A2DP	V2.1 with a2DP, EDR	v2.1 with A2DP, EDR	v3.0 with A2DP
Sensors	Accelerometer, Gyro, Proximity, Compass	n/a	Accelerometer, Proximity	Accelerometer, Proximity, Compass	Accelerometer, Proximity, Compass
OS	OS 5.1	BlackBerry OS 5.0	Microsoft Windows Phone 7.5 Mango	Android OS, v2.3	Symbian^3 OS, upgradable to Nokia Belle
GPS	A-GPS	n/a	A-GPS	A-GPS	A-GPS
Camera	5 MP with geo	2 MP	5 MP with geo	5 MP with geo	12 MP
WiFi	b/g/n/hotspot	b/g	b/g/n/DLNA	b/g/n, DLNA, hotspot	b/g/n, UPnP

The devices were tested with different applications installed using a WLAN network connection and with GSM network connections. The traffic generated on the WLAN network was captured and analyzed to determine what types of data were available when using specific applications. The tests were performed on a range of operating systems (such as Android, Symbian, iPhone and Windows Mobile).

An assessment of current techniques practiced by end users to evade censorship and surveillance of the web on mobile devices was also conducted. Part of the test was also an extraction of the phones data using specialist forensic tools.

- Phase 4 was collecting all the data, analyzing the data, and combining the results of the technical lab testing to understand the current stage of evolution of the mobile markets in the target countries.
- Phase 5 involved writing this report and selecting the relevant public information to include while developing recommendations.

SCORING

Scoring of applications remains a subjective exercise, and was made difficult by the different types of applications tested. In order to provide further objectivity, the following criteria were applied, where possible (if no criteria mentioned only an appraisal was used):

PRICE

1	2	3	4	5
Free	Small fee	Paid	Paid and third party service required	Expensive to operate

APP AVAILABILITY

1	2	3	4	5
Non stock app store	Stock app store	Other sources and app store	Hash included at other sources	Many channels, hash included, added security present

OS INTEROPERABILITY

1	2	3	4	5
1 OS only				Present on all 5 OSs tested

HARDWARE LIMITATIONS

1	2	3	4	5
Only one or few phones available that can run the app		Present on 3 OSs, with no hardware limitation		Present on all 5 OSes tested, no hardware limitations

REQUIRES ROOTING

1	2	3	4	5
1 Requires full root/ jailbreak		Limited functionality if no root present		Runs as default application

PROPORTIONALITY OF "PERMISSIONS"

1	2	3	4	5
Not proportional (unneeded permissions present)		Some doubt towards certain permissions being required		Proportional towards app goal.

ANONIMITY (PERSONAL IDENTIFIERS, PERSONAL DATA)

1	2	3	4	5
1 No Anonimity offered		Some resilience to disclosing users ID and credentials present		Securely stores all credentials.

PREVENTS TRACKING

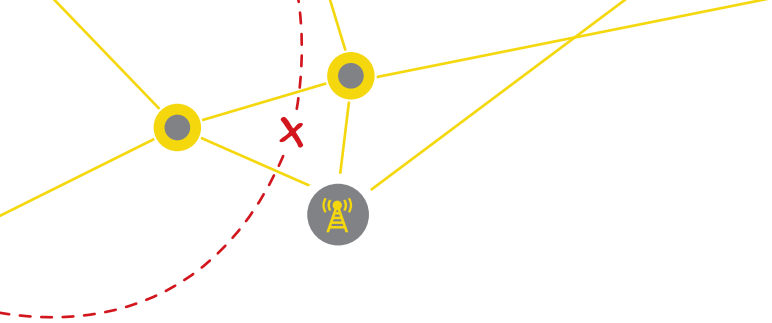
1	2	3	4	5
No anti –tracking features		Some options to erase traces, not fully watertight		Actively designed to prevent tracking of user behavior

APPS SUPPORTED

1	2	3	4	5
Only one application is secure from blocking and monitoring/ threats		Some applications may use this application too, does not work with all		All applications benefit from this app.

CRYPTO - ON THE WIRE

1	2	3	4	5
No encryption present in network traffic		Undisclosed encryption present		Peer reviewed crypto algorithm was disclosed, full encryption present on the wire.



RESILIENCE TO BLOCKING

1	2	3	4	5
No features present		Resilient to DNS or IP blocking.		Resilient to both IP and DNS blocking, uses crypto

CONTROLLED CARRIER CHANGE (MAINLY APPLIED TO CIRCUMVENTION TOOLS)

1	2	3	4	5
Crashes on controlled carrier change, without warning		Crashes with a warning		Survives carrier change without leaking IP address information of the carrier at all

FORCED CARRIER CHANGE

1	2	3	4	5
Crashes on forced carrier change, without warning		Crashes with a warning		Survives carrier change without leaking IP address information of the carrier at all

RESEARCHERS

The in-country research contacts were selected through an extensive vetting process caused by the somewhat sensitive nature of the planned research. They were initially identified through trusted contacts with the focus on individuals who possessed the requisite technical expertise and a willingness to work with project stakeholders.

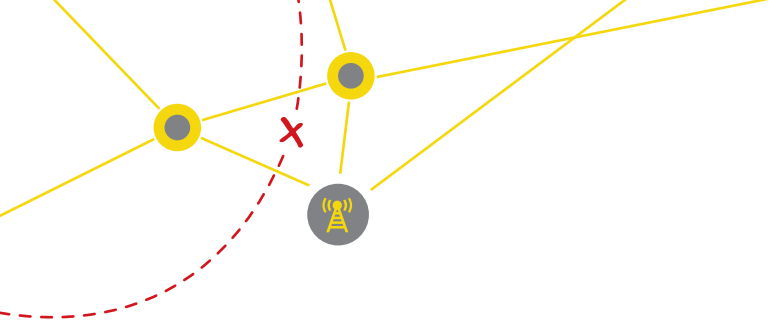
Azerbaijan:	The researcher is an independent journalist with a strong technical background who has worked on previous research projects in a similar field.
Belarus	The researcher is an independent consultant, computer engineer, and programmer.
China	The researcher is an independent consultant with more than five years of experience working at the intersection of technology and media in China.
Egypt	The researcher is leader of a nonprofit involved in projects applying mobile technology to social causes across the Middle East.
Iran	The researcher is an activist with technical expertise and experience with technical research.
Oman	The researcher has over ten years of experience in the public sector working on telecom issues in Oman.
Saudi Arabia	The researcher has over ten years of experience working on telecom issues.
Syria:	The researcher is a local activist with extensive private sector experience in telecommunications.
Tunisia	The researcher is a student focusing on technology policy and social issues in Tunisia.
Vietnam	The researcher leads a consulting company specializing in technical research and analysis.
Uzbekistan	The researcher has years of experience as a telecommunications engineer.

Appendix II

Broadcasting Board of Governors Broadcasting Principles

(From the International Broadcasting Act of 1994) U.S. publicly-funded civilian overseas broadcasts will include:

- News which is consistently reliable and authoritative, accurate, objective, and comprehensive
- A balanced and comprehensive projection of United States thought and institutions, reflecting the diversity of United States culture and society
- Clear and effective presentation of the policies, including editorials, broadcast by the Voice of America, which present the views of the United States Government and responsible discussion and opinion on those policies
- The capability to provide a surge capacity to support United States foreign policy objectives during crises abroad
- Programming to meet needs which remain unserved by the totality of media voices available to the people of certain nations
- Information about developments in each significant region of the world
- A variety of opinions and voices from within particular nations and regions prevented by censorship or repression from speaking to their fellow countrymen
- Reliable research capacity to meet the criteria under this section
- Adequate transmitter and relay capacity to support the activities described in this section
- Training and technical support for independent indigenous media through government agencies or private United States entities



Glossary of Terms

Circuit Switching
A method of communication where a communication channel (either a physical wire or a virtual circuit through a network) is reserved for the duration of a communication session. This is how the telephone network has always operated, and still mostly does.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
Networkingconcept whereby several nodes share a medium and sense that another node is using it. Usually CSMA/CD networking protocols, such as Ethernet, are prone to packet collision: if several nodes start sending to the shared medium simultaneously their transmission is lost and they will have to resend the communication again, preferably at a different point in time to prevent another collision.

DNS Domain Name System
A system that translates human-readable hierarchical names into IP addresses that are necessary to transmit IP packets.

EDGE
GSM Evolution (EDGE) technology provides up to three times the data capacity of GPRS.

GGSN Gateway GPRS Support Node
Network element in mobile networks that allows mobile users to access the internet or (if available) other (often paid) data services offered in the mobile network. The GGSN assigns an IP address to each user requiring internet access and saves all details regarding the session in a PDP context.

GPRS General Packet Radio Service
Extension of GSM networks that allows cheaper, more efficient data transmission on the mobile network through data-only channels. The user only occupies the radio link when he needs to exchanges data, contrary to its predecessor, where a user would dial in, and occupy a radio channel during the entire session.

GSM Global System for Mobile Communications (Originally Groupe Spécial Mobile)
Global standard for mobile telephony. GSM allows for digital compression of the voice signal and is more efficient than its analogue predecessors. Considered a 2G (second generation) mobile technology.

GSM Roaming
The ability for a customer to make and receive calls, send and receive data, or access other services when travelling outside the coverage area of their home network.

HSPA
The set of technologies that enables operators to upgrade their existing 3G/WCDMA networks to carry more traffic and at faster speeds.

IP Internet Protocol
System that allows transmission of data on many different types of physical infrastructure. It can, therefore, be used to interconnect many different types of networks, without the need for conversion of the data. IP may refer to both IPv4 and IPv6 in general, or to just IPv4, depending on the context.

IPv4
Version 4 of the internet protocol (see IP) that uses addresses of 32 bits.

IPv6
Version 6 of the internet protocol (see IP) that uses addresses of 128 bits. Planned widescale implementation in 2012.

LTE
Designed to be backwards-compatible with GSM and HSPA, Long Term Evolution uses the OFDMA air interface, in combination with other technologies, to offer high throughput speeds and high capacity.

MSISDN Mobile Subscriber ISDN Number, Mobile Station International ISDN Number, Mobile International ISDN Number, or Mobile Station International Subscriber Directory Number
A number uniquely identifying a subscriber to a (GSM or UMTS based) mobile network.

NAT Network Address Translation
Used to allow multiple devices to share a single IP address.

Packet Switching
The practice of sending individual packets through a network without the need to first create a connection or session. This is more efficient than circuit switching because network capacity is only used when data is actually being sent. The internet is a packet switched network.

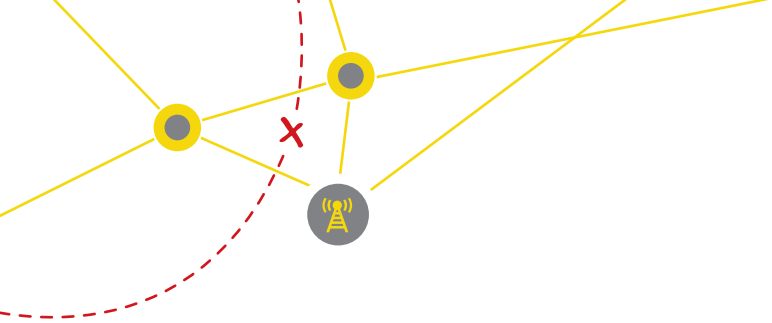
PPP Point-to-Point Protocol
A datalink (layer 2) protocol for sending packets over connections between two points. Used for dial-up access, and also for some broadband deployments.

TCP Transmission Control Protocol
The most widely used transport layer (layer 4) protocol on top of IP. TCP allows for reliable, connection-oriented data delivery.

UDP User Datagram Protocol
A very simple transport layer (layer 4) protocol for sending individual data packets under the control of an application. Is used for very simple transactions with a one-packet request and a one-packet reply (such as with the DNS) or for time critical types of communication, where TCP is unsuitable.

UMTS Universal Mobile Telecommunications System
A third generation (3G) system for mobile telephony and mobile data communication.

WCDMA
The air interface for one of the International Telecommunications Union's family of third-generation (3G) mobile communications systems.



Information Sources

Audience Scapes - An online tool and research program providing media use information on developing countries.
http://www.audiencescapes.org/country-profiles/country-profiles-2

CyanogenMod - An aftermarket firmware for a number of cell phones based on the open-source Android operating system. It offers features not found in the official Android based firmwares of vendors of these cell phones.
http://www.cyanogenmod.com/

Budde.com - Telecommunications research website, focusing on the telecommunications market and its interaction with the digital economy.
http://www.budde.com.au/

Enisa - ENISA was set up by the E.U. to respond to the cyber security issues of the European Union. T
http://www.enisa.europa.eu
http://www.enisa.europa.eu/activities/application-security/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware/at_download/fullReport

Firefox OS - Mozilla's planned fully open mobile ecosystem based on HTML5.
http://blog.mozilla.org/blog/2012/07/02/firefox-mobile-os/

Flurry – A mobile application analytics and data-powered advertising platform.
http://www.flurry.com/

F-Secure Mobile - Security program developer for smartphones and tablet computers.
http://www.f-secure.com/en/web/home_global/protection/mobile-security/overview
http://www.f-secure.com/weblog/archives/00002363.html

GSM Association - Group representing the interests of mobile operators in 220 countries. Sponsors the Mobile World Congress and Mobile Asia Expo.
http://www.gsm.org

Guardian Project
http://prezi.com/-tmhpy_ux1l-/the-guardian-project-2012/

Information Security Coalition - Global development organization focused on economic development, food security and nutrition, and governance and institutions.
http://www.counterpart.org

International Telecommunications Union (ITU) - A United Nations agency, the ITU works to identify, define, and produce statistics covering the telecommunication/ICT sector. Collects information across over 100 telecommunication/ICT indicators. The ITU's Market Information and Statistics (STAT) Division collects its Telecommunication/ICT data directly form governments by means of an annual questionnaire that is sent to the government agency in charge of telecommunications/ICT. This is usually the Ministry or the regulatory agency. The STAT Division verifies and harmonizes data, carries out research, and collects missing values from government web sites and operators' annual reports, particularly for countries that do not reply to the questionnaire. Market research data are also used to cross-check and complement missing values.
http://www.itu.int/ITU-D/icteye/Default.aspx
http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx
http://www.itu.int/ITU-D/ict/index.html

Juniper Mobile Security Report
http://forums.juniper.net/t5/Security-Mobility-Now/Juniper-Mobile-Security-Report-2011-Unprecedented-Mobile-Threat/ba-p/129529

CryptoFone Ltd
http://telecommunication.indiabizclub.com/profile/2193768~cryptofone+ltd.~brisbane+queensland_australia

Liberation Tech Mailing List - The Program on Liberation Technology "Liberationtech" investigates how information technology can be used to defend human rights, improve governance, empower the poor, promote economic development, and pursue a variety of other social goods.
https://mailman.stanford.edu/mailman/listinfo/liberationtech

McAfee Mobile Security - Security company offering software to combat mobile device data loss and threats that target smartphones, tablets, and other mobile devices.
http://www.mcafee.com/us/products/mobile-security/index.aspx

MobileActive.org - Group promoting mobile technology strategies for NGOs worldwide.
http://MobileActive.org

Mobile Business Briefing - Clearinghouse for mobile market information.
http://www.mobilebusinessbriefing.com

mobiThinking - Mobile marketing organization.
http://mobithinking.com/

OpenITP - Supports and incubates a collection of free and open source projects that enable anonymous, secure, reliable, and unrestricted communication on the internet.
http://openitp.org/

Symantec Mobile Security - Mobile device security provider.
http://www.symantec.com/mobile-device-security

SS8 - Business providing interception, monitoring, data discovery and reconstruction services.
http://www.ss8.com/index.php

StatCounter - A free, online visitor stats tool.
http://gs.statcounter.com

TOR - (The Onion Router) is free software designed to enable online anonymity.
https://www.torproject.org/Reference

Wall Street Journal Surveillance Catalog - Documents pertaining to the worldwide market for off-the-shelf surveillance technology, a growing industry since since the terrorist attacks of Sept. 11, 2001.
http://projects.wsj.com/surveillance-catalog/#/

Bugged Planet - Data on intercept and surveillance vendors .
http://buggedplanet.info/index.php?title=Main_Page

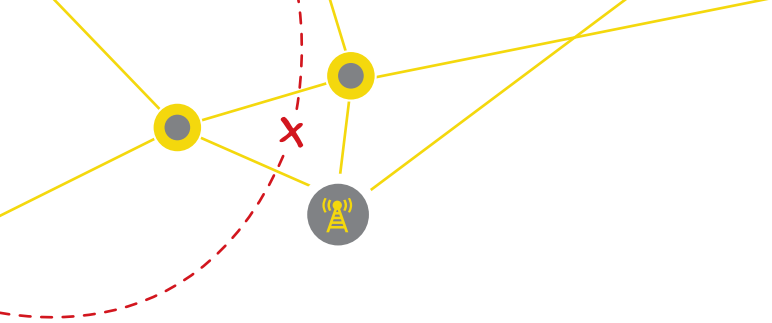
WSJ (October) Huawei Tech. and Iran
http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html?KEYWORDS=Chinese+Tech+Giant+Aids+Iran

WhisperSys - Security and management firm focusing on phones and tablets.
http://www.whispersys.com/

World Bank - Portal for World Bank data.
http://siteresources.worldbank.org/FORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/ICT_Little_Data2011.pdf
http://data.worldbank.org/

Internet World Statistics -Website featuring metrics on world Internet usage, population statistics, travel statistics, and Internet market research.
http://www.internetworldstats.com/middle.htm

Wireless Intelligence - Global database of mobile market information, boasting over 5 million individual



data points on 940 operators (across 2,200 networks) and 55 groups in 225 countries
https://www.wirelessintelligence.com

VisionMobile - Mobile market analysis and strategy firm.
www.visionmobile.com

Zfone - VoIP phone software product.
http://zfoneproject.com/prod_zfone.html

DEVELOPERS

Android Developer
The Android SDK contains tools, sample code, and docs for creating Android-based apps.
developer.android.com

Apple Developer
Apple site containing tools, sample code, and docs for creating iOS-based apps..
developer.apple.com

Windows Mobile Developer
contains tools, sample code, and docs for creating Windows Phone-based apps.
msdn.microsoft.com/en-us/windowsmobile

Mobile Operators
Additional links to the main operators are located in the country profile section.

State Organizations
Additional links to the main operators are located in the country profile section.

This report was supported by:

Broadcasting
Board of
Governors

Freedom House
1301 Connecticut Avenue, NW,
Washington, DC 20036
www.freedomhouse.org

Broadcasting Board of Governors
330 Independence Avenue, SW,
Washington, DC, 20237
www.bbg.gov

designed by catalysto