Project Report

on

A STUDY ON CONSUMER PERCEPTION AND AWRENESS ABOUT SMARTPHONE PRIVACY AND SECURITY

Submitted By
RAHUL SHARMA
2K12/MBA/50

Under the guidance of
MS. MEHA JOSHI
Assistant Professor, DSM

Delhi School Of Management
Delhi Technological University
Bawana Road, Delhi, 110042

CERTIFICATE FROM THE INSTITUTE

This is to certify that the Project Report titled "**A STUDY ON CONSUMER PERCEPTION AND AWRENESS ABOUT SMARTPHONE PRIVACY AND SECURITY** " is a bonafide work carried out by Mr. Rahul Sharma of MBA 2012-14 and submitted to Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42 in partial fulfillment of the requirement for the award of the Degree of Masters of Business Administration.

Ms .Meha Joshi — Prof. P. K. Suri

Assistant Professor — HOD, DSM

Place: Delhi

Date:

Declaration

I hereby declare that the project entitled ""**A STUDY ON CONSUMER PERCEPTION AND AWRENESS ABOUT SMARTPHONE PRIVACY AND SECURITY**" submitted for the MBA Degree is my original work and the project has not formed the basis for the award of any degree, associate ship, fellowship or any other similar titles. It is the result of the project carried out by me under the guidance and supervision Ms. Meha Joshi, Assistant Professor, Delhi School of Management.

I further declare that I or any other person has not previously submitted this project report to any other institution/university for any other degree/ diploma or any other person.

Rahul Sharma

2k12/MBA/50

Place:

Date

ACKNOWLEDGEMENT

I gratefully acknowledge the following people who gave me considerable help and support in making this project report

I would like to express my immense gratitude to mentor guide **Ms. Meha Joshi**, Assistant Professor, Delhi School of Management for her involvement in the project and the regular advices that helped me refine the project as I went along a reality. I really appreciate her continuous guidance and motivation and for helping in whatever capacity she could at various stages in the project. I am indebted to her for her consistent support, for making arrangements, facilitating the study and giving critical inputs and taking time out for me from her busy schedule

I express sincere thanks to Prof P.K. Suri, Head of Department, Delhi School of Management, DTU for providing me the best possible help .I am also thankful to all the faculty members of Delhi School of Management, Delhi Technological University, Delhi.

Rahul Sharma

2K12/MBA/50

MBA 2ND YEAR

DSM,DTU,Delhi

INDEX

Executive Summary

India is the third largest smartphone market place for the mobile device manufacturers. This is mainly attributed to the fact that india has a large population and smartphones have gained wide adoption even by those who do not take advantage of full potential of their smartphone.

Smartphones have been a source of not only connection with the rest of the world but also as the source of instant information. Many people especially the young generation in india use their phones to enjoy multimedia content and at the same time do office work more than ever before.

But what the people are not aware of is how their smartphone actually using their personal information to send it to government as well the advertisers for variety of purposes. India in particular is a place where people have a notion that government can never exploit people with their sensitive information whereas people around the world(where smartphone adoption is high) are extremely critical of their government as far as this is concerned

This has formed the basis for this project as it was specially targeted towards the young Indian customer as to what does he think about his security and privacy rights. Also, the survey done as a part of this project tries to find out awareness among people regarding their security and privacy

Overall the study provides a comprehensive look around difference in consumer opinion when they don't really know how they are being tracked by government and private players.

The survey showed some key characters of Indian people as it showed that they do not take care of their smartphone privacy and security and also their carelessness towards government and private players alike that they have mixed opinion when sharing information with these parties

SMARTPHONE LANDSCAPE IN INDIA

In a matter of five short years, the mobile landscape in India has transformed from voice and text-based handsets that were finding their way in the remotest corners of the country and in the hands of the most unlikely users, to a market that is talking apps, augmented reality, different kinds of OS and versions of Android, iPhone, BlackBerry and the likes -- in all making India a nation that goes to sleep, and wakes up, with a handset every single day. India is one of the hottest mobile markets at present given the sheer number of handsets and subscribers in the market. The Telecom Regulatory Authority of India (TRAI) has put active mobile connections of 91.35 crore (913.49 million) in July 2012

The worldwide smartphone market reached yet another milestone, having shipped one billion units in a single year for the first time. According to the International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker, vendors shipped a total of 1,004.2 million smartphones worldwide, up 38.4% from the 725.3 million units in 2012. This aligns with IDC's most recent forecast of 1,010.4 million units, making for a difference of less than 1%. Smartphones accounted for 55.1% of all mobile phone shipments in 2013, up from the 41.7% of all mobile phone shipments in 2012. In the fourth quarter of 2013 (4Q13), vendors shipped a total of 284.4 million smartphones worldwide, up 24.2% from the 229.0 million units shipped in 4Q12.

India stood out this quarter with smart phone shipments there growing the fastest of the major markets by 129% to hit 9.0 million and make it the world’s third largest smart phone market.

Worldwide smart phone shipments by country Q2 2013

Country	Q2 2012 shipments (million)	Q2 2013 shipments (million)	Growth
Total	**158.3**	**238.1**	**50%**
People's Republic of China (mainland)	42.3	88.1	108%
United States	24.2	32.9	36%
India	3.9	9.0	129%
Japan	6.9	8.6	25%
UK	5.5	7.4	34%
Others	75.4	92.1	22%

Source: Canalys estimates, © Canalys

Given that a bulk (78%) of the phone market in India still consists of feature phones, 2014 is likely to witness a similar explosive growth in smartphone adoption. According to a UK based research agency Media cells , Indian consumers are likely to buy 225 million smartphones in 2014, making India the second biggest market behind China, where consumers will buy almost 283 million smartphones. In comparison, mature markets like the US are witnessing slower growth. According to Media cells, around 89 million smartphones will be sold in the US in 2014.

With smartphones in range of INR 4000 – 50,000, cheap data plans and availability of mobile ready regional content and of course, easy to download free apps, India is considered to be one of the top ranking countries across App stores such as Apple store, Google Play(Rank 3), Nokia (Rank 1), Slide me(Rank 1), and Mobango(Rank 1).

With Android getting its second biggest user base from India, the most popular mobile operating platforms in India are Android, iOS, Blackberry and Windows Phone platform. Also, Amazon has entered the mobile app market in India recently.

Considering the fact that, 52% of the mobile app audience comes from an age group of 18-24, apps that are used widely by Indians are Google map, WhatsApp, and others. Also the hanuman chalisa app is a widely downloaded by the consumers of India.

Internet trends in India

In a span of four years (2008-2012) India added 88 Million internet users reaching to total of 137 Million internet, growing 26% YoY

In 2013, there are 67 million smartphone subscribers, which is 6% of the total subscribers in India, growing at the rate of 52% YoY

More than 50% of Indians share almost everything or most things online in comparison to 15 % in US and 24% Globally.

THE GROWTH OF MOBILE MALWARE

Mobile malware continues to grow at an exponential pace and remains the most popular hacking Technique for devices. Overall, the growth of mobile malware continues to accelerate as the number of mobile users significantly increases. This growth demonstrates a substantial level of maturity with what has become a steady flow of new threats entering the Market each quarter. In March of 2013, the Juniper MTC identified a 614 percent increase in malware across all platforms as compared to the same time period the previous year. Total mobile malware samples across all platforms increased from 38,689 at the end of the first quarter 2012 to 276,259 at the end of the first quarter in 2013.

LITERATURE REVIEW

SECURITY AND PRIVACY RISKS TO SMARTPHONE USERS

Data on a typical smartphone has:

- *corporate & personal e-mail*
- *contacts (phone, sometimes email, sometimes also physical address)*
- *bank info*
- *instant message logs*
- *Pictures*
- *Videos*
- *Credit card info*
- *Location & GPS data*
- *Health info*
- *Calender & schedule information*
- *Username/password info for other systems*

Overall, the security and privacy risks can be identified as:

No.	Title	Risk	Description
1	Data leakage resulting from device loss or theft	High	The smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.
2	Unintentional	High	The smartphone user unintentionally discloses

	disclosure of data		data on the smartphone.
3	Attacks on decommissioned smartphones	High	The smartphone is decommissioned improperly allowing an attacker access to the data on the device.
4	Phishing attacks	Medium	An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.
5	Spyware attacks	Medium	The smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.
6	Network Spoofing Attacks	Medium	An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.
7	Surveillance attacks	Medium	An attacker keeps a specific user under surveillance through the target user's smartphone.
8	Diallerware attacks	Medium	An attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.
9	Financial malware attacks	Medium	The smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or

			subverting online banking or ecommerce transactions.
10	Network congestion	Low	Network resource overload due to smartphone usage leading to network unavailability for the end-user.

1. **Data leakage resulting from device loss or theft**

The smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.

77Smartphones, being both valuable and pocket-sized, are likely to be stolen or lost. In a recent UK government survey, 2% reported their mobile phone was stolen last year. If data on the smartphone memory or its removable media is not sufficiently protected (by encryption) then an attacker can access that data.

Smartphones often contain valuable information such as credit card data, bank account numbers, passwords, contact data, and so on. They are often the user's primary repository of personal data because they are carried around all the time and are always available. Users sometimes protect sensitive information by storing it in an obfuscated form (see example below). Business phones often contain corporate emails and documents and may contain sensitive data.

2. **Unintentional disclosure of data**

The smartphone user unintentionally discloses data on the smartphone.

Users are not always aware of all the functionality of smartphone apps. Even if they have given explicit consent, users may be unaware that an app collects and publishes

personal data trace users and so allow, for example, stalking, robbery or the hijacking of trucks containing valuable goods.

A fundamental underlying vulnerability is the difficulty of collecting meaningful consent for the processing of all the personal data available on a smartphone. Certain types of data collection naturally lend themselves to integration with user consent, without having to assume the persistence of a decision. For example, file upload involves the user in selecting the file and thus giving consent (to that file being uploaded) as an integral part of the process. Other types of data are more problematic and location data is a good example, as it is not feasible for the user to have to consent every time a new location is disclosed. Location data, for example, is often used in social networks – in messages or uploaded photo metadata, in augmented reality apps, micro-blogging posts, etc. this *Most apps have privacy settings for controlling how and when location data is transmitted, but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the privacy setting to prevent*.

3. Attacks on decommissioned smartphones

The smartphone is decommissioned improperly allowing an attacker access to the data on the device.

Due to a growing awareness of identity theft many people and organizations now destroy or wipe computer hard drives before decommissioning. However, the same thing is not yet happening with smartphones. At the same time, more and more devices are being recycled. According to market analysts ABI Research, by 2012 over 100 million mobile phones will be recycled for reuse each year. As previously mentioned, smartphones contain large amounts of sensitive information which may be valuable to an attacker. They are an increasingly attractive target for ‘smartphone dumpster divers’.

4. Spyware attacks

The smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.

The amount of personal data, sensitive documents and credentials stored and processed by smartphones makes them an interesting target for spyware. Furthermore, smartphones provide covert channels through which data may be disclosed (by an application) to an attacker. Even when it seems there is a legitimate need for an app to send data over a particular channel, the permission model of smartphones is not always granular enough to protect users against abuse. For example, a weather app may ask permission to use location data and to connect to the Internet, which seems legitimate (to get fresh location-based weather data). The app may however abuse this permission by sending location-data to advertisement servers for marketing purposes.

Furthermore, data access by apps is sometimes exempt from explicit user permissions. For example, in iOS, the address book is accessible to all apps. No special status is given to the user's own contact details in the address book, meaning that, apart from the large amounts of personal data this exposes, the user's own phone number is also accessible, which can be used for unsolicited marketing. Another important vulnerability is the fact that on the iPhone the keyboard cache is accessible to all apps; although this does not include sensitive information such as passwords, it does contain a lot of private information.

5. Network Spoofing Attacks

An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.

Rogue WiFi hotspots and Bluetooth devices can be used to intercept and tamper with the network communication to the smartphone. Rogue Internet gateway names may be configured on the smartphone by a malicious SMS configuration message. In this attack, a spoofed service configuration SMS is used to change the default access point used by the phone. A rogue WiFi hotspot or other spoofed network nodes can be used as a means to carry out several other attacks, e.g. phishing, SSL downgrade attacks, eavesdropping, etc (making it less likely using 3G networks).

Theoretically speaking, such attacks should be detectable by the user. However, in practice most users do not pay attention to trust cues such as SSL certificates or whether a site uses SSL. For smartphone users the risk is even higher because security indicators (such as a ‘trusted SSL connection’ indicator) are harder to find or missing on smartphones.

For smartphone users the risk is even higher because security indicators (such as a ‘trusted SSL connection’ indicator) are harder to find or missing on smartphones.

6. **Surveillance attacks**

An attacker keeps a user under surveillance through the user’s own smartphone.

Smartphones can be used to keep a targeted individual under surveillance. Smartphones contain multiple sensors such as a microphone, camera, accelerometer and GPS. This, combined with the possibility of installing third-party software and the fact that a smartphone is closely associated with an individual, makes it a useful spying tool.

Given short-term physical and logical access to a device, it is possible to install comprehensive spying tools on it. Sometimes the user can be tricked into helping the attacker by installing malicious apps (see example below). There are also already several examples of legitimate software, whose express purpose is to allow an attacker to keep the mobile user under surveillance. Furthermore, even tools that are not designed for spyware may be configured covertly to allow for tracking.

The GPS sensor deserves particular attention in this regard since it is a source of highly sensitive personal information – e.g. information about when someone is not at home can be useful to burglars. As mentioned above, even a combination of seemingly innocuous sensor data (e.g. magnetic field history) could be used to deduce sensitive information about an individual and their environment.

7. Diallerware attacks

An attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.

Certain smartphone API calls cost the user money, e.g. SMS (including micropayments), phone calls, and data over metered GSM/UMTS. If an attacker can install an app on the user's smartphone, which is able to make such API calls covertly or trick the user into giving consent to their use, they can steal money from the smartphone user. The risk of this attack for consumers is judged as high because they are usually on a more limited budget and are more likely to download rogue apps.

8. Financial malware attacks

The smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.

Financial malware is software specifically designed to steal credentials or perform man-in-the-middle attacks on financial applications or web services. Like PCs, smartphones are also vulnerable to banking malware.

Financial malware may be a key-logger collecting credit card numbers, or it may be more sophisticated and intercept SMS authentication codes to attack online banking applications. Another strategy is for an attacker to submit an app to an app-store, impersonating a real banking app. If users download and use the app, the attacker can mount a man-in-the-middle attack on banking transactions.

Smartphones have been relatively safeguarded from malware (compared to PCs). This may be due to the efforts from platform vendors or simply because traditional PCs still provide an easier and more interesting target for attackers. Nonetheless, malware for smartphones is a serious risk.

Network congestion

Network resource overload due to smartphone usage leading to network unavailability for the end-user.

The uptake of smartphones and mobile Internet increases the risk of network congestion. Network congestion can occur in two ways:

- Signalling overload: always-on smartphone apps are constantly polling the network for updated information. For every bit of data sent, a large number of signalling messages are sent (e.g. keep-alive messages). A typical smartphone generates 8 times more signalling traffic than a laptop with a USB dongle.
- Data capacity overload: Cisco estimates that mobile data traffic will double every year through 2014, increasing 39 times between 2009 and 2014. Mobile data traffic will grow at a compound annual growth rate of 108 percent between 2009 and 2014, reaching 3.6 million terabytes per month by 2014.

To address signalling overload, there are mechanisms that change how often a smartphone switches between idle and active mode, such as the 3GPP Fast Dormancy mechanism.

In terms of data capacity (as opposed to signalling load), solutions such as LTE and WiMAX promise improvements in spectral efficiency, the amount of data that can be transmitted over the air using the same amount of allocated spectrum. At the same time, however, it has been argued that average data demand per network user will outstrip data capacity by 2013 and there are concerns that ‘wireless technology is approaching theoretical limits of spectral efficiency’.

In the longer term in Europe, the risk is reduced by the fact that spectrum is being released by the cessation of analogue TV and 2G services, which is likely to be made available for such applications. However, it is worth noting that while on average, this threat may not be very serious, critical events such as natural disasters which cause a sudden peak in demand (for example the 2010 Eyjafjallajökull volcano eruption) may be create conditions which put data networks used by smartphones under severe strain.

Phishing attacks

An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.

Phishing attacks are a well-known threat for users of traditional PCs. Phishing attacks are actually platform independent, because the attacker does not need to attack the user's device in any way. However, there are a number of reasons why the risk of phishing is important for smartphone users:

- Smartphones have a smaller screen, which means that attackers can more easily disguise trust cues that users rely on to decide on submitting credentials; e.g. cues that show whether the website uses SSL.
- App-stores provide a new way of phishing by allowing attackers to place fake apps in the app-store, disguising them as legitimate apps (such as in the 09Droid case)
- Smartphones provide additional channels that can be used for phishing, e.g. SMS (SMiShing). Users may be less cautious about SMS phishing messages.
- Smartphones are a new type of device and users may not be aware of the fact that phishing is a risk on smartphones as well.

Some Hidden Smartphone Threats

Operating system vulnerabilities

"Some of the main concerns for smartphone and tablet users would be vulnerabilities that might exist in certain parts of the operating system, like browsers or Flash, that can be exploited by going to a certain URL or opening a certain file attachments," said Matthew Dieckman, product line manager for secure remote access at San Jose, Calif.-based SonicWALL. "In this case, the user may be unaware of this tablet or smartphone has been compromised or not."

Vulnerabilities in operating systems are some of the biggest hidden security threats to mobile devices.

"There have also been several vulnerabilities discovered in smartphone operating systems," said Jason Hong, chief technology officer and co-founder of Wombat Security Technologies in Pittsburgh. "For example, in late 2011, some researchers discovered some permission escalation bugs, which would let apps be able to circumvent Android's protection mechanisms and essentially do anything."

Accelerometer data and stolen passwords

"A more subtle vulnerability is with the accelerometer built into all modern smartphones," Hong continued. "Accelerometer data is generally not considered sensitive data. However, researchers have recently developed algorithms that can infer what you are typing on soft keyboards, making it easier to guess one's passwords."

If someone knows your password, he can exploit another hidden threat and remotely install apps onto your phone. "Android smartphones come with remote install functionality," Hong said. "This functionality is useful if your smartphone is stolen, allowing you to add an app to locate your phone after the fact.

"However, remote install is also a potential vulnerability," he added. "If bad guys ever get access to your Google account, they can also access your smartphone meaning that they can install whatever apps they want on your phone, even if they don't have physical access to it."

Hidden Web links

Another security threat found on your smartphone, but not on your PC, is the user's inability to check Web links before clicking on them.

We've been advised for years to always double-check a link's URL, or Web address, by placing the cursor over the hyperlink. If the actual URL doesn't match the destination you think you are heading to, you shouldn't click on anything.

With smartphones, you usually can't read the URL until you click the link and go through to the destination page. That leaves you open to drive-by downloads and other browser-based threats.

While it certainly isn't convenient to do so, it's safer to type the actual URL into the browser address bar yourself, even if you feel you can trust the link or the sender.

Suspicious apps

Speaking of trust, Android users are often warned against downloading apps from third-party websites, since they theoretically won't be screened as thoroughly as apps from the official Android Market. The truth is murkier. Where we get apps is in our control, but how well the apps are vetted is not.

"Google does not do a good job vetting apps," said Denis Maslennikov, senior malware analyst with Kaspersky Lab's global research and analysis team in Moscow. "Getting apps from [the] Android Market is safer, but they aren't going to be 100 percent secure. It is still possible you'll download an app with malware."

"Hackers are creating a lot of fake apps in the hopes of tricking people into installing them," Hong said. "These fake apps might be ones that pretend to be a legitimate one, in the hopes of getting your username and password.

"For example, criminals have created a fake Netflix app, fake mobile banking apps and fake anti-virus apps. These fake apps might also be a free version of a for-pay app, which the criminals have modified to contain malware."

Hidden logging software

This includes software, such as the recently discovered CarrierIQ, that's secretly installed by the smartphone manufacturer or cellular carrier.

"Depending on [the] smartphone, users may be able to run detection software to identify if logging software is installed. However, it's not always possible to disable [it]," said Daniel Ford with Toronto-based security firm Fixmo.

Hostile operator networks

Smartphones are essentially at the mercy of the cellular networks to which they connect. A hostile operator network, which can be set up with a cellular minitower costing a few thousand dollars, can inject undetected software updates into a smartphone, and also install spy software to steal data. This is especially a problem in untrustworthy locations in Eastern Europe.

Rogue SMS messages

Believe it or not, specially crafted text messages can inject code into your phone. So the bad guys send text messages loaded with backdoor Trojans, or they send them with malicious links.

In some cases, the poisoned SMS messages are stealing information off your phone. In other cases, they are using your phone to text-spam your contact list, which can cost you a lot of money if you have a limited texting plan.

Malicious QR codes

This is a relatively new threat. QR codes those two-dimensional barcodes that look like a robot's fingerprint are growing in popularity, as more companies are using them to attract customers for special deals or more information on a product. You're supposed to scan them using your smartphone's camera, then open them up with an app which will bring you to a promotional website.

Not surprisingly, the bad guys have gotten in on the act, and are developing QR codes that take smartphone users to a malicious website. You have no way of knowing this is happening until it's too late.

CONCERN WITH ONLINE SHOPPING

Fraud and security concerns

Given the lack of ability to inspect merchandise before purchase, consumers are at higher risk of fraud than face-to-face transactions. Merchants also risk fraudulent purchases using stolen credit cards or fraudulent repudiation of the online purchase. However, merchants face less risk from physical theft by using a warehouse instead of a retail storefront.

Secure Sockets Layer (SSL) encryption has generally solved the problem of credit card numbers being intercepted in transit between the consumer and the merchant. However, one must still trust the merchant (and employees) not to use the credit card information subsequently for their own purchases, and not to pass the information to others. Also, hackers might break into a merchant's web site and steal names, addresses and credit card numbers, although the Payment Card Industry Data Security Standard is intended to minimize the impact of such breaches. Identity theft is still a concern for consumers. A number of high-profile break-ins in the 2000s has prompted some U.S. states to require disclosure to consumers when this happens. Computer security has thus become a major concern for merchants and e-commerce service providers, who deploy countermeasures such as firewalls and anti-virus software to protect their networks.

Phishing is another danger, where consumers are fooled into thinking they are dealing with a reputable retailer, when they have actually been manipulated into feeding private information to a system operated by a malicious party. Denial of service attacks are a minor risk for merchants, as are server and network outages.

Quality seals can be placed on the Shop web page if it has undergone an independent assessment and meets all requirements of the company issuing the seal. The purpose of these seals is to increase the confidence of online shoppers. However, the existence of many different seals, or seals unfamiliar to consumers, may foil this effort to a certain extent.

Product delivery is also a main concern of online shopping. Most companies offer shipping insurance in case the product is lost or damaged. Some shipping companies will offer refunds or compensation for the damage, but this is up to their discretion.

Lack of full cost disclosure

The lack of full cost disclosure may also be problematic. While it may be easy to compare the base price of an item online, it may not be easy to see the total cost up front. Additional fees such as shipping are often not be visible until the final step in the checkout process. The problem is especially evident with cross-border purchases, where the cost indicated at the final checkout screen may not include additional fees that must be paid upon delivery such as duties and brokerage. Some services such as the Canadian based Wishabi attempts to include estimates of these additional cost,[29] but nevertheless, the lack of general full cost disclosure remains a concern.

Privacy

Privacy of personal information is a significant issue for some consumers. Many consumers wish to avoid spam and telemarketing which could result from supplying contact information to an online merchant. In response, many merchants promise to not use consumer information for these purposes,

Many websites keep track of consumer shopping habits in order to suggest items and other websites to view. Brick-and-mortar stores also collect consumer information. Some ask for a shopper's address and phone number at checkout, though consumers may refuse to provide it. Many larger stores use the address information encoded on consumers' credit cards (often without their knowledge) to add them to a catalog mailing list. This information is obviously not accessible to the merchant when paying in cash or through a bank (money transfer, in which case there is also proof of payment).

CONCERN WITH SOCIAL MEDIA NETWORKS

Social networking sites vary in the levels of privacy offered. For some social networking sites like Facebook, providing real names and other personal information is encouraged by the site(onto a page known as a ‘Profile‘). These information usually consist of birth date, current address, and telephone number(s). Some sites also allow users to provide more information about themselves such as interests, hobbies, favorite books or films, and even relationship status. However, there are other social network sites, such as Match.com, where most people prefer to be anonymous. Thus, linking users to their real identity can sometimes be rather difficult. Nevertheless, individuals can sometimes be identified with face re-identification. Studies have been done on two major social networking sites, and it is found that by overlapping 15% of the similar photographs, profile pictures with similar pictures over multiple sites can be matched to identify the users.

For sites that do encourage information disclosure, it has been noted that majority of the users have no trouble disclosing their personal information to a large group of people.In 2005, a study was performed to analyze data of 540 Facebook profiles of students enrolled at Carnegie Mellon University. It was revealed that 89% of the users gave genuine names, and 61% gave a photograph of themselves for easier identification. Majority of users also had not altered their privacy setting, allowed a large number of unknown users to have access to their personal information (the default setting originally allowed friends, friends of friends, and non friends of the same network to have full view of a user‘s profile). It is possible for users to block other users from locating them on Facebook, but this must be done by individual basis, and would therefore appear not to be commonly used for a wide number of people. Most users do not realize that while they make use of the security features on Facebook the default setting is restored after each update. All of this has led to many concerns that users are displaying far too much information on social networking sites which may have serious implications on their privacy. Facebook was criticized due to the perceived laxity regarding privacy in the default setting for users.

Social network security and privacy issues result from the astronomical amounts of information these sites process each day. Features that invite users to participation—messages, invitations, photos, open platform applications and other applications are often the avenues for others to gain access to a user's private information. In the case of Facebook. Adrienne Felt, a Ph.D. candidate at Berkeley, made small headlines last year when she exposed a potentially devastating hole in the framework of Facebook's third-party application programming interface (API). It made it easier for people to lose their privacy. Felt and her co-researchers found that third-party platform applications on Facebook are provided with far more user information than it is needed. This potential privacy breach is actually built into the systematic framework of Facebook. Unfortunately, the flaws render the system to almost indefensible. "The question for social networks is resolving the difference between mistakes in implementation and what the design of the application platform is intended to allow," said David Evans, Assistant Professor of Computer Science at the University of Virginia. Moreover, there is also the question of who should be hold responsible for the lack of user privacy? According Evan, the answer to the question is not likely to be found, because a better regulated API would be required for Facebook "to break a lot of applications, [especially when] a lot of companies are trying to make money off [these] applications." Felt agrees with her conclusion, because "there are marketing businesses built on top of the idea that third parties can get access to data and user information on Facebook."

MAJOR PLAYERS RESPONSIBLE FOR SECURITY AND PRIVACY OF MOBILE DEVICES

ROLE OF APPLICATION DEVELOPERS

Application Developers

The application developers should:

1. Have a privacy policy and make sure it is easily accessible through the application stores.

2. Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing with third parties sensitive information, such as financial, health, or children's data, where the platforms have not already provided such disclosures and obtained such consent.

3. Improve coordination and communication with advertising networks and other third parties, like analytics companies, that provide services for applications so the application developers can provide accurate disclosures to consumers. Application developers often integrate third-party code to facilitate advertising or analytics within an application with little understanding of what information the third party is collecting and how it is being used. Application developers need to better understand the software they are using through improved coordination and communication with advertising networks and other third parties.

4. Consider participating in self-regulatory programs, trade associations, and industry organizations, which can provide guidance on how to make uniform, short-form privacy disclosures.

Advertising Networks and Other Third Parties

According to the Mobile Privacy Disclosures Report, advertising networks and other third parties should:

1. Communicate with application developers so that the developers can provide truthful disclosures to consumers.
2. Work with platforms to ensure effective implementation of Do Not Track for mobile.

Application Developer Trade Associations

Application developer trade associations, together with academics, usability experts, and privacy researchers can:

1. Develop short form disclosures for application developers.
2. Promote standardized application developer privacy policies that will enable consumers to compare data practices across applications.
3. Educate application developers on privacy issues.

Mobile Security Guidance for Application Developers

Encourages application developers to aim for reasonable data security and evaluate the application ecosystem before development. This guide also includes the following tips:

1. Make someone responsible for data security.
2. Take stock of the data collected and maintained.
3. Understand the differences between mobile platforms.
4. Do not rely on a platform alone to protect users.
5. Generate credentials securely.
6. Use transit encryption for user names, passwords, and other important data.
7. Use due diligence on libraries and other third-party code.
8. Consider protecting data stored on a user's device.
9. Protect servers.

ROLE OF OPERATING SYSTEM IN SECURITY AND PRIVACY

iOS security

Before the arrival of Android, iPhones were smartphone ‘royalty’ and the combination of popularity, and the interest of some users in 'jailbreaking' their devices meant that cybercriminals had a good reason to be interested. However, when kept within the realms of standard usage, Apple has provided a fairly locked-down and safe ecosystem to its customers.

Apps – the primary way of getting malware onto any device – are duly vetted before being allowed into the App Store, and the fact that Apple's app submission process is stringent and well-known to take a little time means that apps might be expected to be checked and checked again. This approach seems to have served Apple well so far, with the first report of App Store based malware coming in June 2012 (an app called “Find and call”).

A second find in the App store in July 2012 was a worm posing no threat to iOS or Mac OS systems, but potentially harmful to Windows systems. This worked on the basis that many users connect iPhones to Windows systems running iTunes.

Apple's presumably long future in the mobile market means it will continue to attract unwanted attention to both jailbroken and non-jailbroken devices, although it has kept the door mostly well locked to date.

Since its initial release, iOS has been subject to a variety of different hacks centered around adding functionality not allowed by Apple. Prior to the 2008 debut of the native iOS App Store, the primary motive for jailbreaking was to install third-party native applications, which was not allowed by Apple at the time. Apple claimed that it will not release iOS software updates designed specifically to break these tools (other than applications that perform SIM unlocking); however, with each subsequent iOS update, previously un-patched jailbreak exploits are usually patched.

Since the arrival of Apple's native iOS App Store, and—along with it—third-party applications, the general motives for jailbreaking have changed. People jailbreak for

many different reasons, including gaining filesystem access, installing custom device themes, and modifying the device SpringBoard. On some devices, jailbreaking also makes it possible to install alternative operating systems, such as Android and the Linux kernel. Primarily, users jailbreak their devices because of the limitations of iOS. It should be noted that depending on the method used, the effects of jailbreaking may be permanent, or can be restored to the original state.

This does not mean that iOS is more secure than Android. In fact, 2012 saw the first confirmed instance of a suspicious mobile application being distributed from both Google Play and the Apple App Store. Kaspersky Lab wrote in July about the Russian language app “Find and Call” which downloaded users’ address books and sends SMS spam to them. 6 Further, enterprises and consumers using Apple devices are not afforded the choice of security solutions to protect their devices. Apple device

security is handled exclusively by Apple, with no insight onmalicious application statistics and detection capabilities made available to the public. This forces consumers and enterprises to put all of their mobile security “eggs” in one basket, so to speak. Android, on the other hand, has seen significant innovation in security products available to users

Android security

Android is currently the most popular mobile operating system worldwide, but it's not just this which makes it likely to be the biggest target for malware makers. The nature of its open source ecosystem, and a large and interested community, opens devices up to rooting and sideloading, both of which come with their own hazards and potential security issues

For its part, Google is trying to add layers of security without restricting its users. The introduction in early 2012 of 'Bouncer' - the server-level security tool used to check apps in the Play Store - added some peace of mind. That was until it was shown that its virtualised testing of apps could be exploited by malware creators.

Android is regularly updated and so can be patched by Google to fix any issues that might be found to cause security problems, although an issue here is that roll-out of updated devices can take some time depending on device and carrier. Google itself is surely looking into its long-term options in helping to keep its users away from harm, yet the numerous security issues to date prove that it is fairly tricky to effectively secure an open ecosystem. Even more so when hardware, network and user variables come into play.

Android applications run in a sandbox, an isolated area of the system that does not have access to the rest of the system's resources, unless access permissions are explicitly granted by the user when the application is installed. Before installing an application, Play Store displays all required permissions: a game may need to enable vibration or save data to an SD card, for example, but should not need to read SMS messages or access the phonebook. After reviewing these permissions, the user can choose to accept or refuse them, installing the application only if they accept. The sandboxing and permissions system lessens the impact of vulnerabilities and bugs in applications, but developer confusion and limited documentation has resulted in applications routinely requesting unnecessary permissions, reducing its effectiveness. Google has now pushed an update to Android Verify Apps feature, which will now run in background to detect malicious processes and crack them down.

The "App Ops" privacy and application permissions control system, used for internal development and testing by Google, was introduced in Google's Android 4.3 release for the Nexus devices. Initially hidden, the feature was discovered publicly; it allowed users to install a management application and approve or deny permission requests individually for each of the applications installed on a device. Access to the App Ops was later restricted by Google starting with Android 4.4.2 with an explanation that the feature was accidentally enabled and not intended for end-users; for such a decision Google received criticism from the Electronic Frontier Foundation. Individual application permissions management, through the App Ops or third-party tools, is currently only posssible with root access to the device.

Research from security company Trend Micro lists premium service abuse as the most common type of Android malware, where text messages are sent from infected phones to premium-rate telephone numbers without the consent or even knowledge of the user.[139] Other malware displays unwanted and intrusive adverts on the device, or sends personal information to unauthorised third parties. Security threats on Android are reportedly growing exponentially; however, Google engineers have argued that the malware and virus threat on Android is being exaggerated by security companies for commercial reasons, and have accused the security industry of playing on fears to sell virus protection software to users. Google maintains that dangerous malware is actually extremely rare, and a survey conducted by F-Secure showed that only 0.5% of Android malware reported had come from the Google Play store.

Google currently uses Google Bouncer malware scanner to watch over and scan the Google Play store apps. It is intended to flag up suspicious apps and warn users of any potential threat with an application before they download it. Android version 4.2 *Jelly Bean* was released in 2012 with enhanced security features, including a malware scanner built into the system, which works in combination with Google Play but can scan apps installed from third party sources as well, and an alert system which notifies the user when an app tries to send a premium-rate text message, blocking the message unless the user explicitly authorises it. Several security firms, such as Lookout Mobile Security, AVG Technologies, and McAfee, have released antivirus software for Android devices. This software is ineffective as sandboxing also applies to such applications, limiting their ability to scan the deeper system for threats.

Android smartphones have the ability to report the location of Wi-Fi access points, encountered as phone users move around, to build databases containing the physical locations of hundreds of millions of such access points. These databases form electronic maps to locate smartphones, allowing them to run apps like Foursquare, Google Latitude, Facebook Places, and to deliver location-based ads. Third party monitoring software such as TaintDroid, an academic research-funded project, can, in some cases, detect when personal information is being sent from applications to remote servers. In August 2013, Google released Android Device Manager (ADM), a

component that allows users to remotely track, locate, and wipe their Android device through a web interface. In December 2013, Google released ADM as an Android application on the Google Play store, where it is available to devices running Android version 2.2 and higher.

The open-source nature of Android allows security contractors to take existing devices and adapt them for highly secure uses. For example Samsung has worked with General Dynamics through their Open Kernel Labs acquisition to rebuild *Jelly Bean* on top of their hardened microvisor for the "Knox" project.

As part of the broader 2013 mass surveillance disclosures it was revealed in September 2013 that the American and British intelligence agencies, the National Security Agency (NSA) and Government Communications Headquarters (GCHQ) respectively, have access to the user data on iPhone, BlackBerry, and Android devices. They are reportedly able to read almost all smartphone information, including SMS, location, emails, and notes. Further reports in January 2014 revealed the intelligence agencies capabilities to intercept the personal information transmitted across the internet by social networks and other popular apps such as Angry Birds, which collect personal information of their users for advertising and other commercial reasons. GCHQ has, according to The Guardian a wiki-style guide of different apps and advertising networks, and the different data that can be siphoned from each. Later that week, the Finnish Angry Birds developer Rovio announced that it was reconsidering its relationships with its advertising platforms in the light of these revelations, and called upon the wider industry to do the same.

The documents revealed a further effort by the intelligence agencies to intercept Google Maps searches and queries submitted from Android and other smartphones to collect location information in bulk. The NSA and GCHQ insist their activities are in compliance with all relevant domestic and international laws, although the Guardian stated "the latest disclosures could also add to mounting public concern about how the technology sector collects and uses information, especially for those outside the US, who enjoy fewer privacy protections than Americans."

MALWARE FOLLOWS MARKETS: ANDROID'S APPEAL

For malware authors

Mobile malware professionals are maximizing their return on investment by targeting Android because of its global market dominance and open platform. Like legitimate businesspeople, malware professionals look to exploit the largest addressable market opportunity.

The complexion of mobile malware has changed drastically in the span of just a few years, following mobile phone adoption and use patterns. Until 2010, most mobile malware targeted Nokia's Symbian operating system and Oracle's Java Platform, Micro edition (Java Me), a widely used mobile device environment that is supported by mobile phones and embedded devices such as TV set-top boxes and printers. Beginning in 2011, the mobile malware landscape changed when the MTC detected a shift in attacks from Symbian to Google's Android mobile operating system. This trend accelerated in 2012 and Q1 of 2013. By March of 2013, the MTC collected 253,304 samples of Android malware, making Android the target of 92 percent of detected threats in the mobile malware arena.

Windows Phone 8 security

With Windows Phone 7 getting off pretty much scot-free in terms of attempted exploits and attacks, you'd be forgiven for thinking that criminals just didn't get around to trying to attack the first Windows Phone OS. Far more likely is that Windows Phone 7 simply didn't prove as popular as iOS and Android, and so malware writers seeking to target the largest-available group of users focused their attention elsewhere.

Windows Phone 8 (WP8) might well be seen in a similar light by cybercriminals. But while mobile security observers are still waiting to see the first case of malware on WP8 appear in the wild, a 16 year-old Indian student named Shantanu Gawde presented an example of a malware-embedded application at November 2012's international Malware Conference, Malcon. Little is known about the specifics of the design, but one thing is

for sure: if Windows Phone 8 becomes a dominant player in the smartphone market cybercriminals will likely pay attention.

Blackberry security

Considered the mobile OS for businesses because of its sure-footed security approach, Blackberry owner RIM has a solid reputation when it comes to securing its customers' devices. In fact Blackberry 7 devices have even been praised for providing excellent corporate security for administrators. But with RIM currently losing traction in the mobile market, and with Apple becoming more and more business-friendly, the security of RIM's ecosystem seems less of an issue than the wait until Blackberry 10 and the question who it will appeal to.

Certainly current Blackberry devices offer a good level of data security, and it seems unlikely that RIM will want to compromise that when it comes to Blackberry 10. An indication of the level RIM are working towards might be taken from the awarding of FIPS 140-2 certification to Blackberry 10. FIPS 140-2 is the (Federal Information Processing Standard), and means that the United States deems the platform fit for federal and government use.

All the mobile operating platforms should:

1. Provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation.

2. Consider providing just-in-time disclosures and obtaining affirmative express consent for other content that consumers would find sensitive in many contexts, such as contacts, photos, calendar entries, or the recording of audio or video content. Providing such disclosure at the time when it matters to consumers, just before the collection of this information by applications, will allow users to make informed choices about whether to allow the collection of this information.

3. Consider developing a one-stop "dashboard" approach to allow consumers to review the types of content accessed by the applications they have downloaded.

4. Consider developing icons to depict the transmission of user data.

5. Promote application developer best practices. For example, platforms can require developers to make privacy disclosures, reasonably enforce these requirements, and educate application developers.

6. Consider providing consumers with clear disclosures about the extent to which platforms review applications before making them available for download in the application stores and conduct compliance checks after the applications have been placed in the application stores.

7. Consider offering a Do Not Track mechanism for smartphone users for allowing consumers to choose to prevent tracking by advertising networks or other third parties as they navigate among applications on their phones.

CERTAIN DISCLOSURES BY GOVERNMENT REGARDING BAD PRACTICES OF APPLICATIONS IN DIFFERENT PLATFORMS

Acc to report funded by privacy commissioner of Canada

Android

- Lookout seems to use a lot of battery power.
- Lookout sends out an ID that is shared with another app (Facebook)
- Facebook sends out an ID that is used by another app (Lookout)
- Shazam reports accurate longs (to within meters)
- TuneIn Radio Pro reports accurate longs unencrypted(to within meters)
- WhatsApp uploads contacts to servers.

BlackBerry

- Didn't capture https on the BB.

iOS

- WhatsApp (free) will continue to upload contacts to their servers, once you have allowed them access, even if you delete and reinstall the app. This may be a problem with how the iPhone handles re-installation of apps. You can however, turn this access off in Settings. When restoring the phone and reinstalling, the app asks for permission again.
- Mix Genius (free) sends out my UDID to ex.Mobmore.com, it is not encrypted over https.
- Mix Genius (free) sends out an ID is used by another app as well (Cut the Rope).
- Cut the Rope Experiments (paid) sends out an ID , this ID is used by another app as well (Mix Genius).
- Cut the Rope Experiments (paid) sends out the MAC address of the phone to a 3rd party.

- TuneIn Radio Pro (paid) asks if it can use location data, if you allow it, the location data is accurate to within a few meters.
- Kick the Buddy (paid) sends out UDID
- Kick the Buddy (paid) sends out Mac Address.
- Pinterest sends out my user name to a 3rd party. My user name is my first and last name.

Windows Phone 7

- The Windows phone logs into http://login.live.com to perform a number of tasks. It sends out my user email in plaintext whenever it does this. This should probably be encrypted.
- Weather: The Weather Channel runs in the background and routinely sends out plaintext logs. This is likely because of its emergency warning feature, but there is no clear (popup) warning that it will continue to do this that would be obvious to a typical user

This shows how different players can use the information in a mobile device for their own personal gains. Therefore a strong lawful system should be in place that should protect the user privacy. This is where the role of government becomes important as they devise the guidelines as to how device data can be used.

OBJECTIVES OF THE STUDY

- *To understand differences in consumer attitudes towards government bodies and private players in sharing their data*
- *To know about customers perception towards service providers and app developers*
- *To study consumer awareness towards his phone and its data*
- *To study customer awareness level about latest threats*
- *To study consumer understanding of different security threats*

RESEARCH METHODOLOGY

The research methodology was included to understand how much importance security and privacy holds in the minds of Indian customer. An online survey was conducted for the research process

PRIMARY DATA

The method of data collection adopted was survey and the sample size is of 99. The target group of primary data collection was young age people as they were expected to be the more frequent user of smartphones and having more awareness about their phones

SECONDARY DATA

As this was a survey based project most of data used is primary. However for the literature of this project report, the data has been sourced from variety of research firms and websites so as to better understand the scenario. Also similar researches which have been done on the customers in the western part of the world have shaped they intent and approach for this project

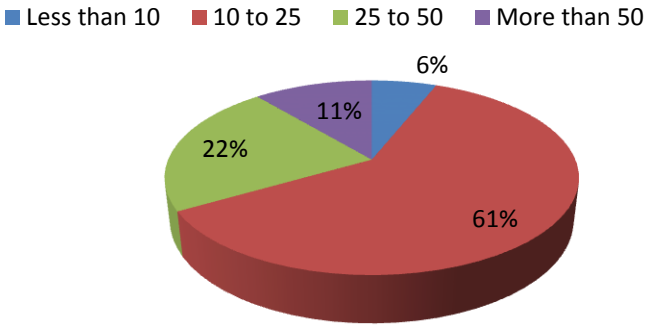
DATA COLLECTION

An online survey was conducted with 99 respondents where they were asked different questions related to security and privacy of their mobile devices. The survey was classified into three parts i.e security, privacy and consumer awareness level. The young age group people were targeted for the study.

SURVEY RESULTS----SampleSize-99

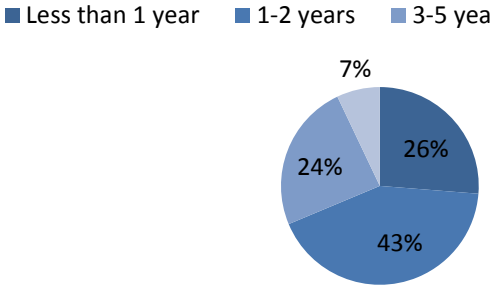
QUESTIONS

Number of applications installed on your phone	Breakup
Less than 10	6
10 to 25	60
25 to 50	22
More than 50	11



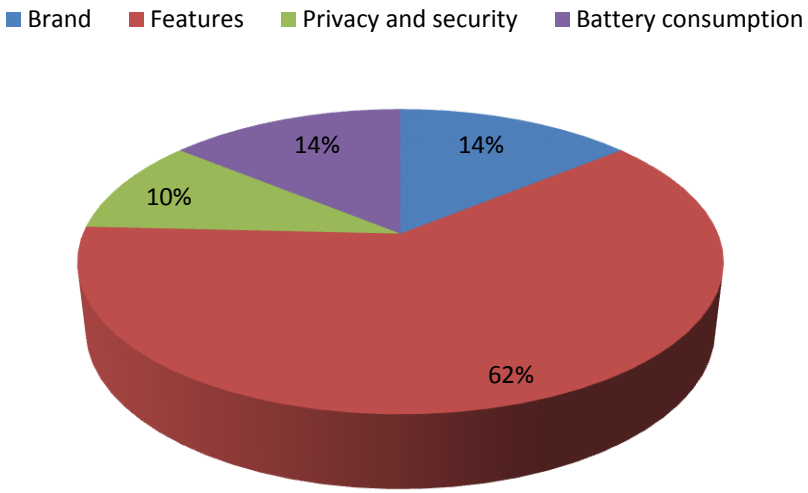
This was an introductory question intended to understand how majority of them use their smartphone and to what extent. The result showed that most of them were moderate user of their smartphone

For how much time you have been using smartphones?	Breakup
Less than 1 year	26
1-2 years	42
3-5 years	24
more than 5 years	7



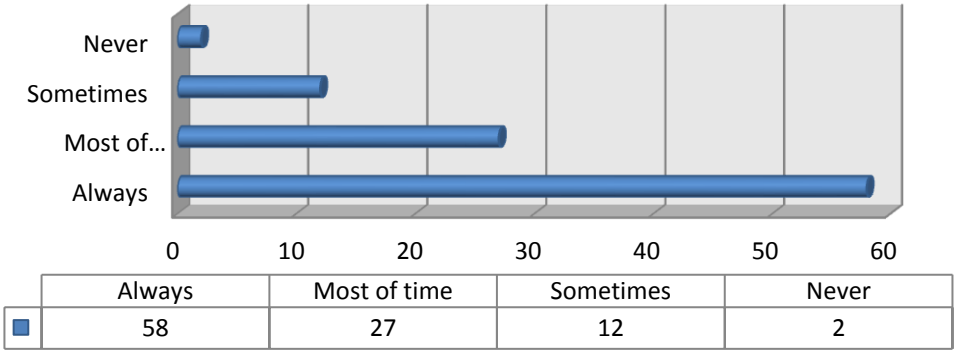
This question was intended to find out breakup of new and old user of smartphones. Results show a good mixture of new as well as old users justifying the growth of this market in India in last 5 years

What is your primary concern while using applications in your smartphone?	Breakup
Brand	14
Features	61
Privacy and security	10
Battery consumption	14

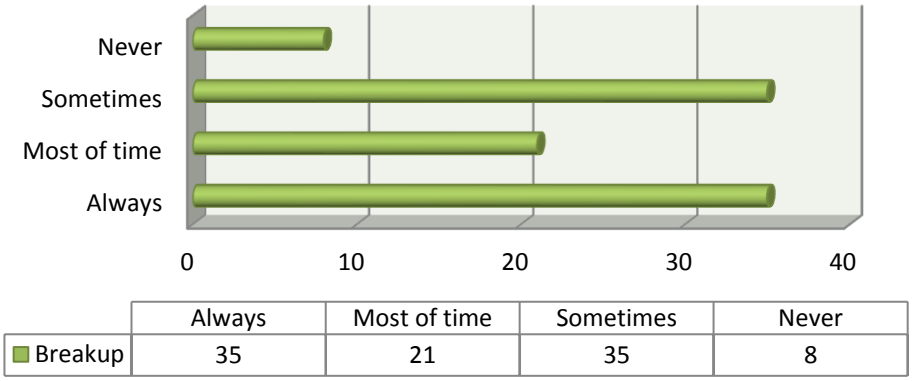


This question intended to find out what the users generally feel about the applications in their phones. The result show that almost 90 percent of people have their concerns in other areas than privacy and security

Are you concerned about your privacy and security whenever you are [Shopping Online]	Breakup
Always	58
Most of time	27
Sometimes	12
Never	2

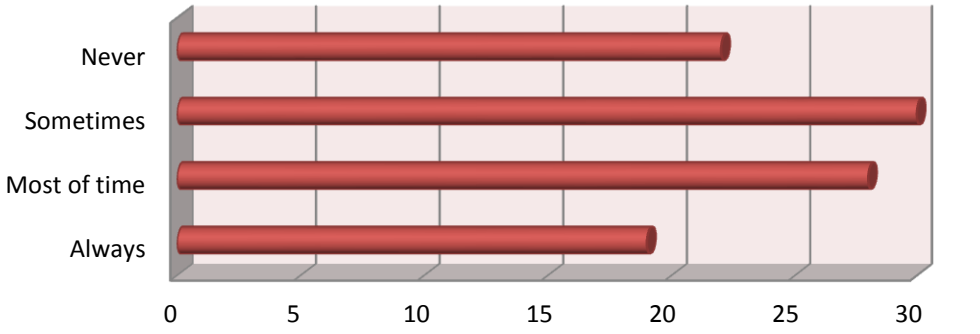


Are you concerned about your privacy and security whenever you are [Social Networking]	Breakup
Always	35
Most of time	21
Sometimes	35
Never	8



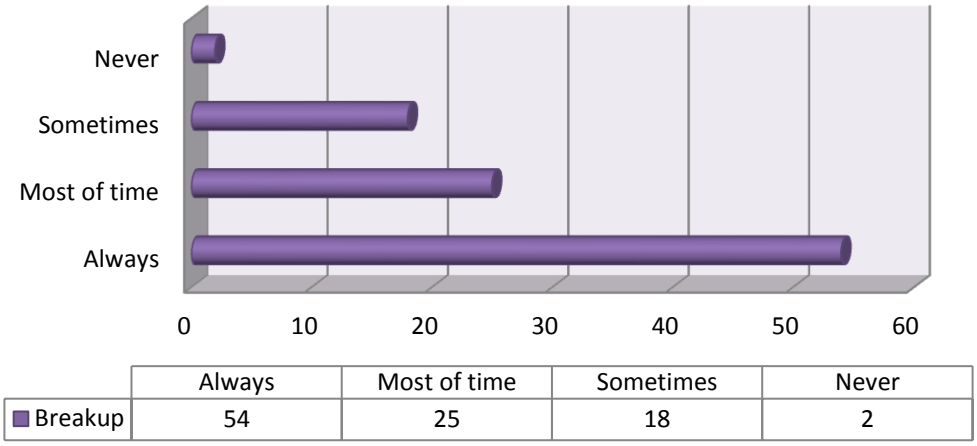
	Always	Most of time	Sometimes	Never
Breakup	35	21	35	8

Are you concerned about your privacy and security whenever you are [Using applications]	Breakup
Always	19
Most of time	28
Sometimes	30
Never	22



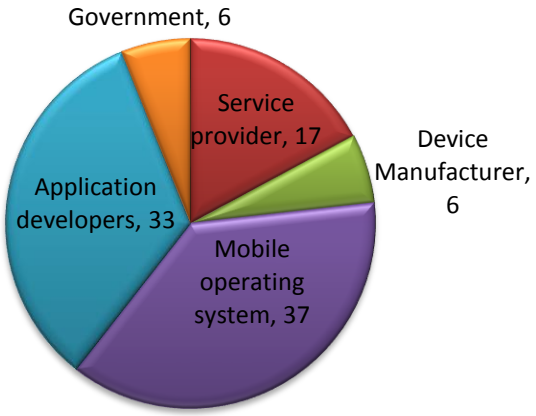
	Always	Most of time	Sometimes	Never
Breakup	19	28	30	22

Are you concerned about your privacy and security whenever you are [Using email]	Breakup
Always	54
Most of time	25
Sometimes	18
Never	2

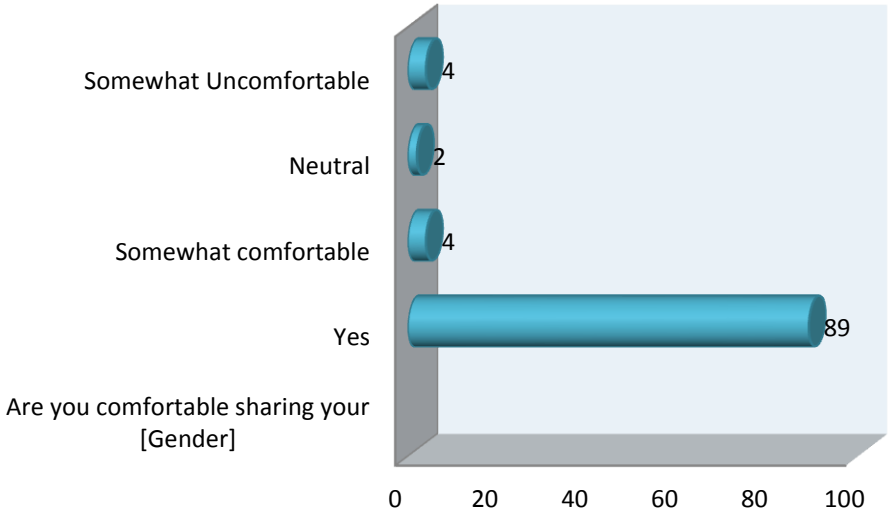


	Always	Most of time	Sometimes	Never
Breakup	54	25	18	2

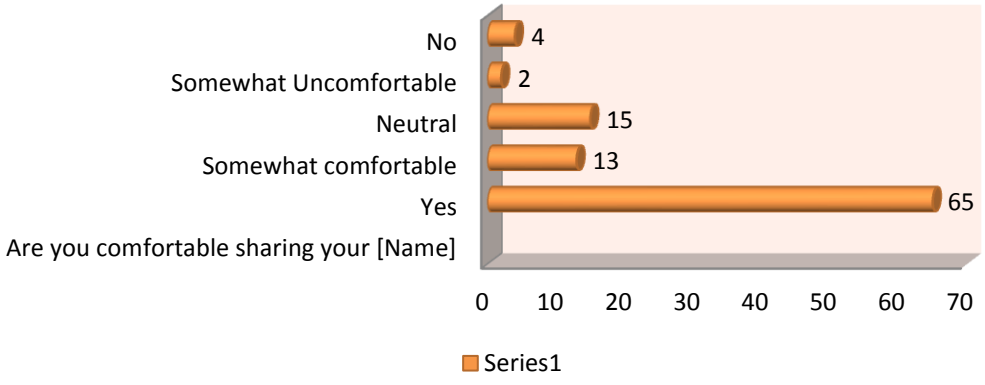
Who do you think is most responsible for your privacy protection besides you?	
Service provider	17
Device Manufacturer	6
Mobile operating system	37
Application developers	33
Government	6



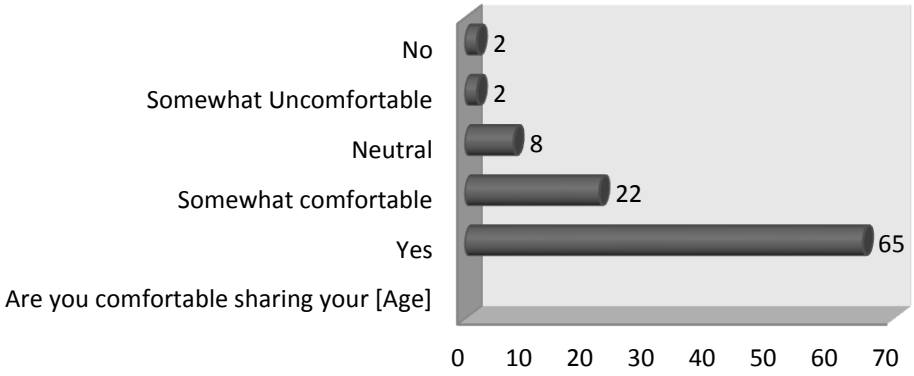
Are you comfortable sharing your [Gender]	
Yes	89
Somewhat comfortable	4
Neutral	2
Somewhat Uncomfortable	4



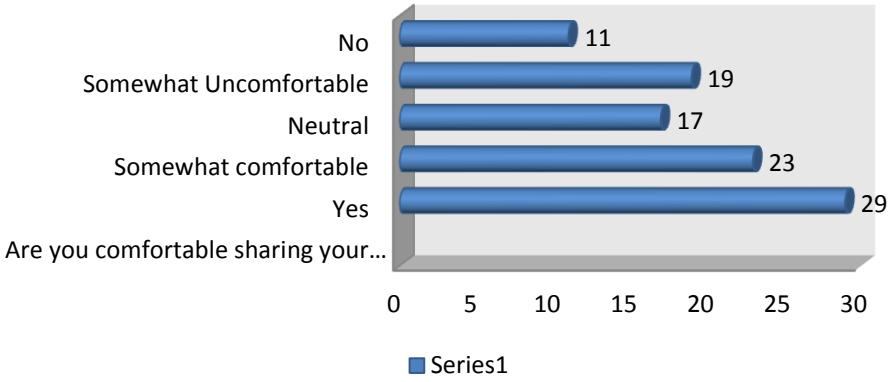
Are you comfortable sharing your [Name]	
Yes	65
Somewhat comfortable	13
Neutral	15
Somewhat Uncomfortable	2
No	4



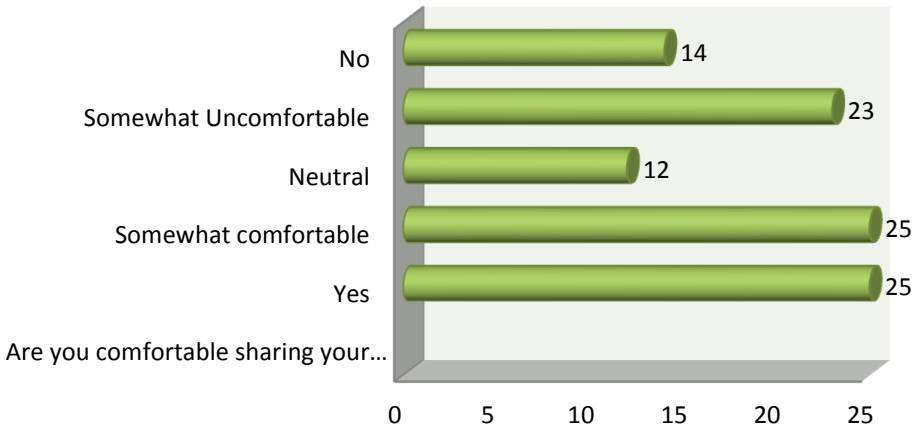
Are you comfortable sharing your [Age]	
Yes	65
Somewhat comfortable	22
Neutral	8
Somewhat Uncomfortable	2
No	2



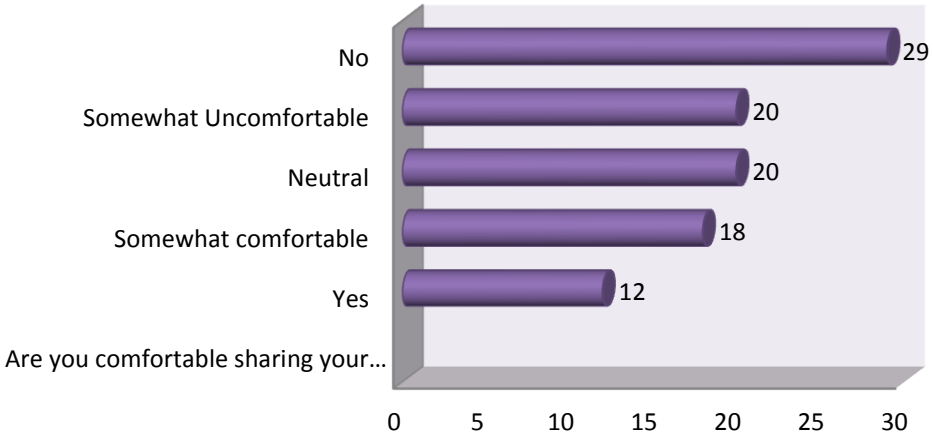
Are you comfortable sharing your [Email]	
Yes	29
Somewhat comfortable	23
Neutral	17
Somewhat Uncomfortable	19
No	11



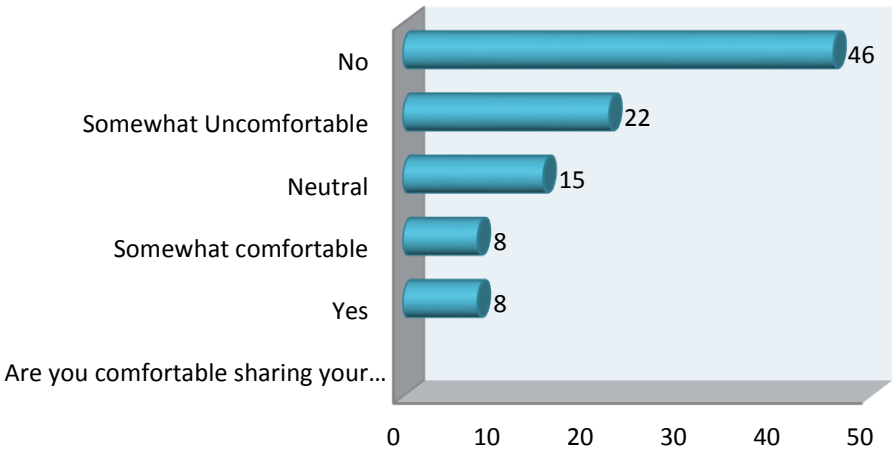
Are you comfortable sharing your [Location]	
Yes	25
Somewhat comfortable	25
Neutral	12
Somewhat Uncomfortable	23
No	14



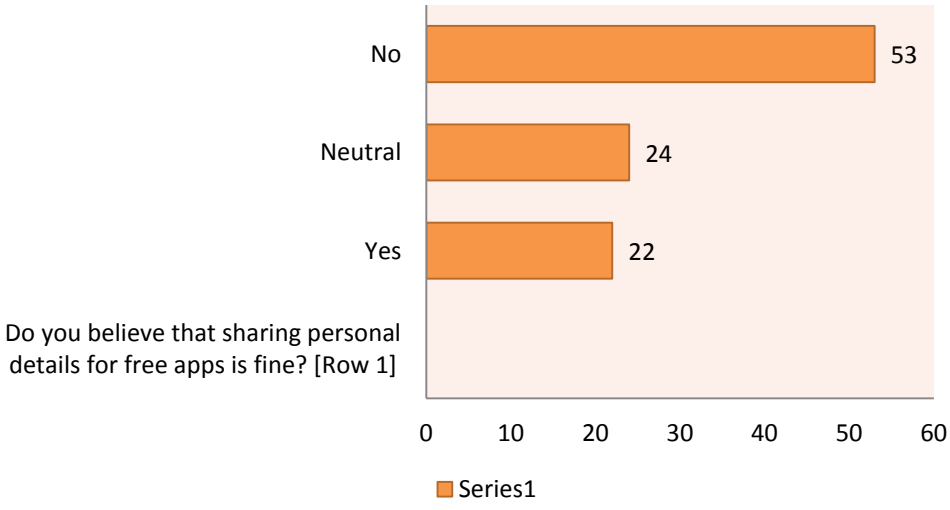
Are you comfortable sharing your [Photos]	
Yes	12
Somewhat comfortable	18
Neutral	20
Somewhat Uncomfortable	20
No	29



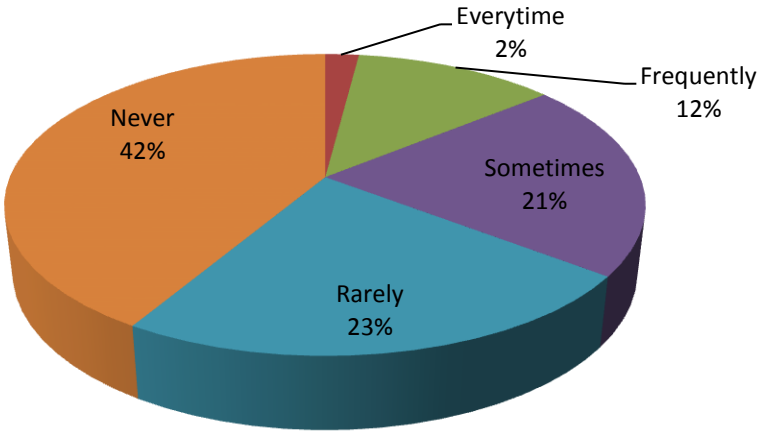
Are you comfortable sharing your [Contacts]	
Yes	8
Somewhat comfortable	8
Neutral	15
Somewhat Uncomfortable	22
No	46



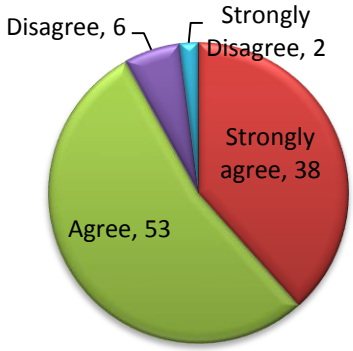
Do you believe that sharing personal details for free apps is fine?	
Yes	22
Neutral	24
No	53



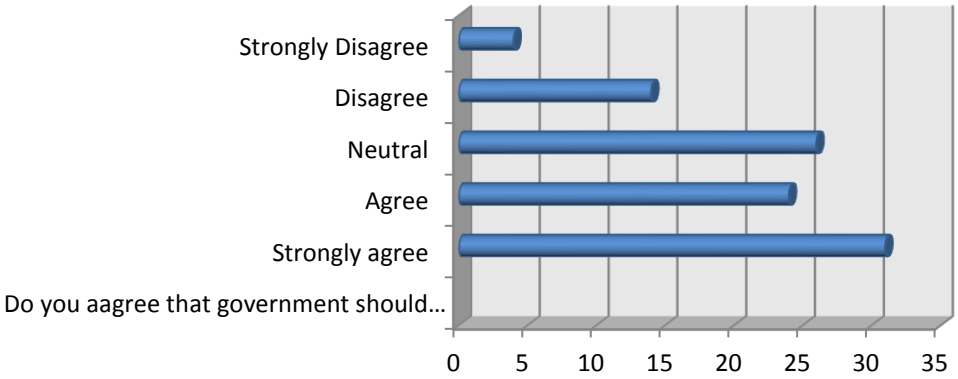
How many times do you read the privacy policy of an application before using it?	
Every time	2
Frequently	12
Sometimes	21
Rarely	23
Never	41



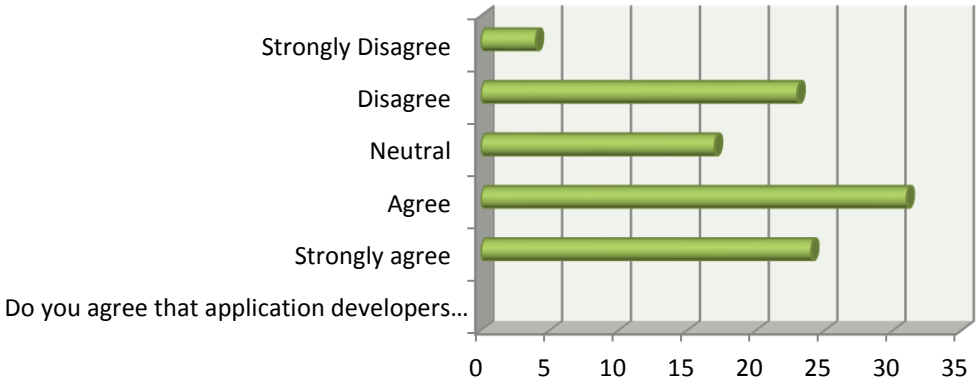
Do you think that government needs to educate people about how and why they are being monitored?	
Strongly agree	38
Agree	53
Disagree	6
Strongly Disagree	2



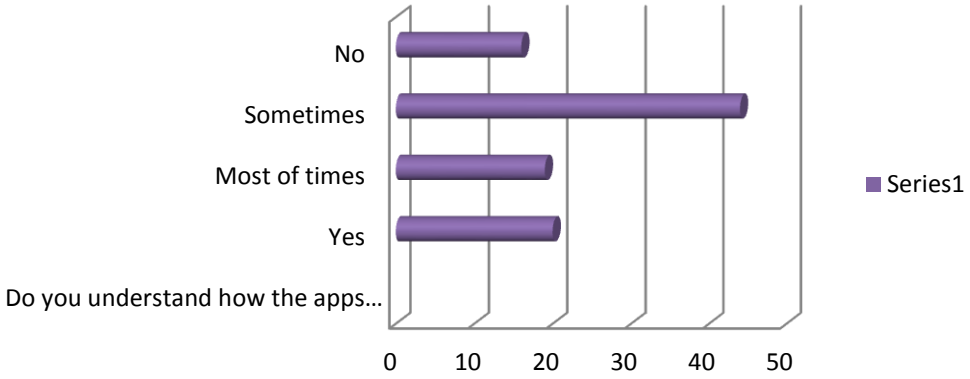
Do you agree that government should monitor people for their own security?	
Strongly agree	31
Agree	24
Neutral	26
Disagree	14
Strongly Disagree	4



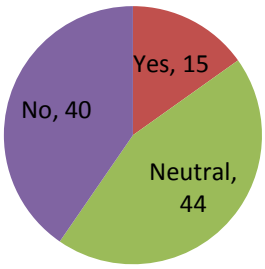
Do you agree that application developers should monitor people to improve their services? []	
Strongly agree	24
Agree	31
Neutral	17
Disagree	23
Strongly Disagree	4



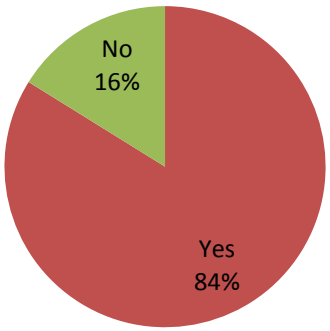
Do you understand how the apps that you have installed in your phone interact with your personal data?	
Yes	20
Most of times	19
Sometimes	44
No	16



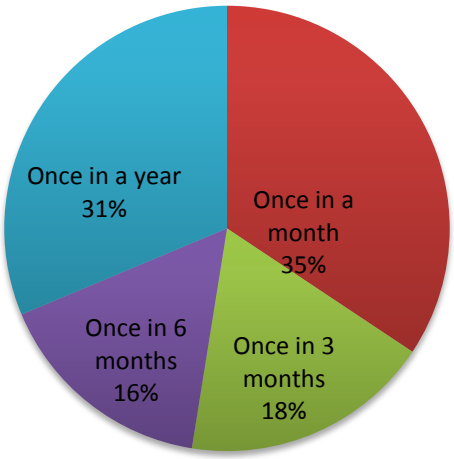
Do you think installing pirated versions of paid apps for personal use is fine?	
Yes	15
Neutral	44
No	40



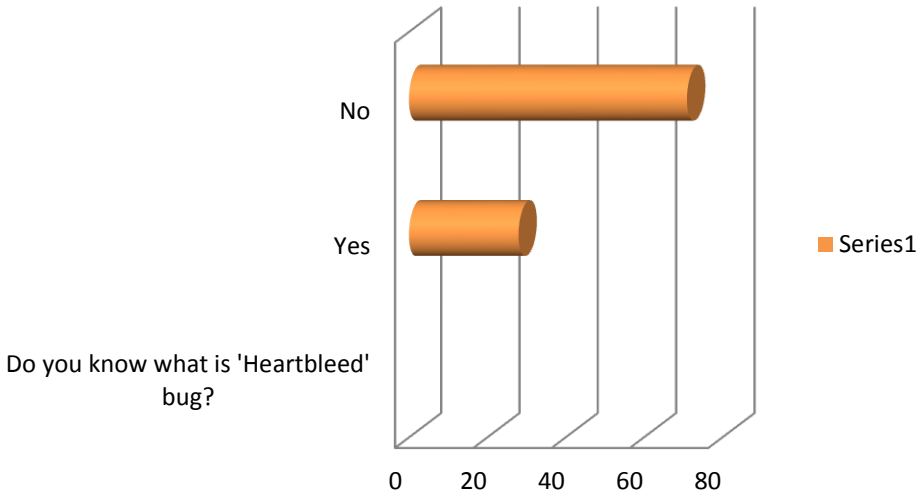
Do you have any secure lock system(password/pattern etc.) on your phone.?	
Yes	83
No	16



How often do you change your passwords?	
Once in a month	34
Once in 3 months	18
Once in 6 months	16
Once in a year	31



Do you know what is 'Heartbleed' bug?	
Yes	28
No	71



CONCLUSION

Key Findings Of the Survey

- Most of the young generation people had started using smartphones in last 2 years.
- Majority of users do not consider privacy and security as the primary concern for an application
- Majority of users are concerned with security while shopping online and emailing but do not show same trend while using applications and social networking
- About 40% user think operating system is responsible for their privacy while 33% think it is application developer
- People are comfortable sharing their name, age, gender and even location but do not want to share photos and contacts
- Even though privacy and security was not a primary concern but 50% people think sharing data for applications is not right.
- About 65% of people have never or rarely read privacy policy of application.
- Most of the people feel that government needs to educate people about privacy and security
- Most of people say they have very little idea as to how they understand data interaction in his phone.
- Only 40% of sample thinks installing paid apps for free is wrong.
- People have basic level of awareness but not advanced level

Overall, the survey showed how unaware and careless Indian young consumer is about their smartphone privacy and security. Although they have basic level of awareness and opinion that government should educate people about this but they themselves do not make any effort in that regard. This is a big threat to the young consumer and this is very well exploited by companies around the world

SOME RECOMMENDATIONS TO KEEP YOUR SMARTPHONE SAFE

Use a PIN/keylock code

There are a number of ways to protect a smartphone. Many new phones offer a “pattern lock” – a personalised shape or pattern that is drawn on the screen to grant access, and this is often faster and less hassle than entering a password. Alternatively a PIN code offers a numeric alternative to a standard password and can also save time. Obviously a password that is easy to guess is less secure – so avoid “1234”, “password” and other common phrases.

A screen lock is useful but won’t stop someone from removing your SIM card and using it on another phone. To prevent this from happening, set up a SIM card lock in the form of a PIN number that will need to be entered when a phone is turned on in order to connect to a network.

Protect sensitive data

While PIN entry and password locks were usually all you’d need to protect mobile phones a few years ago, these days you’re effectively carrying around a miniature computer with its own – often easily removable – storage. Simply preventing someone from being able to turn a phone on isn’t sufficient anymore, as it’s far too easy to retrieve data by simply plugging it into a computer or removing a microSD card.

Protecting sensitive data that may be saved to internal storage is therefore a must, and thankfully there are a number of solutions available. Most smartphone platforms offer software that can encrypt files or folders on a device with industry-standard protection, which means a code must be entered before a file can be viewed or copied. This also goes for information such as passwords, login details, account numbers and other information that may be saved for access to online banks or merchants. Ensuring that this sort of information isn’t easily accessible is obviously important, and it would be wise to install such protection and use it as common practice.

Much of this software is free to download and use and can work effectively with your phone to provide automated and seamless protection, so there's very little hassle involved once it's up and running.

In addition to this sort of software, some security vendors are recommending that sensitive data be stored remotely on secure online servers, rather than on the phone itself. This means that not only is there no physical data on a phone that could be accessed, but in the event of a handheld being lost or stolen it's easy to change the login details for the server or remove the data altogether.

Watch your wireless

Most smartphones now have the option of connecting to wireless networks – be this a router in the office or home, or a wireless hotspot on the move. Opting for wireless is often beneficial for increased speeds or to save on data usage costs, so it's easy to see why many prefer it when available. Any device that's enabled to send data across the airwaves is a potential security concern, but thankfully modern phones are well prepared to help you mitigate this risk.

The first thing to remember is to always switch off a wireless connection when it's not in use. Apart from helping you save on battery power, it ensures that malicious parties can't connect to a device without your knowledge. It's also worth taking a browse through a phone's network security settings as it might be configured to automatically connect to a network when in range. Wireless hotspots and unknown networks are by far the biggest risk when it comes to utilising this connectivity – assuming of course, that any more commonly accessed wireless router in the home or office is sufficiently protected by a pass code.

A (relatively) common threat that pervades unknown wireless networks and hotspots is called the "evil twin" attack. Here a malicious party might be offering access to a wireless connection that looks very much like a legitimate hotspot from a large company. If a user were to inadvertently connect to this "hotspot", they may find

requests for passwords, login details and other information that can then be recorded and used to access their accounts at a later stage. If a little care is taken it's usually not too difficult to spot these attempts, and of course any requests for information that don't seem entirely legitimate and typical should be ignored.

Finally, those who use phones to communicate in a corporate environment should consider the use of a VPN (Virtual Private Network) to set up a secured private network. This allows users to access specific sites and company resources on the move and significantly reduces the risk of potentially sensitive data being intercepted by malicious parties.

Bluetooth

Unlike wireless networking, Bluetooth isn't seen as a potentially risky venture for most mobile users, and the relatively short-range (around 10m) at which it is accessible does mean that it's inherently safer. Attacks do still happen however, and it's important to be aware of the pitfalls of leaving this technology switched on when not in use. Hackers have found ways to remotely access a phone (provided they are within range) and use it to make calls, access data, listen in on conversations and browse the internet.

To prevent this from happening it's a good idea to set default Bluetooth configuration to "non-discoverable" mode by default. This means that users around you who are searching for potential targets won't see your device pop up on their list.It goes without saying that any unknown requests that come through via a Bluetooth connection, such as a request to "pair" with a device or respond to a message from an unknown source should be ignored or declined. Bear in mind that the restrictive range of Bluetooth means that other users or devices must be within this radius in order to connect to your device, and as such busy places such as coffee shops, bars, trains and buses have traditionally been opportunist environments for the Bluetooth hacker.

Caution with applications

Recent press surrounding malware on the Android operating system has reinforced the need to be cautious when downloading applications, and to pay attention to the

requirements this software demands upon install. It's far too easy to simply breeze over these pages in an effort to get the app up and running, but users should exercise caution to ensure that realistic demands are being made on access to various features of a phone, particularly if the software isn't well known. While the Android Market recently succumbed to a malware scare it's generally far safer to use these "official" channels to download applications, and any secured from alternative sources should be treated as a potential risk.

It's also important to exercise caution with respected applications such as popular web browsers, as it's often far too easy to simply accept qualification messages that pop up when you're online. Agreeing to save user details and passwords when logging into websites for future access may be convenient, but makes it very easy for those accessing an unprotected phone to do the same. This is particularly important when it comes to online banks and merchants, as these sites often have bank account details saved automatically under your username and would make it easy for others to make unwanted purchases or transactions.

In addition users should pay attention to any potential security warnings that may be displayed when viewing websites, particularly if accessing them through unknown wireless networks, and not just dismiss these without thought. Web pages that involve the entry of sensitive data such as a username, password or account details should always use encrypted protocols to protect this information. This can be confirmed by the presence of an "s" at the end of "http" at the start of a webpage URL (https://) or a visible padlock icon on the status bar of a browser to confirm that the connection is encrypted. It's a good idea to get into the habit of looking for these when using any websites that have requested personal details.

Rooting your phone

One increasingly popular practice among Android users is "rooting" a phone. This essentially involves modifying the file system to allow users access to read-only files and parts of the operating system that the manufacturer or service provider don't want you to change. Some of the advantages of rooting a phone include the ability to change

or remove read-only applications that you don't want to use, change the boot screen, back up the entire system, run specialised applications and install custom user interfaces and alternative versions of the OS. Rooting is usually only done by "experts", who should therefore be aware of the potential dangers, but if someone offers to root a phone for you while citing the benefits, it's important to be aware of the security risks as well.

Since rooting allows a user access to system-level resources, it also opens these up for potential infection by malware. Part of the reason why this critical data is inaccessible is to protect it from such threats, and while you may benefit from more flexibility in the short term, writers of malicious code can also benefit from full access to your device if it becomes infected. Applications that have requested root access could, for example, record keystrokes entered on an on-screen keyboard, delete or copy data, make phone calls to premium numbers or install "pseudo" applications that look like the real thing, but have ulterior motives in mind.

This may sound like scaremongering, but it just goes to show the importance of being aware of the potential dangers involved with modern smartphones, particularly flexible, open-source platforms like Android.

Back up your data

Discovering that a phone has been lost or stolen is bad enough, but even when discounting the potential damage that could be done by sensitive data getting into the wrong hands, important documents, contacts, messages, appointments and other information could take a long time to replace. Ensuring that regular backups are made is therefore essential, and there are a number of ways to go about it. Most modern phones now allow users to "synchronise" information with a computer or website for productivity or backup purposes. This can include e-mails and contacts with Microsoft Outlook, photos uploaded to online storage or proprietary software supplied by the phone manufacturer to simply backup key data in the event of loss.

Some modern security suites designed for use on mobile devices also offer an automatic backup facility to take the hassle out of doing this manually. There are also a range of services that allow you to automatically backup specific data to an online resource, taking the hassle out of having to connect a phone to a computer. Provided you have a sufficiently healthy data plan, or are connected to a wireless network, this is an excellent way to safeguard against loss.

Security software

Security software can help you avoid many of the potential dangers associated with smartphones and modern suites are tailor-made to address issues that are unique to handhelds. As well as offering more standard malware, spam and firewall protection this software can help you control your phone from afar and if it has GPS capabilities, can show you the location of a device if it is lost or stolen.

Furthermore, it’s possible to lock a device remotely, requiring password access on the handset or a specific unlock request to enable it. If a phone has simply been misplaced in the home, an audible alert request can be sent to the device to signal its location, and it’s even possible to erase sensitive data remotely if you’re sure it has found its way into the wrong hands.

These are some of the more pervasive reasons to invest in a dedicated suite, since as well as protecting a mobile against the latest online threats, the user retains ultimate control of the operation of the device and the ability to render it all but useless in the hands of a thief.

Some of these security concerns are platform-specific, and may not be relevant to all smartphone users, but the ever-changing nature of threats to these devices is such that increasing awareness of the possible pitfalls is a growing concern. Since utilising much of this advice often has additional benefits, such as saving battery power and automatically safeguarding and backing up key data, there’s very little reason not to adopt safe practices as standard when using a phone both at home and on the move. Hackers, malicious users and thieves are usually opportunists, and would rather target those who have offered them an easy way to achieve their goals than spend time

working around obstacles. Follow the advice offered above to make sure you and your phone aren’t easy targets and you’ll stay one step ahead of modern threats.

Protecting stolen phones

Your average thief will try to convert your phone into money as fast as possible and will probably ignore the information on board. Of course, it's better to not give him the temptation, so keep your phone locked with a passcode. This is a very easy step, but it will pay dividends in keeping your phone secure. Android users have a number of options to choose from, including passcodes, pattern codes, face recognition, fingerprints, and others, depending on the device. iOS also supports biometric logins on the iPhone 5S, and a simple four-digit passcode or a complex passphrase for other devices.

Limitations of the study

- The respondents selected were young indian consumer(typically between 18-30years of age).Therefore, the results can not be an indicative of all consumers of india
- Due to time and resource Constraints,the survey was done through online medium
- Personal interaction with all respondents was not possible and therefore output is not controlled
- Onliine survey does not verify the presence of real individual as far as authenticity of results is concerned
- Time was a constraint in conducting the study

REFERENCES:

- See more at: http://www.canalys.com/newsroom/china%E2%80%99s-top-five-vendors-account-20-world%E2%80%99s-smart-phone-shipments#sthash.RMwJtmng.dpuf

http://www.iamwire.com/2013/06/indian-mobile-landscape-2013/#_amkip3nj

http://www.iamwire.com/2013/05/2013-internet-trends-report-kpcb/#_amkip3nj

http://www.idc.com/getdoc.jsp?containerId=prUS24645514

http://www.bullguard.com/bullguard-security-center/security-articles/mobile-security---the-deal-with-apps-for-android-phones.aspx)

http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security

http://www.juniper.net/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks

http://www.itproportal.com/2014/03/15/you-are-your-phone-why-smartphone-security-is-of-paramount-importance/#ixzz30jNxOleE

http://www.technewsdaily.com/7613-hidden-smartphone-threats.html

http://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CDoQFjAC&url=http%3A%2F%2Frebootpeterborough.ca%2Fwp-content%2Fuploads%2F2013%2F04%2FSmartphone-Apps-Permissions-and-Privacy-Report1.pdf&ei=eQlmU7blGISRrAexz4DoBQ&usg=AFQjCNEZ1Lgw6Ro_5_LgsBsk6BYBZCHJsg&sig2=9l-hlhGmooAYWhy1jYVnmw&bvm=bv.65788261,d.bmk