The Role Of Data Protection Technologies: A Case Study

Shafqat Hameed*, Mujtaba Hassan Agha**, Muhammad Abbas Choudhary***

*, National University of Sciences & Technology (NUST), Islamabad, Pakistan
** Department of Mechanical Engineering, Mohammad Ali Jinnah University, Islamabad, Pakistan
***University of Engineering and Technology (UET), Taxila, Pakistan
Shafqat.hameed@ceme.nust.edu.pk

ABSTRACT: In today's digital era, Consumers information plays a very significant role for the companies. They are utilizing this information in different ways to cater the costumers with novel products and services. But the privacy of this information is of much more importance for the service providers as well as for the consumers. The privacy and the protection of the Customers' personal information is a growing concern for the consumers of the telecommunication services all over the world. The importance of telecommunications is apparent from the revenue this service generates for the world economy. There have been innumerable cases around the globe which demonstrated lack of security of customers' personal data. The causes might be different apart from lack of investment in the sophisticated technology for this growing concern. The aim of this study is to analyse the privacy policy of the telecommunication companies, the laws related to customer data protection, different incidents related to customer's privacy and the role of different data protection technologies to overcome this soaring issue.
[Shafqat Hameed, Mujtaba Hassan Agha, Muhammad Abbas Choudhary. **The Role Of Data Protection Technologies: A Case Study**. *Life Sci J* 2012;9(4):1270-1279] (ISSN:1097-8135). http://www.lifesciencesite.com. 192

Key words: Telecommunications, privacy, data, information, protection, technology

1. INTRODUCTION

The mobile telecommunications sector is growing at a large scale in Pakistan. Telecommunications is not only one of the fastest growing sectors in Pakistan but also all around the world. It plays a significant role in global economy. Pakistan was the third fastest growing telecommunications market in the world in 2008 (Wilson J, 2009) and it is estimated that in April 2011 it has 108 million mobile subscribers (CIA, 2011). In Pakistan, cell phone coverage has been provided to approximately 90 percent of the areas and more than half of Pakistan's population has access to a cell phone.

With the evolution of technology, the privacy has been the most important issue for the customers associated with information technology. The aim of this study is to identify the significance of the customers' privacy and their data protection and how the technology can be used to improve the privacy and to protect the customers 'data?

Every country possesses written laws for the protection of personal information and the limits under which the private information can be accessed or used are provided by the concerned authorities. Consumer privacy has become a crucial issue with the advent and evolution of the mass communications, electronic methods, telecommunications and Web. In telecommunications, Personal information includes call traffic details, service usage data i.e. email/ internet and customer information which includes name, address, fixed line number, mobile number, email address and all other contact details. And when personal information of costumers is misused or deficiently protected, its consequences can be identity theft, financial fraud, and other problems that collectively cost people, businesses, and governments millions of dollars per year. In the telecommunications sector, lack of privacy and data protection is a perturbing situation for the consumers which need to be addressed. The main objective of all the businesses, by and large, is to satisfy the customers at an optimum level.

"Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise"(Jericho Forum, 2007).

In addition, early definitions of consumer privacy concentrate on two types of control: 1) control of presence of others in the marketing environment and 2) control of transactional information (Goodwin 1991; Jones 1991). These definitions of privacy were elaborated to include the information regarding the consumers' knowledge about the organization's information practices and privacy policy (Foxman and Kilcoyne 1993; Nowak and Phelps 1995).Consumers assert that they have a right to privacy in marketing situations, But consumer privacy is not considered absolute for the following reasons: 1) Conflicts of

consumer privacy with other consumer and marketer rights, 2) what represents consumer privacy is culturally, and individually determined 3) Moreover, who "owns" consumers" private information, the terminology differs in marketers and consumers (Foxman and Kilcoyne 1993; Milne and Gordon 1993).Similarly ,The literature inquired the ethical dimensions of consumers" right to privacy and marketers" information practices. Researchers have examined the different associated justifications of regarding control of information, the privacy trade-offs that customers make with a firm and the application of several theories to explain perceptions of authority, trust, and equity regarding a firm's information practices.

It is legitimate for the consumers to question the companies about their concerns related to the services and the obligation of the service providers is to address their concerns. Data Protection and Privacy is a challenging problem for the telecommunication companies. It is not easy to manage and handle the large data of billions and trillions terabytes and even more. Undoubtedly, Technology has solved myriad problems and it will continue to do so in future. It is evolving day by day as the solution of numerous problems which are encountered daily. Technology is also trying to provide solution for this issue of privacy and data protection. In this paper we will analyse in detail the role of different data protection technologies and privacy enhancing techniques to address this surging issue.

2. Literature review:

2.1. Concept of Privacy in Telecommunications

The concept of privacy in telecommunications is not different from the concept of privacy in other spheres of life. Although, there is confusion regarding the interpretation of word Privacy, yet in literature this word has been defined in detail. (Rodríguez, 1997) defined the term privacy in four levels.

2.1.1. Descriptive level

In the descriptive sense privacy does not relates to explicit legal or moral connotation. This refers to the most primitive opinion of privacy. The versions available in dictionaries are said to be of descriptive level. Which are based on two concepts, one is the concept of seclusion which is known as a "zero relationship", and the other one is the concept of secrecy.

2.1.2. Value level

In a value sense, it is the individual who decides which aspects of his life he believes should not be shown to public eye. Moreover, the entire society should also form an opinion that to what extent the individual's privacy should be respected, and what is the socially acceptable scope of privacy.

2.1.3 Legal level

In a strictly legal sense, the term privacy refers to the special sphere of privacy protected by law. Privacy also refers to the right to privacy in the strict sense.

2.1.4 Interest level

Sometimes the term privacy is often used to refer not to the right itself, but to the interests justifying the protection granted to some right.

The role of the interests is played by privacy that lay behind the protection of other corroborative rights e.g. the secrecy of telecommunications

Generally, privacy is defined as "the control over one's seclusion and secrecy. In telecommunications privacy this definition can justify the recognition of the secrecy as a right, one's freedom of action which is one's freedom to express oneself freely in telecommunication as a medium of communication that is the utmost reason for the protection of secrecy in telecommunication industry (Rodriguez, 1997).

2.2. Privacy protection approaches

Quinn (2005) divided the approaches to privacy into two categories:

2.2.1. Free market approach

In this approach, the Commercial entities can do whatever they want but with the expectation that customers will choose to do business with those corporations which respect consumer privacy to an appropriate degree. And if few companies do not sufficiently respect privacy, then they would ultimately lose market share. This approach may be confined by limited competition of enterprises in a market, who are not offering favourable privacy options to the user, or the deficiency on the user's part regarding the information about actual privacy practices. Moreover, the claims made by the organizations about the privacy protection may be hard for consumers to affirm.

2.2.2. Consumer protection approach

In consumer protection approach, it is recognized that customers may have lack of time or knowledge to make any informed choices, or lack of reasonable alternatives available (Jensen and Pots, 2004) Mostly average person cannot comprehend the privacy policies and this approach justifies government definition of privacy and privacy standards.

2.3. Privacy in location based services

Problems associated with customer's privacy are increasing for location tracking capabilities of mobile devices are increasing; customers' perspective and preferences comprise personal information and unlawful usage that breaches user's privacy. Various methods have been suggested to protect user's privacy when using location based services which includes the methods of anonymizing servers, encryption of information blurring etc. Several methods for privacy quantification have also been proposed, for calculating

the balance between the advantage of providing precise location data and the disadvantages of personal privacy risking (Voulodimos and Patrikakis, 2009). Furthermore, Customers of such services can be allowed to choose to display more generic location information e.g. "In the City" or "Islamabad" or "Work" to whom they want to inform by displaying only selected information in location, like their exact address, to Family members and close friends.

2.4. Data Protection

(Clark, 2008) defines data protection as an umbrella term which blankets a broad range of technologies for safeguarding data assets. Data yielded and controlled by upper-layer applications is the raw material of useful information. Loss of data is directly proportional to loss of revenue, the consequence of which is ultimately the loss of the enterprise itself (Clark, 2008).

Because data is very crucial for the viability of a firm, detecting the ways to restrict access to data and ascertain the integrity of the data is fundamental to an IT strategy. Data is ultimately stored on any form of storage media which includes solid state disk, optical media, and tape and in disk media in the form of storage arrays. Some examples include Network attached storage which processes files to upper-layer applications, but it is unable to do reliably without underlying safeguards at the block level, also includes redundant array of inexpensive disks (RAID), alternate pathing, data replication, and block-based tape backup (Clark, 2008).

2.5. Customers' Data to be protected in Telecommunications

(Nut, A. 2008) It is vital for the success business to secure the data and information of the companies and customers. In the present world where identity theft is at rise small firms are regrettably not prepared to handle the responsibility of the data security.

Some small businesses realize the significance of provision of secure storage for their customers' data. They have observed the consequences of improper storage of data. When customers get to know about the loss of their personal information, customers begin to think twice about doing business with that company (Nut, A. 2008).

2.5.1 Kind of data to be protected

Data Protection Commissioner Ireland (2008) has defined the kinds of data to be protected in telecommunications to be as follows:

2.5.1.1 Detailed telephone record retention

Detailed records of customer's telephone calls may be kept for the required period to settle bills and payments but no longer than that. But few companies may require retaining personal details for a longer time.

2.5.1.2. Storing and accessing information on terminal equipment i.e. "Cookies"

Information can only be stored on or retrieved from a user's computer or any terminal equipment after the individual allows this. Moreover, it is the right of individual to refuse the placing or accessing of this information.

2.5.1.3. Calling Line Identification

It is lawful for telecommunication users to hide their contact number, which is invisible to other user. It is not necessary for the users who make marketing calls to hide their phone number when making these calls.

2.5.1.4. Location Data

If the individual allows the processing of location or other traffic data then it may be accessed for providing the value added service to the customer.

2.5.1.5. Public Telephone Directories

Public telephone directories also provide the user's personal information. The Individuals have the right to exclude themselves from the directory for protecting their privacy.

2.5.2. Customer

If the personal details of the customers are obtained for product marketing then web-mail and SMS marketing are only allowed to take place if a service is user friendly and an opportunity is given to object to these marketing messages.

2.5.3. *Consent*

For sending the marketing messages the consent of the individual is required if the person is not the customer. E.g. the individual must be asked that if he wishes to receive marketing material.

2.6. Privacy Policy of Telecommunication companies in Pakistan

Every telecommunication company provides its customers with privacy policy. Through the privacy policies the company describes the details to the customer that how the company will use the customer's personal information. To whom the company discloses the customer's personal information and the reasons for the disclosure are provide. Following are the privacy policies of the few telecommunication companies in Pakistan.

2.6.1. Ufone GSM

2.6.1.1. Personal Information

The information or data that identifies the customer is a Personal Information. Ufone presumes that the

personal information provide to them is true, accurate in complete is all respects. The personal data with Ufone includes customers' name, their birth date, their addresses, their telephone numbers, emails, credit card and their bank account details, occupation, details of references, PIN and passwords of Ufone account (Ufone, 2012).

2.6.1.2. Use of Personal Information

Ufone informs the customers that their personal information may be used for:

- Affirming customer's personal identity
- Aiding customer to subscribe to ufone's services.
- Provision of the services which customers require
- Managing the services like charging, billing and collecting debts.
- Conducting suitable checks for credit worthiness
- Understanding the needs of customers' information and communication to provide them with a better and improved service.
- The Promotion and marketing of Ufone services for the benefit of customer.

Ufone pledges that it does not disclose customer's personal information third parties e.g. other cellular service providers, banks and credit card companies and their agents which can ultimately lead to invasion to customer's privacy. In contrast, company may affiliate with such agencies for the benefit of the customers to provide them with better services. And the company may reveal customers' personal data to these agencies for marketing or any other purposes. Ufone aims to ensure that these organizations are obliged to and will protect customers' personal data and information. Furthermore, Ufone may disclose customers' personal information to:

- Authorized representatives of customers'
- The agencies like Credit- reporting and fraud-checking agencies
- The companies related to Ufone.
- Professional advisors, accountants and lawyers etc of Ufone.
- Regulatory authorities and Other Government organizations authorized by law.
- And those firms which manage Ufone's business and corporate strategies.

Moreover, Ufone may also reveal customers' personal data for good if it considers its necessity as a legal requirement to protect and defend the rights and interests of its customers (Ufone, 2012).

2.6.1.3. Information Security

Ufone desires employees and contractors to perform their duties with responsibility in such a way that is coherent with Ufone's legal responsibilities regarding customer privacy. Ufone is committed to respect the privacy of the customers' on a priority basis and ensures that this personal information will not be disclosed to any outside Organizations other than those organizations working on behalf of Ufone (Ufone, 2012).

2.6.2. Warid Telecom

Warid shows its commitment to respect customers' privacy and to abiding by the applicable data protection and privacy laws (Warid, 2012).

2.6.2.1. Personal Information Collection

Warid pledges to collect and use customers' personal information only with their knowledge and consent. The personal information which Warid collects includes their name, address, birth date, gender, telephone and fax numbers, email address, and credit/debit card information. The personal information collected would be used only for providing the particular service to the customer. (Warid, 2012).

2.6.2.2. Usage of Personal Information

Warid uses customers' information for various purposes which include: Customers' order processing, management of their account; for delivery of service, for responding to complaints or account enquiries; administering debt recoveries; verification of their identity when required for example; to help the customers for data protection if they lose their password or PIN information (Warid, 2012).

2.6.2.3. Disclosure of Information

The customers information may be disclosed by Warid, to the companies designated as 'Warid Affiliates'; and in case that Warid experiences re-organization or sold to a third party, in this case customers agree that any personal information we hold about them may be transferred to that re-organized entity or third party for the purposes.

Moreover, Warid does not sell or pass your personal information to third parties without the consent of customers. The customer data can be revealed for the validation of credit card details or to obtain payment for billing

Warid can reveal customer's data to comply with the legal requirement (Warid, 2012).

2.6.2.4. Information Security

Warid is aware of the customers' increasing concern about the protection of their personal information and how they protect their data from

misuse. Warid is continuously reviewing and enhancing its procedures which include technical, physical and managerial procedures for the protection of customer's personal data from unauthorized access, accidental loss or destruction. The technology used by Warid for data protection is secure sockets layer (SSL) technology, which helps to encrypt sensitive information such as customers' finance related information (Warid, 2012).

The communications on the Internet are not secure until they are encrypted as the data may route through different mediums and links before delivery. Warid is not responsible for loss of personal information which is beyond its control (Warid, 2012).

2.6.2.5. Monitoring and recording of customer's communications

Prevention of crime is essential for any country. The law permits the Monitoring or recording of customer's calls, emails, text messages and other communications for the security objectives (Warid, 2012).

2.6.3. Telenor

The privacy policy of telenor also describes all of the above mentioned points. (Telenor, 2012).

2.7. Data Protection Technologies

Several telecommunication companies have used data protection technologies and privacy enhancing techniques to increase the efficiency of organization to protect the customers' private data. Moreover, Data protection solutions and technologies can be categorized by the scope of defense they provide. Protection against component, link, or device failure is provided by lower level solutions; while protection against system, business application, or site failure is provided by higher level solution, as shown in Table 1.

Table 1. Data Protection Mechanisms (Clark, 2008)

Type of Data Protection	Protection against	Recovery time objective	Recovery point objective
RAID	Disk drive Failure	Instantaneous	No data loss
Mirroring	Link, disk or array failure	Instantaneous	No data loss
True CDP	Data corruption	Seconds – minutes	No data loss
Near CDP/Snapshot	Data corruption	Seconds – minutes	Some data loss
Synchronous Replication	System/site Failure	Seconds – minutes	No data loss
Asynchronous Replication	System/site Failure	Seconds – minutes	Some data loss
Disk to disk tape emulation	Array Failure	Minutes	Some data loss
Local Tape Backup	Array Failure	Minutes – hours	Some data loss

2.7.1. Hitachi Data Systems

Telecommunications companies are in a dire need of more storage capacity due to enormous growth rate in this industry. The increasing concern of telecommunication companies is the protection of this bulk of data, which is vital for their business which includes their (BSS) business support data, the content of customer for securing their data.

However, Telecommunication operations demand heterogeneous storage systems because of geographically distributed telecom systems. Therefore, data protection in telecommunications becomes a challenging task because of its distributed nature. The Innovative data protection and management solutions for their telecom customers to help them recover and protect the data along with the data replication and data security offerings are provided by Hitachi Data Systems (Hitachi Data System, 2012).

2.7.1.1 Hitachi data systems solutions for data protection (Benefits)

- One of the benefits is that it protects following data which includes BSS data, customer content like rich media customer content and data centre customer content and it reduces the risk of financial loss with the help of high performance storage infrastructure and automation.
- Another benefit is that it reduces management and training costs and increases IT efficiency having common interface for different operations like backup and recovery, de-duplication, continuous data replication, application protection, virtualized backups, remote office protection etc.
- Another benefit is that it replicates critical data disk-to-disk for speedy restore, testing, development and remote disaster recovery protection.
- It helps in making effective use of existing infrastructure and reduces investment in storage with data reduction methods, for instance, de-duplication and archiving.
- It helps in improving protection, and recovery of important applications with advanced assessment, design and implementation services (Hitachi Data System, 2012).

2.7.2. Yosemite File Keeper recommended by Safari Telecom

File Keeper's technology protects every document a user edits at the time they save their documents to disk, wherever the documents are stored or the system is disconnected from the network (Safari Telecom, 2010).

2.7.2.1 Challenges

- The individual users manage a wide variety of critical information which is stored on servers, desktop and laptop.
- Laptop computers are unreliable for data protection the reason may be hardware failure and theft, and the result is loss of critical information.
- The users are unable to back up files when disconnected from the network.

2.7.2.2 Solutions

- This technology assists those users who are occasionally-connected by storing changed files on the local disk and then copying them to the file backup locations when users reconnect to their network.
- This technology backs up files as they are created and updated. Reduces the financial effect of data loss by insuring that the updated versions of a user's data are protected.
- The agents of this technology operate in the background and do not require direct interaction with the user. User data is automatically and continuously protected without affecting productivity of the end user.
- Through this technology the users can rapidly and easily restore their own data, which increases their output.

2.7.2.3 Results

- Continuous file protection
- Reduced financial impact as a consequence of data loss.
- The Information stored on the most vulnerable and unreliable equipment in an organization's network is protected.

3. METHODOLOGY

The aim of this study is to measure the extent to which the customers' are concerned about their privacy in the telecommunications. On the whole, approach is descriptive as well as quantitative in nature. Questionnaire tool is used as a base for survey. The questionnaire is prepared to collect data from different groups of people who are customers of different telecommunication companies. It is usually mailed to the informants to be answered. The data is to be used to analyze the effect of privacy protection on the customers.

The questionnaire is created in English. Simple and accurate questions with specific answers were used. The survey questionnaire is comprised of 18 questions and it has been divided into three parts.

- Continuous file protection
- Part one is focused on the customer's general information. It comprises of five questions.
- Part two focuses on the customer's view. This part comprises of eleven questions.
- Part three is comprised of amalgamation of both and the customer views related to solutions to privacy.

The questionnaire is composed of open ended as well as close ended questions. A five point Likert-type scale is used for closed ended questions to measure the degree of concern of customers related to privacy by looking for agreement of the respondents to the survey statements and questions. The respondent is supposed to put up a mark of 1 to a particular question if they strongly agreed to a particular question.

However, if they strongly disagreed they put up a mark of 5 to a given question. For the open ended part of the questionnaire the respondents are supposed to describe their experiences regarding the telecommunications services and their views on privacy.

The questionnaire was made on Google survey and the link was given to different people for giving their views regarding the privacy in their network.108 questionnaires were filled and the data was collected based on the answers given by the customers of different telecommunication companies.

4. RESULTS AND ANALYSIS

The aim of this research was to identify the extent of privacy needed to the customers in their day to day communications via mobile phone. At present, five mobile telecommunication companies are operating in the country. The data is collected from the customers of different companies and from different cities.

The key questions asked and their results are as follows:

4.1. *Which cellular network do you use?*

Table 2. Customers of telecommunication companies Data

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Mobilink	12	11.1	11.1	11.1
Telenor	15	13.9	13.9	25.0
Ufone	54	50.0	50.0	75.0
Warid	21	19.4	19.4	94.4
Zong	6	5.6	5.6	100.0
Total	108	100.0	100.0	

108 customers responded to the questions, out of which Ufone has the maximum number of customers numbering 54 then Warid with 21 customers, Telenor with 15, Mobilink with 12 and Zong having 6 customers in the sample data.

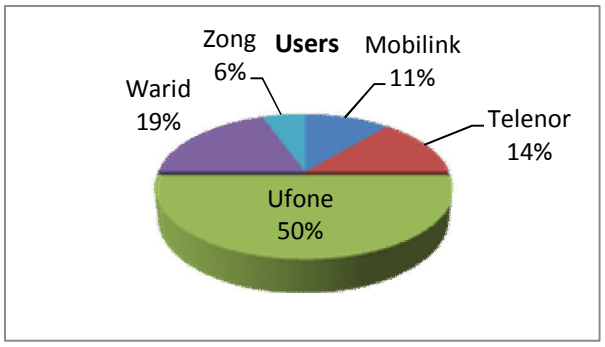

Figure 1. Users of telecommunication companies of Pakistan

According to the data, 50 percent of the customers in the sample are using Ufone, 19 percent Warid, 14 percent Telenor ,11 percent Mobilink and 6 percent Zong.

4.2. *Are you satisfied with privacy given to you by your telecom network?*

The next question asked was related to the satisfaction level of the customers related to their telecommunication network. Following are the results:

Table 3. Data of customer satisfaction related to privacy protection

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
1	6	5.6	5.6	5.6
2	12	11.1	11.1	16.7
3	54	50.0	50.0	66.7
4	33	30.6	30.6	97.2
5	3	2.8	2.8	100.0
Total	108	100.0	100.0	

Out of 108 customers only three customers (all of Warid telecom) are extremely satisfied with the provision of privacy by the telecommunication companies. Maximum customers (54) are moderately satisfied with the privacy provided by the companies. Six customers are very dissatisfied with the privacy services.

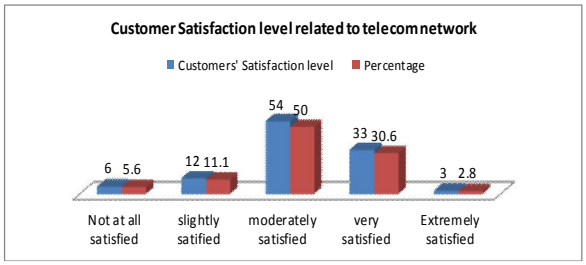

Figure 2. Customer Satisfaction Level

4.3. *I am satisfied with the privacy of the voice data of my network given to me?*

The next question was related to the privacy of voice data provided to the customers' .For instance, the call records of the customers the talk time of the customers etc. Following are the results which are based on the sampling and research.

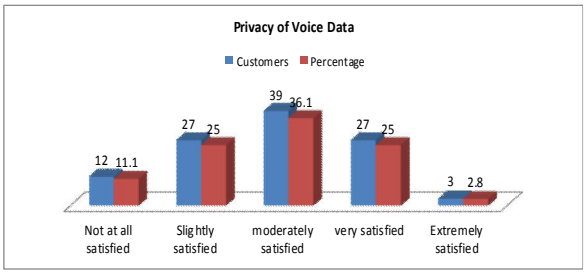

Figure 3. Privacy of Voice data in Telecommunication companies

36.1 percent of the customers are moderately satisfied with the privacy of the voice data provided by the telecommunication companies.25 percent are slightly satisfied and rest of the 25 percent are also satisfied with the privacy. Furthermore, 11.1 percent of the customers are not at all satisfied with the privacy.2.8 percent are extremely satisfied with the privacy of the voice data given to the customers.

4.4. *I should know at what time cellular company is monitoring my SMS, MMS in the mobile.*

Another question that was asked from the customers' was on their concern regarding the monitoring (by the service provider) data which is textual form or in the form of pictures and videos. Following are the results.

Table 4. Data privacy of SMS/ MMS according to the customers

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
1	6	5.6	5.6	5.6
2	3	2.8	2.8	8.3
3	18	16.7	16.7	25.0
4	81	75.0	75.0	100.0
5	0	-	-	-
Total	108	100.0	100.0	

75 percent of the customers' strongly agree with the statement that they should know when and why their data is being monitored.16.7 percent remained undecided about this matter. 2 percent disagreed with the statement whereas 5.6 percent of the population of sample strongly disagreed that they should not be provided with the information about the monitoring of their SMS and MMS data.

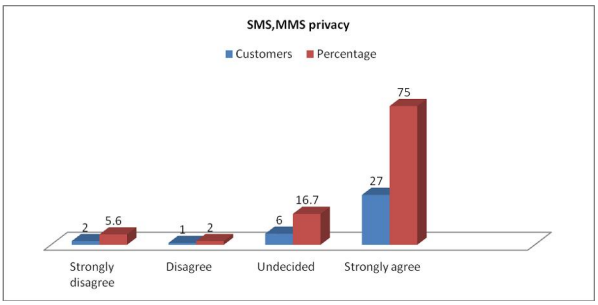

Figure 4. Customer views on SMS and MMS privacy

4.5. *I should know at what time my voice is being recorded by some other person?*

Next sequential question was based on the monitoring and recording of the customers' voice. Following are the results and the data collected from the customer'.

Table 5. Data of voice monitoring and recording

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
1	0	-	-	-
2	9	8.3	8.3	8.3
3	3	2.8	2.8	11.1
4	15	13.9	13.9	25.0
5	81	75.0	75.0	100.0
Total	108	100.0	100.0	

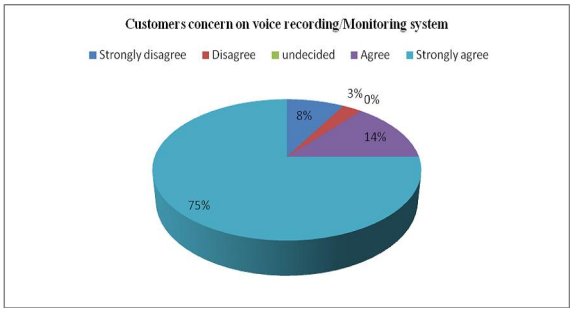

Figure 5. User concerns on Voice Data Recording

75 percent of the sample population strongly agreed with the statement that they should know when their voice data is being monitored/ recorded by third party. 14 percent agree with the statement, 3 percent disagree and there was no disagreement with the strategy of disclosing the information about the timing of the voice recording data.

4.6. *Are you satisfied with the customer service when you feel any complain of privacy?*

The next question that was asked in the questionnaire was based on the customer services that were given by the company to the customers that whether they are beneficial for the customers' related to the privacy matters or not. Following are the results collected from the data.

Table 6. Data of customer services provided by the telecommunication companies

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
1	24	22.2	22.2	22.2
2	24	22.2	22.2	44.4
3	36	33.3	33.3	77.8
4	15	13.9	13.9	91.7
5	9	8.3	8.3	100.0
Total	108	100.0	100.0	

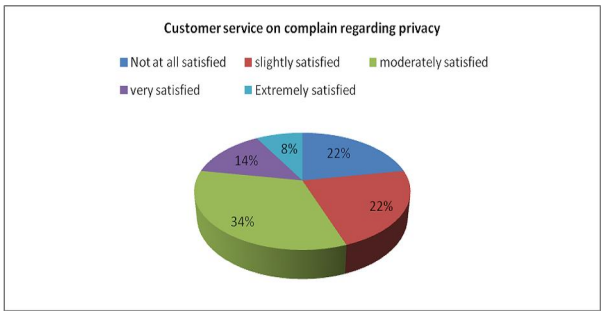

Figure 6: Customers' services on privacy complaints

According to the data collected, 34% of the customers are moderately satisfied by the customers' services provided by the telecommunication companies. 22% are slightly satisfied, 22% are not at all satisfied, 8% extremely satisfied where as 14% are very satisfied with the customer services.

4.7. *Have you signed any network privacy agreement before getting the connection?*

The next question was based on the privacy agreement that was signed by the customers' when buying the product or services by the telecommunication companies

Table 7. Data of privacy agreement signed by customers

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Don't Know	42	38.9	38.9	38.9
No	48	44.4	44.4	83.3
No, Don't Know	6	5.6	5.6	88.9
Yes	12	11.1	11.1	100.0
Total	108	100.0	100.0	

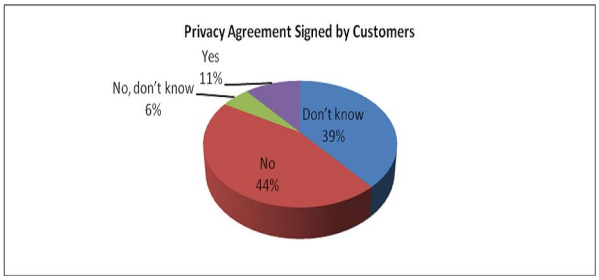

Figure 7: Data on privacy agreements signed by the customers

According to the data collected 44 percent of the customers express that they did not sign any privacy agreement when buying the services. While 39 percent of the customers' don't even know whether they signed the privacy agreement or not, 11 percent agree that they have signed the privacy agreement.

4.7. *Is the government efficient in inculcating the privacy of the customer in telecom sector?*

Moreover, Customers' were asked about the measures taken by the government in inculcating the privacy as well as making the operations efficient and secure for the customers' privacy. Following are the results of the data collected.

Table 8. Data of measures taken by Government according to customers

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Don't Know	24	22.2	22.2	22.2
No	72	66.7	66.7	88.9
No, Don't Know	3	2.8	2.8	91.7
Yes	9	8.3	8.3	100.0
Total	108	100.0	100.0	

According to the data collected 72 percent of the customers' say that government is not efficient in inculcating the privacy in the telecommunication sector. 24 percent say that they don't know about the measures taken by the government in order to make the communication secure for the customers.

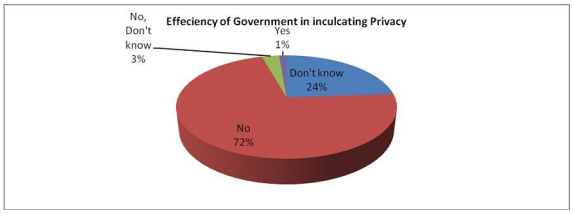

Figure 8. Customer views on measures taken by government in improving the privacy

4.8. *Do you feel any role of the technology in giving you the privacy in the network?*

The customers were also asked about their views regarding the role of technology in the provision of privacy to the customers. Following are the customers' views regarding the role of technology for the provision of privacy.

Table 9. Data regarding role of technology in enhancing privacy

Valid	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Don't Know	21	19.4	19.4	19.4
No	21	19.4	19.4	38.8
No, Don't Know	0	-	-	38.8
Yes	66	61.1	61.1	100.0
Total	108	100.0	100.0	

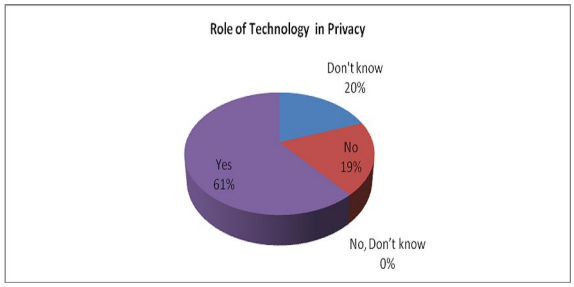

Figure 9. The role of technology in the view of customers

According to the data, 61 percent of the customers' view that there is a role of technology in the provision of privacy in the network, 19 percent say that there is no role of technology in the provision of privacy whereas 20 percent don't know whether there is a role of technology in providing a privacy to the customers or not.

5. CONCLUSION AND RECOMMENDATIONS

Telecommunications is a very important technology which is widely used in Pakistan for different purposes. Therefore, the privacy is crucial for the safe and secure communication. We have collected the data from which it is evident that the customers' are highly concerned about the privacy of their data. They are of the view that the permission should be sought before the usage of their information for various purposes.63.9 percent of the customers strongly recommend that there should be a proper coded method or data encryption for the transfer of information from one point to another and the third person should not be able to comprehend the language of the data transferred.97.3 percent of the customers recommend that there is a need of increasing the privacy of the customers. The customers' also recommend that their suggestion should be valued and the choice should be given to the customers and they themselves should choose the level of the privacy they want from the service providers. Moreover, there must be strict controls followed by the company to ensure privacy of the clients. Any person accessing the data should be monitored and no data should b given to any third person without proper documentation in its support. Furthermore, every employee should not have

access to the private information of the customers of the company. This information should only be disclosed to government agencies. The telecommunication companies should keep a vigilant eye over their employees so that they must not disclose the private information of the customers. The customers face different types of problems regarding privacy from different fronts which should be repressed and the higher technology should be considered an only mean through which the privacy of the customer data could be enhanced and protected.

REFERENCES

1-Jericho Forum. Position Paper Principles for Managing Data Privacy, May 2007.

2-Clinton D. Lanier & Saini A. "Understanding Consumer Privacy: A Review and Future Directions", Academy of Marketing Science Review, Volume 12, Article no. 2, 2008.

3-Wilson, J. Telecom Regulatory and Policy Environment in Pakistan: Results and Analysis of the 2008 TRE Survey, LIRNE*asia*, 22 January 2009.

4-Rodríguez, B. Privacy in telecommunications: a European and an American approach, Kluwer Law International, 1997.

5-Quinn, Michael J. Ethics for the Information Age, Second Edition, Addison Wesley, 2005.

6-Jensen, C & Pots, C. Privacy policies as decision-making tools: an evaluation of online privacy notices, Proceedings of SIGCHI conference on Human factors in computing systems (CHI'04), April 2004, Pages 471-478.

7-Voulodimos A.S. & Patrikakis C.Z., Quantifying Privacy in Terms of Entropy for Context Aware Services, Special issue of the Identity in the Information Society journal, "Identity Management in Grid and SOA", Springer, vol. 2, no 2, December 2009.

8-Clark, T. "Strategies for data protection: A strategic approach to comprehensive data protection", First Edition, Brocade, 2008.

9-Nut A. (2008) "The importance of data security" Data protection Commissioner Ireland, Data Protection in the Telecommunications sector. http://www.dataprotection.ie/viewdoc.asp?DocID=906.

10-Ufone GSM Pakistan, "Privacy Policy" http://www.ufone.com/privacy.aspx.

11-Warid Telecom Pakistan, "Privacy Policy". http://www.waridtel.com/privacy_policy.php

12-Telenor Pakistan, "Privacy Policy". www.**telenor**.com.pk/**privacy-policy**.

13-Hitachi data systems "Hitachi-solution-profile-data-protection-management-telecom" http://www.hds.com/assets/pdf/hitachi-data-systems-solutions-for-data-protection.pdf.

15-Safari Telecom, "Safari-telecom-recommends-yosemite-filekeeper-simple-yet-effective-data-protection".

16-CIA (June 2011) "Pakistan Country Report"; "The World Fact book".

5/12/2012