CONSULTATION PAPER ON SPAM, UNSOLICITED CALLS AND OBNOXIOUS

This Consultation Paper is in line with the functions of the Pakistan Telecommunication Authority (the "Authority") to protect the rights and interests of consumers under Pakistan Telecommunication (Re-organization) Act, 1996 (the "Act").

The stakeholders are requested to respond to the specific questions and issues raised in this consultation paper (paper) as well as highlight other areas that are not covered herein for consideration of the Authority. This Paper does not convey in any sense, any decision of the Authority in respect of the issues discussed in this paper.

Your responses may be sent on or before 26th May 2008 in writing or through e-mail to Ms. Erum Latif, Assistant Director (Law & Regulation), PTA, F -5/1 Islamabad, Phone: 2878137, E-mail: erum@pta.gov.pk

Pakistan Telecommunication Authority

Table of Contents

Consultation Paper on spam, unsolicited and obnoxious calls

Executive Summary

Spamming is an act of sending unsolicited (commercial) electronic messages in bulk. It has severe negative effects on consumers and networks, as it consumes storage and network resources as well as human time and attention to unwanted messages. It has various indirect effects which are very difficult to account for i.e., the spectrum reaches from measurable costs like spam filter software and administration and there cost can not be measured.

Anti-spam laws aimed at sanctioning spammers which may be of a little use in developing countries if the spammers are outside their jurisdiction. The challenge is to tailor legislation to patterns of usage in developing countries and to consider all avenues to combat spam, such as implementing enforceable regulations for Internet service providers (ISPs), mobile operators and wireless local loop (WLL) operators.

In Pakistan with the promulgation of the Prevention from Electronic Crimes Ordinance 2007 ("Ordinance") 'spamming' under section 14 of the ordinance is an offence.

Unsolicited calls are another source of nuisance for public at large. Telemarketing is a continuous disturbance to consumers. A do not call registers would be a solution as adopted by many countries. In addition, obnoxious calls misleading and harassing consumer is yet another challenge faced by operators and the Authority in safeguarding the rights and interests of consumers.

With the intent to control and curb the rapid spread of the menace of spam, unsolicited and obnoxious calls, the Authority having some legal and technical arrangement with the operators can play a vital role against such illegal and immoral and unethical practices.

Consultation Paper on spam, unsolicited and obnoxious calls

Objective

The objective of this paper is to identify the various characteristics and features of spam, unsolicited and obnoxious calls and sort out ways to have an effective mechanism/framework to curb these illegal, immoral and unethical activities.

What the Authority can do in collaboration with operators possibly to reduce significantly the spam, unsolicited and obnoxious calls problem?

1. Definition of spam

1.1 What is Spam?

Literally, It is a trademark for a canned meat product made mainly form ham[1]. Generally, spam (Specialized Automated Mail) is the electronic version of "junk mail, un-requested e-mail messages that advertise products to consumers that have Internet e-mail boxes.[2]

Spamming is an act of sending unsolicited[3] (commercial[4]) electronic messages in bulk. This word is originally derived from spiced *ham* (luncheon meat), which is a registered trademark of Hormel Foods Corporation. Monty Python's Flying Circus used the term *spam* in the so called "spam sketch" as a synonym for frequent occurrence - and someone adopted this for unsolicited mass mail. Based on the origin of the word spam, all other (desired) e-mail is called *ham.*[5]

Spam can be distinguished five different types: i) Beyond e-mail spam; ii) there is messaging spam (often called *spam* - *spam* using instant messaging); iii) newsgroup spam (excessive multiple postings in newsgroups); iv) mobile phone spam (text messages); and v) Internet telephony spam (via voice over IP)[6]and through WLL service.

As discussed above the terms *unsolicited bulk mail (UBE)* or *unsolicited commercial e-mail (UCE)* is commonly used for spam which can be defined as under:

1.1.1 Unsolicited Commercial E-Mail (UCE): It is an electronic mail which contains commercial information that is sent to a recipient who has not asked to receive it "or" an unsolicited e-mail having advertisement material sent by e-mail without the recipient either requesting such information or otherwise explicitly expressing an interest in the material advertised;[7]

---

[1] Oxford Dictionary

[2] McGraw-Hill Illustrated Telecom Dictionary Third edition, Jade Clayton

[3] The word 'unsolicited' means '*not asked for*'

[4] Commercial' as defined in the Oxford English Dictionary is 'making or intended to make profit'

[5] Anti-spam methods State of the Art by W.Gansterer,M. Ilger,P.Lechner,R.Nuemayer,J StrauB

[6] Anti-spam methods State of the Art by W.Gansterer,M. Ilger,P.Lechner,R.Nuemayer,J StrauB

[7] Anti-spam methods State of the Art by W.Gansterer,M. Ilger,P.Lechner,R.Nuemayer,J StrauB

1.1.2 Unsolicited Bulk E-mail (UBE): An electronic mail with substantially identical content sent to many recipients who have not asked to receive it. UBE or UBE is internet mail that is sent to a group of recipients who have not requested it.[8]

There is no international agreed definition of what is and what constitutes illegal spam. Followings are the definitions provided by Australia, European Union and United States.

i. **Australia:** defined as "unsolicited commercial electronic messages" (though the word "Spam" is not specifically mentioned), judicial provisions are technologically neutral: legislation includes Email, SMS, MMS and instant messaging; while faxes and voice-to-voice telemarketing are excluded, no reference to bulk messaging - a single unsolicited commercial electronic message could be Spam

ii. **European Union:** The term Spam is neither defined nor used, the term "electronic mail for the purposes of direct marketing" is used, judicial provisions are technically neutral: legislation includes Email, calling machines, faxes and SMS messages

iii. **United States:** The term Spam is neither defined nor used, a FTC-definition of a "Commercial Electronic Mail Message" exists, judicial provisions not limited to Email: inclusion of mobile Spam subject to implementation (Action by the Federal Communications Commission on mobile Spam)[9].

1.2 Purpose of spam

The most common purpose for spamming is advertising. Offering goods range from pornography, computer software and medical products etc. Many of these products may have an ill-reputed or questionable. The main motivation for spamming is commercial profit. The costs for sending millions of spam mail messages are very low. In order to make good profit, it suffices, if only a very small fraction (0.1 % or even less) of the sent out spam are replied to and lead to business transactions.

1.3 Effect of spam

Spam has severe negative effects on e-mail users. It consumes computer, storage and network resources as well as human time and attention to unwanted messages. Moreover, it has various indirect effects which are very difficult to account for - the spectrum reaches from measurable costs like spam filter software and administration to not measurable costs like a lost e-mail (expensive for a business, not that expensive for a private person).

1.4 Types/Modes of Spam

---

[8] Anti-spam methods State of the Art by W.Gansterer,M. Ilger,P.Lechner,R.Nuemayer,J StrauB

[9] www.fttc.gov/opa/2005/01primaryurp.htm

1.4.1 E-mail Spam

It is a spam sent through e-mail to several recipients without their implied of express permission. Spammers may have different ways to conceal identity. Normally, spoofing technique is being used, by which the receiving mail looks as if it is sent from a different mail identity. Spammers also use false e-mail IDs or stolen e-mail IDs, to send mails. Often they change the e-mail IDs once the ISP marks it as spam. The subject is changed constantly. Spammers also try to get through the filter by intentionally changing the wording and mis-spelling them. But the receiver cannot reject all the mails based on wrong spelling as there is a risk of rejecting legitimate mails.

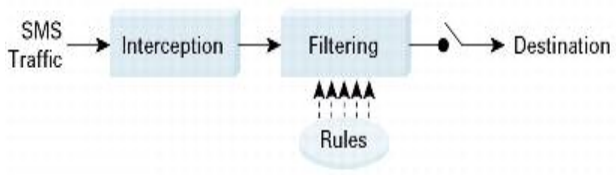
Aim to be a step ahead of the ISPs by finding ways to get through the filters. Some of these spammers also use spam to send virus, which would do a lot of harm to unprotected systems.[10]

1.2.2 Mobile Spam[11]

Spam can also be sent through mobile phones. The spammers misuse the text messaging service in mobile telephony. It is not only inconvenient for the mobile user but also increases the financial cost if the user has to pay for the received message.

Mobile phone spam is a form of spamming directed at the short message service (SMS) service of a mobile phone operators. Furthermore, some of that spam is sent from fake addresses, causing inaccurate billing for subscribers and revenue penalty for the mobile operator, which cannot bill the sender for the termination.

Mobile operators can deploy SMS spam prevention system on their signaling network, where the system intercepts SMS(s), applies filters to identify spam, and drops offending messages. Following diagram depicts the solution:



Various solution providers like Cisco, Nokia etc are offering their products to the mobile operators for preventing Spam spreading through text messaging services. Telecom Authorities across the world are also preparing necessary guidelines and directing the operators to set up spam prevention system. Malaysian Communications and Multimedia Commission (MCMC) had given the orders to all cellular service providers, or celcos that they must set up an avoidance system that automatically blocks spamming

[10] Spam an Introduction Edited by D Satish,K Rajesh Prabahlar
[11] Includes all forms of short messaging spam

and spoofing of SMS messages by the end of September 2007.Spam messages/text messages are also sent through WLL systems.

1.4.3 Message spam

Messaging spam makes use of the instant messaging system like Yahoo and msn messengers. Many of the advertising companies can get a directory containing the names and addresses of people to whom they can send instant messages. Here also, the cost involved in this advertising is low as apart from the directory the spammer requires scriptable software. These messaging spammers also target Internet Relay Chat Channels and bombard people with advertising.

Message spam can also be sent through the messenger services using Microsoft windows. This service is used to send pop up messages from the servers, when they are connected to the internet without adequate firewalls, this system can be misused by the spammers. However, the messenger can be disabled. Nowadays, all the instant messaging service providers are providing the privacy options to the customers to safeguard them against messaging spam.[12]

1.4.4 Search Engine spam

In this form of spam, die spammers usually do spamdexing by which they target the HTML pages to increase their rank so that the person using the search engine would notice the website fast. spamdexing is dishonest and misleading. A "white hat" technique is a technique which makes websites indexable by search engines without misleading the indexing processes.[13]

2. The Spam Problem

The problem of spam is well established. The extent of the problem is plain to anyone who relies upon electronic mail for communications and related forms of messaging such as “blogs” (short for “Web logs”) and SMS that have become an important and popular means of communication around the world. These services are cheap, they have global reach, and they are playing a key role in the development of e-commerce.

2.1 Cost Factors

The following list summarizes a few of the cost factors characteristic for spamming businesses.

[12] Spam an Introduction Edited by D Satish,K Rajesh Prabahlar
[13] Spam an Introduction Edited by D Satish,K Rajesh Prabahlar

2.1.1 Product: Most of the spammers do not sell anything to the recipients of spam - they are just acting as marketers (thus, spammers do not have any investments for actually purchasing products).

2.2.2 Marketing Material*:* The creation of an e-mail does not need any highly specialized software or knowledge. Thus, producing the marketing material is very cheap, and -one of the most important differences to classical marketing - the costs for sending out marketing material do *not* increase proportionally with the number of potential customers reached.

2.2.3 Spam Tools*:* Tools for generating and sending out millions of personalized e-mail are available inexpensive (often even for free) and easy to use.

2.2.4 Address Harvesting Tools: Tools for collecting addresses automatically on the Internet can be downloaded and addresses can be bought or rent. Although the price for e-mail addresses depends on their "quality", they are generally quite inexpensive.

2.2.5 The Spam Campaign*:* Set up an Internet connection (for example, a free trial account), send out millions of messages from this account in a short period, and move to the next ISP for getting a new (free) account.

2.2.5 Other Costs*:* These include hardware and maintenance costs, but may also include costs for responding to interested buyers (automated, in order to avoid personal interaction, for example, via a Web interface).[14]

2.2 Profit Factors

A list some of the most important sources of income and profit for spammers are given below.

2.2.1 Direct Income*:* The most common form of income for spammers is that they act as marketing companies and are paid for marketing campaigns.

Web Banner Revenues*:* In many cases, spammers get revenue for every visit on a Web site, which is advertised, in a spam e-mail.

2.2.2 Validation of Contact Information*:* Another source of income for spammers is to validate e-mail addresses (for example, responses to "unsubscribe here" invitations in spam messages) and to sell this information to other spammers or direct marketing companies.

2.2.3 Sell Spam Business Models*:* The above is a special case of a more general concept where spammers sell the information collected from responses to spam messages to others.

2.2.4 Scams: In many cases, spam messages are hidden attempts to find out personal or access information ("phishing"), such as credit card information, bank account information, etc., which can then be used for criminal activities (theft, illegal investment, etc.). Other kinds of scam could be: dubious job offers, ponzi schemes[4], Internet gambling, auctions, sexual offers and pre-paid purchase orders with no supply of the ordered goods.

[14] Anti-spam methods State of the Art by W.Gansterer,M. Ilger,P.Lechner,R.Nuemayer,J StrauB

2.2.5 Product Selling*:* Only a minority of companies who send out spam are also selling the advertised products themselves.[15]

3. Approaches to control Spam

Two approaches have been adopted in several legal frameworks globally. Each approach has it positives and negatives impact. Opt-in means that nobody is allowed to send UBE unless the receiver has explicitly agreed to receive such messages. In an opt-out system, anybody is allowed to send UBE to anybody else as long as the receiver has the possibility to opt out at any time he wants, that is, to declare that he does not want to receive such messages any more.

3.1 Tackling Spam

Lawsuits – although few and far, and limited to certain jurisdictions – represent a ray of hope that enforcement by ISPs, with the help from customers, might get the job done against spam. Indeed, the success of these efforts suggests that ISPs could become the most valuable players in the effort to end spam. The challenge for lawmakers is how to create a fair, effective regulatory regime that takes advantage of ISPs' ability to help end spam without placing an undue burden on law-abiding companies.[16]

The same is the case with SMS. Mobile spam can be controlled to quite an extent if Mobile and WLL operators assist in the application of tools at source.

3.2 A Combination of Approaches

The persistence of spam problem has led policy-makers, technologists, academics, and many others to come up with a wide range of possible strategies to end it. The chairman's report of the ITU, Thematic Workshop on Countering Spam in 2004 contains a range of proposals, suggesting an intersection of many methods of spam-fighting. This comprehensive, five-part approach calls for a combination of:

- Strong, enforceable legislation;
- The continued development of technical measures;
- The establishment of meaningful industry partnerships, especially among ISPs, mobile carriers and direct marketing associations;
- The education of consumers and industry players about anti-spam measures and Internet security practices; and,
- International cooperation among government, industry, consumer, business and anti-spam groups, for a global and coordinated approach to the problem.

Most of the existing anti-spam laws are directed at controlling spammers' behavior. This seems appropriate, since spammers directly cause the problem. But the current slate of laws has failed even to curb the *growth* of spam, much less to reduce the

[15] Anti-spam methods State of the Art by W.Gansterer,M. Ilger,P.Lechner,R.Nuemayer,J StrauB

[16] Stemming the International tide of Spam by John G. Palfrey, Jr., Executive Director, Berkman Center for Internet & Society and Clinical Professor of Law, Harvard Law School

problem. Why have they failed? Some observers argue that the countries generating the largest proportion of the world's spam have done too little at home to stop the problem. Those making this argument especially criticize reliance upon "opt-out" rules that allow spam unless consumers specifically ask not to receive it. Even then, opt-out rules are not enforced aggressively enough.[17]

4. Spam in Developing Countries

Spam is arguably a bigger problem in developing countries than in wealthier countries, where anti-spam mechanisms are more robust. Many developing countries do not yet have anti spam laws, and those that do often do not have resources to enforce them. Meanwhile, the effects of spam are often relatively more costly in developing countries. ISPs are frequently deluged by spikes in spam, which lead to network slowdowns and breakdowns.

Moreover, many people in developing countries send emails from shared internet connections and equipments, such as at cybercafés or other public access centers. These services ordinarily rely on hosted email services with limits on inbox sizes. Accessing e-mail becomes too expensive if per-minute charges paid to cybercafé owners are consumed by cleaning spam from their inboxes. Even worse, legitimate emails are bounced because the limited space of their inboxes is consumed by spam.

Anti-spam laws aimed at sanctioning spammers may be of little use in developing countries if the spammers are outside their jurisdiction. The challenge is to tailor legislation to patterns of usage in developing countries and to consider all avenues to combat spam, such as implementing enforceable Standard operating procedures (SOP) for ISPs, Mobile operators and WLL operators.[18]

5. Steps to control spam

a. SOP issued by regulator for ISPs and Mobile Operators and WLL operators.
b. Industry Initiatives-Private initiatives
c. Education and awareness
d. Anti-spam Law
e. Law enforcement Agencies

6. Unsolicited calls

6.1 An overview of unsolicited Calls in developing countries

[17] Stemming the International tide of Spam by John G. Palfrey, Jr., Executive Director, Berkman Center for Internet & Society and Clinical Professor of Law, Harvard Law School

[18] Stemming the International tide of Spam by John G. Palfrey, Jr., Executive Director, Berkman Center for Internet & Society and Clinical Professor of Law, Harvard Law School

Unsolicited calls are also a major source of disturbance in developing countries than in wealthier countries, where strictly enforced mechanisms have been implemented. Examples of unsolicited calls include informative calls about health and social campaigns and fund raising. They create nuisance because unlike other communication media, the telephone generally demands immediate attention because people do not want to miss important and emergency calls, which takes time and effort.

Pakistan like other countries has a caller party pays regime both in fixed and mobile telephony, telemarketers call indiscriminately. Telemarketing also imposes a significant burden on the functioning of telephone networks. For example, according to information gathered in the USA during the Federal Trade Commission's rulemaking on telemarketing, respondents submitted that, "commercial telemarketers complete over 16 billion calls a year." This is across about 270 million fixed line telephones, which comes to about 60 calls per phone per year.

Given the need to ensure that service providers do not have to use network resources to carry unwanted calls, there is a case from the perspective of promoting efficiency in the operation of telecommunication services in restricting unsolicited calls. The Authority primarily aims to identify the measures it should take to stop the bulk of unsolicited commercial communications to those who do not want it.

Based on the network impacts of telemarketing and other unsolicited commercial communications (UCC), which consume network resources and scarce spectrum, the Authority believes it is necessary to promote efficiency in the operation of telecommunication services and in the use of spectrum by reducing the number of such calls. The Authority also seeks public responses about possible technological improvements in networks that can reduce the number of UCC. In addition to telemarketing calls, the Authority has received a number of complaints from consumers that they receive many unsolicited SMSs from their service providers. Both unified access service licensees (UASLs) and cellular mobile service providers (CMSPs) send messages to consumers about promotional offers, value added services/premium rate services such as ring tones, quiz, and tele-voting, and these messages cause unnecessary disturbance to them during work and at odd hours in the day and night.

Many countries around the world have implemented, or are in the process of implementing solutions to reduce unsolicited commercial communications. Countries such as USA, UK, and Ireland have implemented a do-not-call (DNC) registry. By enlisting on such a registry, subscribers opt-out of receiving telemarketing or sales calls. Australia has recently begun the process of setting up its DNC service. In Hong Kong, a telemarketer has to seek permission of the called party and if denied, cannot call again.

In almost all these countries, there has been a combination of industry effort, regulatory intervention, and even legislation to curb telemarketing activity. The DNC registers are often set up by the regulator or government, with telemarketers paying to access the register and scrub their calling lists to keep them up-to-date and avoid calling listed subscribers. In the case of infractions, subscribers in the USA complain to the regulator

or file suit in court, while in UK they complain to the Information Commissioner. Heavy fines are imposed on violators. In Hong Kong, on the other hand, subscribers complain to their service provider, and the telemarketer can be disconnected if found to be in violation of the rules. Details of different international practices are given below.

6.2 Obnoxious calls

Obnoxious calls are a source of irritation to consumers. Blank and silent calls make the scenario even worse, which may result in severe anxiety to the receiving party. The inconvenience is particularly intense for mobile phone users who are on international roaming because such calls use their chargeable time.

7. Case study on legislation on Anti-Spam, unsolicited and obnoxious calls

7.1. Australia

Australia's anti-spam legislation came into effect on 10 April 2004. The Australian Communications Authority (ACA) was responsible for implementing and enforcing the Spam Act, 2003 and the spam (Consequential Amendments) Act 2003 and has the authority to pursue a number of enforcement options, from issuing warnings and infringement notices, to pursuing court action. A court finding that a contravention of the Act has taken place can order offenders to surrender financial gains, compensate victims and pay penalties of up to A.U. $1.1 million per day. Two separate industry codes of practice - one for the e-marketing industry and one for the ISP industry - have also being developed to complement the Spam Act. The spam regulation approach in Australia is an Opt-in one.

As of 1 July 2005, ACA merged with the Australian Broadcasting Authority (ABA) to form the Australian Communications and Media Authority (ACMA)[19].

7.2 Awareness initiatives in Australia

7.2.1 Scam watch

A clear and lively website designed to inform consumers about various “too good to be true” schemes. Its internet scams section focuses mainly on fraud-oriented spam such as pyramid schemes, ramping and unexpected promotions.

7.2.2 Private awareness initiatives

7.2.2.1 The Internet Industry Association (‘IIA’) National Spam Initiative

The IIA is the national, non-profit, industry organization representing internet businesses in Australia. The "National Spam Campaign" section of its website provides a

[19] ITU Survey on Anti –Spam Legislation Worldwide Document:CYB/06

list of mail filtering services. All cited companies have agreed to commit to a minimum one-month free trial of their products so that users have the chance to try some options and find a solution that works best for them.

7.2.2.2 Australian Direct Marketing Association "Do Not Contact" Service

The Australian Direct Marketing Association represents over 500 companies. The banks, insurance companies, publishers, mail order companies and charities which make up its membership have agreed to cease sending marketing materials, including via e-mail, to any person who may request it. Individuals can sign up to the free "Do Not Contact" service via the ADMA website.

7.2.3 ENFORCEMENT AGENCIES IN AUSTRALIA

7.2.3.1 Australian Communications and Media Authority

The Australian Communications and Media Authority (ACMA) is responsible for the regulation of broadcasting, radiocommunications, telecommunications and online content. Amongst other things it aims to protect consumers and other users whilst fostering an environment in which electronic media respect community standards and respond to audience and user needs.

7.2.3.2 Australian Federal Police/ Australian High Tech Crime Centre

The Australian High Tech Crime Centre (AHTCC), hosted in Canberra by the Australian Federal Police (AFP) aims to provide a coordinated approach to combating high tech crime in Australia. Crimes can include computer intrusions, unauthorized modification of data and the creation or distribution of malicious software (viruses or Trojans). It should be noted that a crime is not necessarily considered 'high tech' because technology has been used, for example frauds that are conducted online are not always regarded as 'high tech'.

7.2.3.3 Australian Security and Investments Commission (ACCC)

The Australian Securities & Investments Commission enforces and regulates company and financial services laws to protect consumers, investors and creditors. It provides general information about spam via its consumer website, FIDO.[20]

7.2.4 Legal frame work on prevention from unsolicited calls in Australia

On 22 June, 2006 the Minister for Communications, Information Technology and the Arts announced that legislation to establish national telemarketing standards and a Do Not Call Register (the "Register") had passed through Parliament. The Do Not Call Register Act, 2006 (DNCR Act) and the Do Not Call Register (Consequential Amendments) Act, 2006 make the ACMA responsible for the setting of the telemarketing

[20] www.oecd-antispam.org

standards and establishing the register on which people can register their telephone numbers to enable them to opt out of receiving unsolicited telemarketing calls. Budget funding of AU$33.1 million has been provided over four years for the arrangements, with industry anticipated to contribute AU$15.9 million over that period through the payment of fees to access the Register.

The standards apply to all telemarketing calls, including voice calls, made to an Australian number to market, advertise or promote goods and services, conduct opinion polling and to carry out standard questionnaire-based research. The standard will not apply to non-telemarketing calls, including non-telemarketing calls by persons that also carry out telemarketing activities (for example, non-telemarketing calls from charities). The ACMA recently released a discussion paper inviting comments on the central issues addressed in the telemarketing standard.

ACMA will be responsible for the enforcement of the legislation and a range of penalties will be available depending on the nature of the breach. ACMA will be able to issue formal warnings or infringement notices or commence court proceedings. Federal courts will be able to impose fines ranging from $1,100 to $1.1 million, with the highest penalties targeted at entities that recurrently breach the legislation.[21]

7.3 United Kingdom [22]

7.3.1 Applicable law

The UK Department for Trade and Industry (DTI) implemented the new anti-spam regulation, based on the EU Directive 58/2002 with the Privacy and Electronic Communications (EC Directive) Regulation, which came into force on 11 December 2003. The enforcement of this new instrument is under the responsibility of the Information Commissioner; however considering that several issues relating to spam also concern consumer protection and trade, the Office of Fair Trading is also active in this field, in particular on the subject of online scams.

• Statutory Instrument 2003 No. 2426 The Privacy and Electronic Communications (EC Directive) Regulations 2003

7.3.2 Government awareness initiatives

7.3.2.1 London Action Plan

The first meeting of the London Action plan took place on October 11, 2004. Though held in the UK, it was in fact an international initiative in which government and

[21] Telecom Regulatory Authority of India Consultation Paper on Unsolicited Commercial Communication

[22] http://www.oecd-antispam.org/rubrique.php3?id_rubrique=43&Valider=ok

public agencies from 27 countries responsible for enforcing laws concerning spam met to discuss cooperation opportunities. Several private sector representatives also collaborated in parts of the meeting

7.3.3 Private awareness initiatives

7.3.3.1 ISPA support of the Worldwide Sweep on Spam

The Internet Service Provider's Association promotes competition, self-regulation and the development of the Internet industry. Its members are subject to the ISPA code, which includes guidelines on spam. As a supporter of the London Action Plan, it was involved with the analysis of a sample of 138,904 spam emails sent to trap accounts. The initiative was designed to identify common spamming practices and routine offenders.

7.4 Enforcement Agencies

7.4.1 The Office of the Information Commissioner

The Information Commissioners Office is a UK independent supervisory authority reporting directly to the UK Parliament. It oversees and enforces compliance with both the Data Protection Act, 1998 and Freedom of Information Act, 2000

7.4.2 The Office of Fair Trading

The Office of Fair Trading is the UK's consumer protection authority. Its website provides information for consumers designed to promote and defend their interests. It also hosts a page specifically about spam.[23]

7.5 Legal framework on prevention from unsolicited calls in UK

The Telephone Preference Service ('TPS') is a central opt out register whereby individuals can register their wish not to receive unsolicited sales and marketing telephone calls. The original legislation was introduced in May 1999. It has subsequently been updated and now the relevant legislation is the Privacy and Electronic (EC Directive) Regulation 2003. The Government receives no money to run TPS. Instead, the direct marketing industry pays for it. The UK Information Commissioner's Office enforces the TPS.[24]

7.6 United States of America (USA)

[23] www.oecd-antispam.org

[24] Telecom Regulatory Authority of India Consultation Paper on Unsolicited Commercial Communication

On 1 January 2004, the Can-Spam Act, which stands for "Controlling the Assault of Non-Solicited Pornography and Marketing Act" came into effect in the United States. This law puts specific requirements on senders of commercial e-mail and places enforcement in the hands of the Federal Trade Commission and State Attorney's General.

7.6.1 Regime: Opt-out.

While many U.S. states have also passed laws addressing spam, they are pre-empted by CAN-SPAM except to the extent to which they address falsity or deception in commercial email messages. CAN-SPAM applies to commercial electronic messages, but not to messages relating to transactions and existing business relationships. It requires all commercial electronic messages to include an indication that the message is a solicitation, opt-out instructions and the physical address of the sender. False or misleading information in commercial email is forbidden, including in headers, subject lines and the message text.

ISPs are exempt from liability under the CAN-SPAM Act. Further, the Act provides a private right of action for ISPs. Violators of the Act can be fined up to US 250 per violation, to a cap of US 2 million, for non-wilful noncompliance; and up to US 6 million for intentional violations, plus unlimited punitive damages for fraud and abuse. In the most severe cases, prison sentences of up to five years are available as penalties.

7.6.2 Government awareness initiatives

7.6.2.1 Federal Trade Commission Spam Homepage

Anti-spam website aimed at consumers and businesses. It features simplified summaries of anti-spam legislation and provides individuals with tips about inbox protection and avoiding common scams. There is also an online complaints form, where spam victims can directly notify the FTC of abusive practices.

7.6.3 Private Awareness Initiatives

7.6.3.1 GetNetWise.org: Spam

GetNetWise.org is a website set up by Internet industry corporations and public interest organizations with the aim of informing individuals about Internet security threats. The spam section of the website features tips, tools and active measures available to those interested in fighting spam. Broadband users can also download explanatory videos about spam.

7.6.4 Enforcement Agencies in USA

7.6.4.1 Federal Trade Commission (FTC)

The FTC is the official consumer protection agency of the United States. It is an independent agency which reports directly to congress on its actions. Tasks regarding the Internet include taking action against irresponsible e-commerce and marketing practices

7.6.4.2 Department of Justice

The DOJ is the government body responsible for enforcing the laws of the US. As such, individuals and companies may refer to it in cases of Internet fraud or violations of the CAN-SPAM Act.

7.6.4.3 Federal Communications Commission

The Federal Communications Commission (FCC) is an independent United States government agency, directly responsible to Congress. It is in charge of regulating national and international communications by radio, television, wire, satellite and cable. As such, when it comes to matters related to spam and the CAN-SPAM Act, its scope mainly covers unsolicited messages on mobile devices. (www.oecd-amtispam.org)

7.6.4.4 Legal framework on prevention from unsolicited calls in US

The Telephone Consumer Protection Act (TCPA) of 1991 was created in response to consumer concerns about the growing number of unsolicited telephone marketing calls to their homes and the increasing use of automated and prerecorded messages. In 2003, the FCC revised its rules implementing the TCPA and established, together with the Federal Trade Commission (FTC), a national do-not-call registry. The FCC also adopted restrictions on the number of abandoned calls9 that are permissible. The FCC and FTC have established a National Do-Not-Call Registry. The registry applies to all telemarketers with the exception of certain non-profit organizations. Commercial telemarketers cannot call a subscriber if that number is on the registry. As a result, consumers can reduce the number of unwanted phone calls to their homes. Subscribers may register their residential telephone numbers, including wireless numbers, on the National Do-Not-Call Registry by telephone or by Internet and at no cost. In addition, there are do-not-call lists at the company and state levels, which allow consumers to block specific calls while allowing others. According to the FCC's Annual Report on the DNC registry, 88 million telephone subscribers have signed up between June 2003 and September 2005.

For the companies who continue to call subscriber after they have requested to be placed on a "do not call" list, some states permit consumers to file lawsuits against violators. Courts can award damages or actual monetary loss, whichever is greater, and increasing if the complainant can show that the caller willfully and knowingly violated do-not-call requirements. States themselves may initiate a civil suit in a federal district court against any person or entity that engages in a pattern or practice of violations of the TCPA or FCC rules.[25]

7.7 India

The Information Technology Act, 2000 (IT Act, 2000) is the sole Cyber Law of India and it lacks on both the counts of Spam Prevention as well as its Punishment. IT Act, 2000 is due for amendment. In the absence of proper law in place, the only recourse is to rely upon the traditional criminal law of India, i.e. Indian Penal Code, 1860 (IPC) that is highly insufficient for cyber crimes in India. Alternatively, a purposive, updating and organic interpretation of the existing provisions of the IT Act, 2000 and IPC by the judiciary must be tried.

India's Information Technology Act 2000, which became effective from 17 October 2000. This Act applies to whole of India, and its provisions also apply to any offence or contravention, committed even outside the territorial jurisdiction of Republic of India, by any person irrespective of his nationality. In order to attract provisions of this Act, such an offence or contravention should involve a computer, computer system, or computer network located in India. The IT Act, 2000 provides an extra-territorial applicability to its provisions by virtue of section 1(2) read with section 75.

India's Information Technology Act 2000 has tried to assimilate legal principles available in several such laws (relating to Information Technology) enacted earlier in several other countries, as also various guidelines pertaining to Information Technology Law. The government of India appointed an Expert Committee to suggest suitable amendments into the existing IT Act, 2000. These amendments, perhaps with some modifications, have been approved by the Cabinet in India on 16th October, 2006 and very soon the amendments will be laid down before the Indian Parliament for suitable legislation.[26]

7.7.1 Spam Regulations in India

At the current point in time India has no specific law on spam. The Bill makes sending of content which is grossly offensive or of a menacing character through a computer or mobile phone a punishable offence. The Standing Committee observed that

---

[25] Telecom Regulatory Authority of India Consultation Paper on Unsolicited Commercial Communication

[26] http://www.prsindia.org/docs/bills/1168510210/1168510210_The_Information_Technology__Amendment__Bill__2006.pdf, http://www.prsindia.org/index.php

the Bill does not adequately address the issue of unwanted commercial e-mails (spam). The Standing Committee stated that the issue of unwanted commercial e-mails (spam) has not been addressed.

7.7.2 Mobile Spam

TRAI issued The Telecom Unsolicited Commercial Communication Regulations 2007 for regulating unsolicited communication under section 11 of the Act. (TRAI website) These regulations only address unsolicited commercial communication over the telecom system.

India is a member Asia Pacific Coalition against Unsolicited Commercial Email ('APCAUCE') CAUCE is the world's largest volunteer anti spam organization, with groups in the USA, Canada, the EU and the Asia Pac region APCAUCE activities include:

1. Technical tutorials and conferences;
2. Speakers include technologists, ISPs, blocklist operators and lawmakers;
3. Annual "Regional Update" meetings that bring together regulators, governments, ISP associations and interested citizens from around the region at an informal round table discussion of anti spam laws and initiatives in the region; and
4. Contribution of public policy papers on spam related issues.[27]

7.8 Fighting Internet and Short Messaging Service Spam in Pakistan

7.8.1 Spam over the Internet

With the effective telecom policies being enforced by the Government of Pakistan duly implemented by the Authority caused rapid advancement and growth in technologies, led to unprecedented growth in the telecom sector in Pakistan. Access and affordability of telecom services have enabled to a greater segment of the population of Pakistan, to enjoy the benefits of the advancing technologies. The issuance of the Broadband policy promulgated in 2004 played a vital role in the proliferation of broadband in Pakistan. Internet access was made unprecedented, affordable to a large number of people. Internet has no boundaries, which makes at an extremely vulnerable mode of communication to such fraudulent attacks. Territorial limitations make it a cumbersome task to regulate illegal activity through legislation. It has been observed globally as highlighted earlier that anti-spam regulation is most effective if conducted with a combination of approaches, which includes anti-spam law, international cooperation and regulating licensees through codes of practices, education and awareness, industry initiatives.

[27] International Cooperation Working together to stop spam in the AsiaPac region APNIC 20, Hanoi, Suresh Ramasubramanian Coordinator, APCAUCE)

Although there is no express provision in the Act that includes the term 'spam' in its literal sense, however, since the Act defines the term 'intelligence' which includes speech, sound, data, signal, writing, image or video' this also includes 'spam'. Plain interpretation of the relevant provision i.e., 4(a) of the Act empowers the Authority to regulate the telecom system and services. Meaning thereby any transmission either data or voice transmitted through telecom system falls within the ambit of Authority. Section 31(d) of the Act expressly prescribes that unauthorized transmission of any intelligence through a telecommunication system or telecommunication service believed to be false, fabricated, indecent or obscene is an offence. In light of the above, it would not be wrong to state that Authority was fully empowered to regulate all transmission of intelligence, which includes spam and unsolicited messages.

Section 14 of the ordinance prescribes the offence of spamming, as reproduced below:

> **Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk to any person without express permission of the recipient, or causes any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.**
>
> **(2) Whoever commits the offence of spamming as described in sub-section (1) shall be punishable with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or fine, or with both.**

The ordinance has an overriding effect on any other law for the time being in force. The bare interpretation of section 46 leads to the conclusion that once the offence of 'spamming' is committed the trial and enforcement of punishment shall be governed by section 46 of the Ordinance which states:

> **"The provisions of this Ordinance shall have effect notwithstanding anything to the contrary contained in any other law for the time being in force."**

In the case titled *Chandavarkar Sita Ratna Rao Asbalata*, the court has thus explained the principle: A clause beginning with the expression 'notwithstanding anything contained in this Act or in some particular provision in the Act or in some particular Act or in any law for the time being in force or any contract' is more often than not appended to a section in the beginning with a view to give the enacting part of the section in case of conflict an overriding effect over the provision of the Act or the contract mentioned in the non-obstance clause. It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned, the enactment following it will have

its full operation or that the provisions embraced in the non-obstante clause would not be an impediment for an operation of the enactment[28].

From the above stated it can be construed that transmitting, harmful, misleading and illegal **unsolicited** electronic messages in bulk to any person **without express consent** or causing any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for **commercial** purpose shall be punishable for **spamming**.

7.8.2 Cause of consultation by the Authority

The Authority has received numerous complaints of spam and the need has been felt to seek views from the stakeholders on controlling spam. Presently, spam is severely affecting the privacy of consumers. It imposes a cost to the receiving party in terms of time and effort to read and delete unsolicited messages in addition to risking loss of legitimate messages in this process.

As per section 4 (1)(c) of the Act the Authority shall:

"Promote and protect the interests of users of telecommunications services in Pakistan"

As per section 4 (1) m of the act the authority shall:

"… protect consumer rights'

Question: Which of the solutions discussed below are in your view the most effective to control spam?

a) Solutions to be implemented by the ISP
b) Solutions focused at the subscriber

Proposal

A centralized solution at the server side will be the most effective since it will be uniform action for all individual users. While from client side, solution would depend entirely on the will of each user, negligence on the part of one user may affect the complete network of the ISP(s) which will mean that a solution yet not a guaranteed solution other users etc.

The Authority is of the view that solutions targeted at the *server side* (ISP) as opposed to methods designed for the client side (individual user), are more effective.

[28] NS Bindras Interpretation of statutes MN Roa,Amita Dhanda,tenth edition

Question: What is Authority's role in regulating spam after promulgation of the Ordinance?

Proposal

The Authority as the telecom regulator has a vital role in curbing the rapid spread of the menace of spam affecting public at large in Pakistan. As discussed earlier a combination of initiatives is required. The role of the Authority is reduce/control spam from being generated. This phase is before enforcing/punishing a spammer. All Internet service providers licensed to establish maintain and operate an electronic information system are responsible under the license conditions to ensure that:

"The services shall not create problem or shall not be unsuitable directly or indirectly as to:-

i. Bring contempt to the country or its people or tends to undermine integrity or solidarity of state;
ii. Violate any provisions of the constitution of Pakistan or relevant of law of Pakistan for the time being in force;
iii. Promote or support sedition, terrorism, anarchy or violence in the country;
iv. Bring contempt to the Defense Forces, Police Force or any other institution of Government of Pakistan or to divulge any secret information relating to Defense and other services;
v. Contain any propaganda in favor of any foreign state having bearing on any point of dispute or against a friendly foreign state;

The service shall not in any way undermine Islam or ridicule, disparage or attack any religion, sect, caste or creed;

The service shall not glorify, vice, crime, violence, black-marketing, smuggling, bribery, corruption or any other social evil;

The service shall not fan racial, sectarian, parochial, linguistic, and regional or class hatred."

Same is the case with WILL licensees and cellular mobile Operators. The Authority feels it the need of the time to take appropriate action to in accordance with the Act, Rules regulations and License conditions to reduce spam.

Question: What in your opinion should constitute the standard operating procedure (SOP) to be prepared by the ISPs under the regulations by the Authority on spam to effectively manage the Spam Problem?

It is proposed by the Authority that the Internet service Providers shall develop an SOP under the regulations to be issued on the subject by the Authority and submit the same for approval. The SOP should include effective provisions to address the following issues:

1. Prohibit **spam, phising and spoofing** on ISPs networks;
2. Support use of spam filters;
3. Suggest updated and effective technological tools for customers and ISPs to fight spam;
4. Responsibility by the ISP to keep tabs on those customers who are engaged in illegal activity and spurn off for premium payments to provide spammers with an onramp on the internet.
5. Certification of the format which the ISPs will use in their advertisements, to ensure customers that the ISP is taking all available steps to protect its customers, and the network at large, from spam.
6. ISPs must block potentially infecting email file attachments. In the case of filtering email or email file attachments based on content properties, in this context prior agreement is to be attained from the customer;
7. ISPs actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately
8. ISPs establish appropriate inter-company processes for reacting to other network operators' incident reports, also accepting end user complaints. .
9. ISPs, communicate their security policies and procedures to their subscribers ISPs and network operators take measures to ensure that only their account holders use their e-mail submit servers;
10. ISPs ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records are responsibly maintained with correct, complete and current information, and that this information includes points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address;
11. ISPs ensure that all their publicly routable and Internet-visible IP addresses have appropriate and up-to-date.

Question: How effectively in your opinion can the technical solutions that are currently available with the rapidly advancing technology, help control the volume of spam currently being experienced by consumers?

Proposal:

The Authority proposes that the following technical solutions may also be adopted for achieving the purpose of this question. The Authority does also acknowledge that these are the currently available/possible solutions which shall be updated by ISP's

on the availability of more effective and achievable solutions, which shall according be communicated to the Authority.

7.8.3 Technical Approaches to Control Spam

a) Black & White Lists

Both these solutions are based on the same technology, having a predefined database which will check the sender of the email address and depending on the result of the query it will allow the email or not. In the case of blacklists it will contain a database of known IP addresses, which send out spam; therefore if the user receives an email from one of those IPs it will reject the email address. Furthermore, these databases will also hold data from known open mail relays as well as open proxies, which could be exploited by spammers.

On the other hand, white lists work in the same way as Instant Messaging software is currently working where it only allows emails from sender who has previously been given permission.

b) Electronic Signatures

Authorized dealers can only give out an electronic signature. This can be a tool used when sending an email to identify that the sender of the email is legitimate. This tool complements the security measures to white lists as it proves the sender of the email.

c) Content and Collaborative Filtering

Content filtering has been widely used in the Internet for parental control systems where based on the level of protection used it will allow to access websites based on their content. It is now also being implemented to try and prevent spam by checking the content of the email, especially the characters, to choose whether an email should be classified as spam or ham.

On the other hand, there is collaborative filtering, which is based on what a group of users, a **neighborhood**, describes an email as spam. For example, if a user receives an email about a Nigerian Advance Fee Scheme and describes it as spam, once a user from the same neighborhood receives that email the filter will automatically filter it out as spam.

d) Bayesian Filtering

It is based on Bayes Theorem of probability. The way it works is similar to content filtering in that it check the content of an email address to decide whether an email is spam or not, but instead of making that decision based a predefined set of words which a user must have set, it is based on the probability of such characters being used in Spam.

Table below shows the main advantages and disadvantages of the different technological methods.

Technique	Advantage	Disadvantage
Black List	· Easy to Implement · Relative high success rate · Block known open relays and open proxies.	· Administrator have control of the IPs that get blacklisted · It does not blacklist a single spammer but an IP · Relatively high level of false positives · Not customized to single user requirements
White List	· Easy to implement · Could help in prevent SMS spam	· Restricting users from receiving emails · Increase number of bounce email · Relatively high level of false positives
Electronic Signature	· Complements implementation of white lists · Low number of false positives	· Cost · Not used widely by web mail companies, like hotmail
Collaborative Filtering	· Can react to changes in spam quite fast · Based on what users believe is spam	· 55% success rate · High level of false positives · Not a unique solution per user
Content Filtering	· Easy to implement · Good for parental control content	· Not very robust · High number of false positives · Low Success rate
Bayesian Filtering	· Highly effective (over 90% success rate) · Solution based on customers individual requirement · Extremely good at handling mad-lib · Very flexible to changes by spammers	· Takes time to train · Large amount of corpus material needed to be effective

Question: What in your view should an ISP's assistance in education and awareness be focused at?

Proposal

The Authority recommends that a customer agreement published on the reverse side of an application form should contain the following information for the awareness of consumers:

How to protect your e-mail address:

- Try not to display your e-mail address in public. This includes Web sites, newsgroup postings or in an online service's membership directory.
- Where a public e-mail address is required, you can request the IT department to create a generic account, e.g. spam.project@oecd.org
- Consider masking your e-mail address. It is simple to add a space just before and after the @ (for example joedoe @ myisp.com), this might prevent harvesting machines and other automatic spamming technologies from recognizing your address. It may however not be advisable to use this system if you need to receive confirmation of a service, for example.
- Decide if you want to use one or more e-mail addresses – one for professional messages, another for newsgroups and directories, etc. Alternative free e-mail addresses can be obtained at most major ISPs.
- Check the Privacy Policy when you submit your address to a Web site. See if it allows the company to sell your address or for which kind of promotional activities it can be used.
- Read and understand the entire form before you transmit personal information through a Web site. Often there are pre-selected boxes saying you agree to receive e-mail from the company's "partners".

7.8.4 How to protect your computer

Do not forget that a spam message may contain more than just a special offer on an important drug. It could also contain a virus, so be extremely careful if you decide to open the message. Should you receive a suspicious e-mail, the best thing to do is to delete the entire message, including any attachments. Then delete it from your deleted items folder. If you have to open an attachment, then the following procedure is suggested:

- Be sure your virus software is up to date
- Save the file to your hard disk
- Scan the file using your anti-virus software
- If no viruses were detected, open the file

It is also a good idea not to reply to unsolicited messages. Hackers and spammers sometimes look for a response to confirm an e-mail address is active, before they add an unwitting user to a distribution list. You can use free anti-spam software filters, such as Spam Assassin or others, to automatically move spam messages to a "junk mail" file.

7.8.5 How to protect your data

- Use secure passwords, change them frequently and do not disclose them over unsecured communication mechanisms, such as e-mail.
- Also additional mechanisms may consist in:
  a) "Lock the door when you leave the house" – Turn off the computer and disconnect from the network if you are not using it.
  b) Do not run programmes of unknown origins. Despite their qualifications, they may install spy ware and other malware on your computer, and even transform it into a remotely run zombie drone.
  c) Report serious incidents.
  d) Help other people in your company to protect their e-mail, computer, and the network (www.oecd-antispam.org)

7.8.6 Mobile /Short message service (SMS) Spam

Mobile phone spam is a form of spamming directed at the text messaging service of a mobile phone. It is described as mobile spamming or SMS spam, but is most frequently referred to as Mobile Spam.SMS spam is also sent through the WLL service phones. Often these messages consist of a simple request to call a number. Normal mobile phone etiquette often results in the call being returned by the user. When they then return the call, they are unaware that they have been fraudulently induced to call a premium-rate line. There is frequently an attempt to get them to hold on the line for as long as possible in order to maximise revenue from this fraud.

Another form of mobile phone/sms fraud is the one-ring fraud, where an incoming call to a mobile phone/WLL phone is timed such that it will ring once (or without any sound at all), and then cut off before the user can answer. This leaves the missed call number on their phone, and the rest of the fraud is as above. In this case, it is the (real or apparent) calling number details which are being spammed to the phone, as these calls are made in the hundreds of thousands by autodialers at little or no cost to the originator, as there is no charge for calls which do not connect. The return number can also be a premium number. Both of these frauds can be combined with other frauds such as the advance fee fraud, as they act as a pre-screening stage for fraudsters to capture the telephone numbers of particularly trusting individuals.

In addition to the legal perspective and approach, this issue requires evaluation on technical grounds as whether it is technically viable or otherwise and input from all Mobile Operators/WLL opeartors before taking any further action. Reduction in taxes by the Government and aggressive competition in this segment of the telecom sector brought about major reduction in the price of a mobile handset, a much cheaper mobile connection and all the more lower call rates. Where the Policy enable/achieved the tremendous growth in the subscriber base, it also gave incentive to fraudulent activity and unsolicited messages in bulk.

Increase in the number of mobile operators, emerging competition pushed operators to offer extensive value added services which would make one service more

popular than the other in the market. Cellular mobile service providers send messages to consumers about latest promotional offers, value added services/premium rate services such as ring tones, sales, new openings and tele-voting, which cause unnecessary disturbance to them during work and at odd hours in the day and at night The consumer is also forced to read and scroll through these messages to locate important messages which results in unnecessary wastage of time and effort. These messages also consume the storage memory in the consumer's handset leading to non-receipt of wanted and important messages. To avoid such an eventuality a consumer is again forced to go through the messages promptly and delete unsolicited messages

To add to this inconvenience are the fraudulent, misleading and harassing messages received from anonymous people/sources.

WLL phones also have the capability to transmit SMS service.

7.8.7 Verification of Antecedents

Authority is entrusted with the following functions:

"(c) promote and protect the interest of users of telecommunication services in Pakistan "

"(m) …….. protect consumer rights"

The Authority has also issued several directions to operators to ensure complete verification of antecedents by consumers in the interest of National security and also to update records incase any illegal activity is being carried out using this medium of communication.

The Authority has also posted consumer alerts on its website to warn consumers of the potential calls and messages as reproduced below:

'Hoax Calls and Falsified / Unsolicited SMS(s)

Be aware of hoax calls and falsified / unsolicited SMS(s) that are being called / sent to subscribers to buy scratch cards and notify scratch number to calling party for prizes of immense value. You are requested to be mindful of receiving hoax / unsolicited calls and SMS(s) notifying that you have won a prize of immense value. However, in order to retrieve the prize, you have to inform the calling party the hidden numbers on the prepaid scratch cards. As a result, you will be deprived of the value of the Scratch Cards.'

7.8.8 Cause of Action for the Authority

Persistent complaints in this regard prompted the Authority to take notice and issue a clarification through media to consumers to beware of the fraudulent activity prevailing in the market.

Question: To what extent have these measures taken by of the Authority helped in reducing Mobile/SMS spam and unsolicited & obnoxious calls?

Operator's views are sought on the feedback they have received.

7.8.9 License Obligations

Enforcing the license issued to a mobile operator ("Operator") by the Authority the operator is under an obligation to take all "reasonable steps to track and locate and prevent the source of harassing, unsolicited, offensive, fraudulent or unlawful communication"

The license condition obliging the operators to control illegal activity reproduced below:

Harassing, offensive, unsolicited or unlawful communication

The licensee shall take all reasonable steps to track and locate and prevent the source of harassing, unsolicited, offensive, fraudulent or unlawful communication. For that purpose:

Any customer of the Licensee may request (the Requesting Customer), the Authority or other duly authorized authority in Pakistan to authorize the Licensee to monitor calls to the Requesting customer's mobile handset or device. The Authority or other duly authorized authority in Pakistan may direct a Licensee to monitor communication to and from a customer's telephone. The Licensee shall provide to the Authority the information resulting from the monitoring of communication to and from a customer's telephone, including the identification number or details of the party or parties that are the source of harassing, offensive fraudulent or unlawful communication and the dates of occurrence of such calls and their frequency; and

The Authority may direct the Licensee to undertake appropriate action to protect the public from harassing, offensive, fraudulent or unlawful communication. Such direction may require the Licensee to co-operate fully with and/or provide relevant information to such other parties identified as being competent authorities by the Authority in its direction. The Licensee shall, at the request of the Authority, terminate service to any customer that is the source of harassing, offensive, or illegal communication"

With the Promulgation of the Ordinance the scope of spam regulation by the Authority has changed. The enforcement of anti-spam law once the offence is committed falls within the ambit the Ordinance, i.e., will be decided by the Tribunal established under section 40 of the Ordinance.

Question: What in your view should the content of a standard operating procedure (SOP) issued by the Authority under the regulations to fight mobile/sms spam?

Proposal

The Authority proposes that the Mobile & WLL operators shall devise a specific SOP for spam on the following guiding principles:

Under the SOP, the mobile & WLL operators shall commit to:

1. Include anti-spam conditions in all new contracts with third party suppliers;
2. Provide a mechanism that ensures appropriate customer consent and effective customer control with respect to mobile & WLL operators' own marketing communications;
3. Work co-operatively with other mobile & WLL operators to address spam issues;
4. Provide customers with information and resources to help them minimize the levels and impact of mobile/sms spam; and
5. Undertake other anti-spam activities to minimize the level and impact of mobile/sms spam[29].

The SOP should display the efforts of the mobile & WLL operators' to combat mobile spam and reduce the impact that it has on customers.

This SOP shall apply to unsolicited communication sent via SMS and MMS (referred to as 'mobile spam') and specifically include:

i) Commercial short messages or multimedia messages sent to customers without consent (e.g. marketing messages).
ii) Commercial short messages or multimedia messages sent to customers encouraging them directly or indirectly to call or send a short message or other electronic communication to a premium rate number.
iii) Short messages or multimedia messages sent to customers in bulk and which are fraudulent (e.g. faking, spoofing or scam messages).

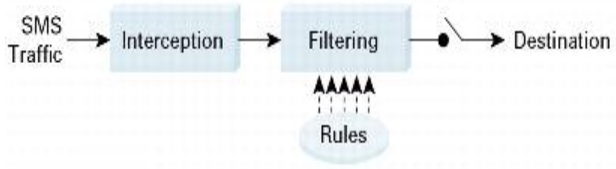
For the purpose of the SOP, "commercial short messages or multimedia messages" mean SMS or MMS messages designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial activity or exercising a regulated profession.

Additional solutions to be incorporated in the SOP are encouraged to help achieve the Authority objectives.

[29] GSM association code of Practice –Mobile Spam February 2006

Question: What technical solutions are available with Mobile & WLL operators to assist in implementing the SOP explained above? Other solutions may also be suggested

One of the solutions is that Mobile & WLL operators can deploy sms spam prevention system on their signaling network, where the system intercepts SMS messages, applies filters to identify spam, and drops offending messages. Following diagram depicts the solution:



7.8.10. Obnoxious Calls

Obnoxious calls can be defined as below:[30]

"*Offensive; Objectionable"*

In accordance with section 4 (1) of the Act the Authority is entrusted with the functions to:

"(c) promote and protect the interest of users of telecommunication services in Pakistan "

"(m) …….. protect consumer rights"

Through license conditions the Authority has put in place a guideline for operators to follow in the event of obnoxious communication, as reproduced in section 7.8.9 of this paper.

The low call rates have on the one hand benefited consumers but this has also facilitated in the illegal activity using mobile communication. One ring fraud, misleading, harassing calls are a source of major inconvenience and botheration for the consumers.

Question: What in your view would be the best approach to be adopted by the operators to curtail at maximum obnoxious calls?

[30] Blacks Law Dictionary

Proposal:

The Authority Proposes that in this regard the operators shall introduce an 'obnoxious call prevention service' where the consumer has dedicated helpline/hotline for registering these complaints which shall be easily accessible to all users instantly for complete resolution the serious complainants can enjoy the service.

The Authority in this regard may in addition also issue necessary regulations and guidelines to protect the subscriber from obnoxious call threats.

A dedicated hotline should be established by the telecom operators to receive complaints of customers to report obnoxious calls. The procedure that should be followed by the operators on the following strictly enforced guidelines:

1. Register complaint;
2. Investigate Complaint;
3. Issue Warning to caller; and
4. Disconnect connection if caller persists.

7.8.11 Unsolicited Commercial Calls

The growth in this segment of the telecomm sector in Pakistan has led to a rise in the use of such services for advertising, marketing and direct sales to reach potential customers. Where such communication is initiated without any consent or request of the receiving party the calls shall be unsolicited.

Question: How effective will a do not call register be for handling unsolicited calls?

Proposal:

It is proposed that a do not call register (DNC) may be maintained by telecom operators. The DNC Register will be a database having the list of all telephone numbers of the subscribers who do not want to receive unsolicited calls. After the establishment of DNC register a subscriber who does not wish to receive Unsolicited calls, can register their telephone number with their telecom service provider to be included in the DNC. Operator shall upload the number to the DNC within 45 days of receipt. The Telemarketer will have to verify their calling mobile numbers list with the DNC register before making a call. An amount of Rs 300/- per call/message should be prescribed to discourage telemarketers who make calls to numbers registered in Do Not Call list. The defaulter telemarketer will face legal action.The impact of imposing a higher charge for calls and messages which have a comercial purpose attached to them will to some extent

ensure that only legiltimate calls are made i.e calls to recipients who do not have any problem with attending commercial calls.

7.8.11.1 Public Awareness

Considering that even a very low rate of response to spam allows spammers to make a profit from their activity, increasing education and awareness is an important part of a comprehensive anti-spam strategy as it helps in reducing the potential "market" for spammers and consequently their financial incentives to continue spamming

A comprehensive anti-spam strategy must take into account end-users, who are the final recipient of spam, the possible victim of viruses and scams, and, at the same time, the persons having control over their computers and personal information. A media campaign should be planned out using which the public at large should be informed, about the spam its sources, and ways to tackle and report spam.

Question: What strategy if adopted for a media campaign would be most effective in creating maximum spam, unsolicited & obnoxious calls awareness and measures to control to the public?

Proposal

The Authority puts forward a media campaign check list which shall be followed by the Authority in collaboration with operators to create spam awareness:

a) Public awareness activities to target users first and foremost, but also large corporations, small and medium-sized enterprises, direct marketers and online operators.

b) General awareness activities to be posted on the Web or other media such as television, newspapers and magazines. Brochures may be distributed in schools, made available on all operators' websites, and also distributed as a leaflet in IT magazines. Educational cartoons about spam, unsolicited and obnoxious calls controlling and reporting and online security broadcast.

7.9 Additional Comments

With the rapidly increasing figures in spam and consequently solutions to curb the same it is important that this subject is taken up in a serious manner for which the Authority would request the stakeholders to provide any additional comments relating to technical, commercial & regulatory aspects of spam that in your opinion are not covered or adequately covered in this paper.