CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT

Consultation Paper
on
Review of
The Telecom Commercial Communications Customer Preference Regulations, 2010

Security in cellular telecommunication framework is important to secure safe communication and signaling data from interception as well as to prevent the cellular telephone scheme from various electronic interferences and threats. The GSM network applies different security techniques but openness of the wireless transmission makes the communicating parties vulnerable to information. It is a well-known that the GSM Network cannot provide several important security services simultaneously. Thus, it is common for this feature to be exposed to some security risks during SMS

contents transmission. Many encryptions standards are being used by mobile operators to ensure the integrity and confidentially of transmitted content.

To gain unfair advantage, an adversary may bribe the server to launch various kinds of attacks --- to convince that an invalid signature held by a client is a valid one (say for providing false information or reputable commitment) or to claim that a valid signature is invalid (say for spoiling the offer provided by an opponent). However, these concerns are not properly captured by existing security models.

In our study we have seen that problem of UCC and "Phishing SMSs " are running simultaneously. So we have to understand both of the situations simultaneously and find out the solution.

Service provider is the principle gate keeper between the UCC and the mobile consumers. It is their responsibility to check UCC. The Legislation should recognize this role and addresses the problem of UCC.

Because of illiteracy and lack of awareness most of the consumers are not aware about NCPR. It can be seen from registration number of PCPR. (Only about 18% are registered) There is no silver bullet to end the UCC or phishing but :

1. **Greater consumer awareness and use of available technological** counter measures clearly hold the greatest promise for curbing these abusive practices.

2. Apart from this, users must have given prior consent before telemarketing SMSs. In other countries like Spain, Italy, U.K., Denmark, Austria etc., the distribution of promotional of advertising communications by electronic or equivalent electronic means is forbidden if, they have not been explicit authorized by the consumer.

ISSUES FOR CONSULTATION

1. What are your views on the proposal of blocking the delivery of SMS from the source or number or entity sending more than a specified number of promotional SMS per hour with similar signatures as proposed in the above Para?

They should be warned three times and then after block immediately.

Other approach is to tackle the problem come from self regulation and software applications by the service provider. (Filter Technologies)

2. What should be the limit on the number of SMS per hour to be specified in this regard? Please give your views along with reasons thereof (para 2.1.1 to 2.1.4).

< 100 SMS per hour

Because :

1. Estimated average number of advertising messages delivered is about 250 to 300/day.
2. Nearly half 46% SMS delivered goes unopened.
3. It may blocks out some worthwhile messages in consumer's mobile.
4. Consumers are mentally screening the messages so it will save the time and improve their productivity.

Traffic congestion:

5. Inadequate infrastructure to support the vast number of subscribers on the network.
6. Too many users on the network.
7. Marketing strategies and pricing schemes also affect traffic behavior since this would have increased the number of subscribers on the network.
8. Use of the old equipment facilities instead of new ones.

9. Although service provider may suffer a loss of business and, indeed, reputation due to continued clogged bandwidth.
10. Typically a record is maximum attempted at 7-10 times.
11. Servers quickly become clogged when inundated with the large volume of SMSs—massive amounts of bandwidth and memory are consumed and associated administrative costs are incurred.
12. **The costs in increasing bandwidth to deal with SMS will simply be passed on to the consumer in the form of higher access fees.**

3. Please give your comments on the proposal to mandate the telecom service providers to obtain an undertaking/agreement from registered telemarketers and other transactional entities that in case they want to outsource promotional activities to a third party, they will engage only a registered telemarketer for such promotional activities. What are the other options available to control such activities? Please give your views along with reasons thereof (Para 2.2.1 to 2.2.3)?

These measures are not sufficient. Following can be included:

1. Technical measures
2. Codes of conduct : (Self regulation)

(a) Consumers can be confident that their personal data and privacy will be respected.

(b) Consumers shall be informed as to how their personal data will be used and informed of their rights thereon.

(c) Sets guidelines such as opt in or opt out systems, limited number of messages, etc.

(d) Prior consent is necessary to send commercial communications. This consent must be a real consent. A simple click in general terms of a contract is not a real consent to use the e-mail address or mobile Telephone number to send commercial communications.

(e) Same Company: Subsidiaries or mother companies are not the same Company.

(f) Similar products: The opinion of the Working Party is that the similarity could be judged in particular from the reasonable expectations of the recipient.

(g) Data non obtained by unlawful manners: The collection of personal data on public Internet places could be unlawful under data protection rules. Etc. etc..

3. Alternative Dispute Resolution Systems.

4. One of the solutions is to use lists of known spammers, and discard messages originating from those addresses or domains.

5. There were several cases where SPs incorrectly blocked legitimate personal communication as unwanted email. Legitimate messages were wrongly tagged as junk mail, half went to junk-mail folders and half was never delivered. Bearing in mind all of the above, we believe a co-operative approach is needed, utilized by Service Providers as the primary gatekeepers between senders and recipients. Further research should be continued in this direction.

The agreement should be a perfect contract, it is not sufficient ask for information about some products or services of the company.

We should also conscious about the problem of " Phishing ". They are sending fraudulent messages which appear to be legitimate business and thereby fooling the recipients into divulging personal information's such as credit card number etc.. While this legislation may provide some assistance in the fight against UCC and Phishing. But it is limited by the global nature of the internet and the ease with which phisher can hide and avoid judgments. Although this act can play a supporting role in the battle. Technological and creating awareness are the most effective means of reducing or eliminating UCC and phishing attacks. In consumer awareness common sense and a healthy level of suspicion go a long way toward not becoming a victim of phishing.

We can face following hurdles :

1. The internet allows anonymous communications that are virtually impossible to trace through internet nodes. Cyber tort favors frequently use falls email headers and anonymous remailers to make it difficult to retrace the steps of wrong doing. Computer records are easy to alter and it is likely that spoliation of electronic evidence is wide spread. No threat of legal action can even hope to effectively reduce the growing phishing problem until; there is some way of finding the phishers.

2. The second hurdle obtaining jurisdiction over the phisher. Cyber crime has always seen across border enterprises. Even if the perpetrator can be located, it is very possible that the person is located in foreign countries where cyber crime flourishes rend to have weak laws dealing with computer crime, low enforcement agencies that lack computer developed apparatus for collaborating with law enforcement agencies in other countries.

3. The solution to the spam problem is not one easily solved. Senders of spam routinely investigate new and innovative ways to avoid having their emails blocked. Blocking spam by using technology can be difficult because what constitutes spam in one organization is often a legitimate message to another.

4. Please give your comments along with reasons thereof on the proposal to disconnect telecom resources after ten violations, of entities for whom the promotion is being carried out? Also indicate whether ten violations proposed is acceptable or needs a change. Justify the same. (Para 2.3.1 to 2.3.3)?

Disconnect telecom resources after three violations, of entities for which the promotion is being carried out . (After giving notice)

We can also think about different jurisdictions may apply widely different interpretations to the term "commercial."

5. What additional framework may be adopted to restrict such subscribers or entities from sending UCC, other than the one proposed above (Para 2.3.1 to 2.3.3)?

In this recent era, it is more evident of emergence and growth of phenomenon known as " Phishing ". They are designing a look like SMSs, E-mails and Websites of well known legitimate businesses, financial institutions and Govt. agencies in order to deceive the mobile usurers into disclosing their bank and financial account information or other personal data. We should know that spammer can send 6,50,000 messages in an hour at virtually no cost. Studies indicate that number of phishing incidences is increasing at an alarming rate i.e. 30% each month and data suggest that phishers

are able to convince up to 5% of the recipients to respond them. Further research has estimated the cost of these phishing attacks on consumer is more than 2.4billion $ worldwide.

It is important to recognize that when message is sent from one point to another, it can follow complex path as it travels through multiple servers. In such cases, the senders are using an unsecured server known as an "open relay "in order to help hide their identity. Despite the best efforts of the investigating team, it is possible; one may not able to determine who really sent the message.

The only way to effective eliminate the phishing problem is to focus on technological changes and have legislation play a supporting role. The possible technological solutions should aim to be:

1. The strong web site authentication
2. The server authentication for source verification
3. Digitally signed with desktop verification. It will verify the authenticity and
4. Digitally signed with getaway verification: it almost indicate to the third recommendation. However instead of relying on the end usurer's to verify, getaway server would verify the signatures before they were even received by the receiver's server.

In short a combination of signed SMS with desktop verification and either getaway verification or server IP verification would solve all aspects of problems for all consumers, business usurers and service providers.

Developing a security application in the SMS market is a critical aspect of the software development from the software engineering view, since proved that the value of the mobile applications begins to assume serious inter-related highly confidential matters and that as a result there are predominantly urgent needs to protect the electronic transmission of data. Furthermore as application techniques are independent from the mobile operator sphere of activity, it can also reduce the security overhead.

Safe mobile application structure or framework should provide different safety features and requirements. It should provide powerful tools for protecting sensitive communications over a public network. it should not imposes an overhead in terms of additional computational processes as, this limitation can threaten the usability of the embedded devices (for example smart phones) with severe constraints on the computational power, battery life and user latency which impose limits on the amount of encryption operations that can be performed without a severe degradation of the device.

For E-commerce:

Service providers, whether involved in e-commerce or not, should provide the following minimum information, which must be easily, directly and permanently accessible:

- The name of the service provider must be given somewhere easily accessible on the site. This might differ from the trading name and any such difference should be explained.
- The **email address** of the service provider must be given. It is not sufficient to include a 'contact us' form without also providing an email address.
- The geographic address of the service provider must be given. A PO Box is unlikely to suffice as a geographic address; but a registered office address would. If the business is a company, the **registered office address** must be included in any event.
- If a company, the company's **registration number** should also be given.
- If the business is a member of a trade or professional association, membership details, including any registration number, should be provided.
- If the business has a **VAT number**, it should be stated – even if the website is not being used for e-commerce transactions.
- Prices on the website must be clear and unambiguous. Also, state whether prices are inclusive of tax and delivery costs.

- Finally, do not forget the overlapping information requirements of other laws:

The other solution may be one that combines industries initiatives such as voluntary labeling and universal exclusion list with technical approaches such as filtering and SMS blocking. Individual users could choose from service providers that supply of various levels of protection from unsolicited messages and ideally service providers could design services individually tailored to each customer's preferences.

6. What are your views on the time frame for implementation of the facility for lodging UCC related complaints on the website of service providers? Please give your comments with justification (Para 2.4.1 to 2.4.3).

Agree with the actions taken by TRAI. But it should be transparent and publicized widely.

7. Do you propose any other framework for registering UCC complaint for easy and effective lodging of complaints (Para 2.4.1 to 2.4.3)?

More and more awareness should be created among the consumers and regular reporting to the TRAI and amendment if necessary.