The Unsolicited Commercial Communications (UCC)Code of Practice for Detection of Voice and SMS Spam ("CoP –Detect")

Index:

A. Foreword:

I. The Telecom Regulatory Authority of India (TRAI) has issued "The Telecom Commercial Communications Customer Preference Regulations, 2018, dated 19.07.2018 "TCCCPR-2018"

II. In terms of Clause 5, TRAI has obligated upon the Access Providers to develop and maintain an ecosystem which inter-alia includes detection, identification and action against sender(s) of Commercial Communication who are not registered.

III. As per Clause 8, TRAI has also mandated every Access Provider to undertake and develop Code(s) of Practice for Unsolicited Commercial Communications Detection (CoP-UCC_Detect) as per Schedule-IV; before allowing any commercial communication through its network(s). Extracts of Schedule IV are enclosed as Annexure 1

IV. This CoP is the outcome of mandate given in TCCCPR-2018 and has evolved with the joint initiative and concurrence of all the Access Providers.

B. Scope

I. This CoP seeks to establish industry wide practices and procedures relating to measures, SOP and process to be followed for detection of spam/UCC which is in breach of the “TCCCPR-2018”dated 19.07.2018.

II. The CoP intends to establish minimum acceptable practices for Access Providers to follow in relation to:

   a. actions to be taken to detect senders sending UCC in bulk against the Regulation to extract information relevant to detect and minimize Spam;

   b. technical initiatives essential to the process of reducing Spam

   c. Build intelligence in system basis the behavior analysis.

III. If there is a conflict between the requirements of this CoP and any requirements imposed on Access Providers by statute, regulation or legally binding or code of practice, the Service Provider will not be in breach of this CoP by complying with the requirements of the statute, regulation or code of practice.

IV. Date of Implementation of this Code will come into effect from_____

C. Applicability

I. This CoP applies to all Access Providers as defined in the TCCCPR-2018.

II. The CoP only applies to all commercial communication sent either by Voice and SMS that falls within the definition of a TCCCPR -2018 via the telecom network of the Access Providers.

III. This CoP is based on the premise that the detection of spam is to be initiated basis the analysis and study of data wrt traffic, complaints, incidents etc:

D. Definitions:

I. In this Code of Practice, unless the context otherwise, the Definition of various terms used under different clauses of the document will be according to the Definitions given under Regulation 2 of the Telecom Commercial Communications Customer Preference Regulations, 2018.

E. Data Availability:

I. All complaints data received by an access providers should be preserved and be available for analysis to initially build and subsequently enhance intelligence measures.

II. Data to be maintained for all reports made by customer within 3 days from the date of receipt of UCC.

III. Signatures created in the Antispam tool and those shared between TSPs from their respective Antispam tools.

IV. Data from Honeypot solution

V. Inputs from any other network element(s)

F. Proposed Detection Methods:

I. Ratio of silent calls to total attempted calls (for Auto dialer cases):

a. TSP to examine Ratio of Silent Calls to total attempted calls (i.e. matured calls) for a registered entity exceeding 1% over a period of 24 hour by an entity using Auto Dialer for Commercial Communications Calls;

b. In case any entity found making auto dialer calls more than above threshold, TSPs to take action against this entity i.e. notice on first instance and each of the subsequent two instances.

II. Ratio of Abandoned Calls to total attempted Calls (Auto Dialer):

a. TSP to examine Ratio of Abandon Calls to total attempted calls for a registered entity exceeding 3% over a period of 24 Hours by an entity using Auto Dialer for Commercial Communications calls;

b. For above, TSP to mandate the Registered Entities using auto dialer not to cross the above threshold. In case, the threshold is breached, the entity to declare the same to TSP. or All such entity should be submitting a monthly report on the abandoned as well as total attempted calls.

III. Signature solutions (pattern detection) and enhancements of signature solutions

a. All Access Providers to identify Signatures, keywords and phrases and ensure that no SMS, having similar signature, from any source or number originating more than threshold to be configured, is delivered through its network. This will not be applicable in case of registered Telemarketers, transactional message sending entity or the telephone number exempted by the Authority, by direction, from time to time.

   For the avoidance of doubt, Signature means contents of commercial communications having same or similar characters or strings or variants thereof, but does not include subscriber related information.

   Criterion : Antispam tool to keep a real-time count of content signatures, and the moment they cross a threshold of xx messages across users, all subsequent SMSs with that signature, after a defined number per SIM, will be blocked for next xx hours. Example : 100 SMS within 10 minutes threshold defined in the system. The moment the signature crosses 100, it will count 5 sms with same signature from any single user and all same SMS beyond 5 will be blocked for that user. Likewise for any other user for the next 48 hours

b. The list /database maintaining the signatures are continuously updated.

c. All Signatures detected from the DL-complaints /reports to be captured periodically after due diligence.

d. All such signatures or new patterns detected or learned by one Access Provider to be shared amongst the Access Providers on weekly basis as per the agreed mode. Let the DL Complaints create a report and send to al APs

e. Use of Artificial Intelligence (AI) to improve Signature Solutions on an ongoing basis for detection and upgradation.

IV. Deploying honeypot(s) and using information collected by it:

a. In terms of TRAI TCCPR, use of honeypots has been emphasized and TRAI has stated as under:

> *In computer terminology, a **honeypot** is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.*

b. TSPs to identify 5 MSISDN from any series (for each LSA) which are not recycled.

Remark: TSPs to comment

c. These numbers to be used for Honeypots solution whereby random calls from any subscriber (normal, UTM, RTM) can land. Such calls are to be recorded for future reference and analyse the usage of such calling numbers for further action.

d. The output of honeypots i.e. CDR analysis and content recorded to be used for investigation and establishment of complaints.

V. Usage Pattern Analysis of reported number and associated numbers:

a. Extract customer call details for last 45 days and check below threshold for spam through SMS/ Call

<u>SMS</u>

i. Average per day Out Going SMS count >=80 (Yes/No)
ii. Out Going SMS contribution in overall transaction was >=90% (Yes/No)
iii. Similar pattern observed >=3 days for SMS and >=5days for Voice in last 45 days (Yes/No)
iv. >=95% recipient numbers were unique in last 45 days (Yes/No)

v. If all the above checks are found Yes, then disconnect the number as per process else we will exclude from UCC action and close under category 'Not a telemarketer'.
vi. Keep associated numbers with suspicious usage pattern under 'restricted usage' and disconnect if required
vii.

Calls

i. If the outgoing calls are concentrated during business hours and there are almost negligible OG calls during night
ii. Define thresholds for number of calls in a day
iii. OG calls >= xx% is suspicious
iv. >=xx% of recipients was unique
v. Average call duration <= xx seconds
vi. Call terminated by B party >= xx%
vii. If all the above checks are found Yes, then disconnect the number as per process else we will exclude from UCC action and close under category 'Not a telemarketer'.
viii. Keep associated numbers with suspicious usage pattern under 'restricted usage' and disconnect if required.

VI. Dictionary attacks:

a. Basis the data of numbers which have been rejected by TSP's.

b. The scrubber (Entity-Scrubber) will ensure identification of this on a best effort basis.

Annexure 1

Extracts of Schedule-IV of TCCCPR-2018

Schedule-IV

Action Items for preparing Code of Practice for Unsolicited Commercial Communications Detection (CoP-UCC_Detect)

1. Every Access Provider shall establish, maintain and operate following system, functions and processes to detect sender(s) who are sending Unsolicited Commercial Communications in bulk and not complying with the regulation(s), and act to curb such activities: -

   (1) System which have intelligence at least following functionalities: -
   a. identifying sender(s) on basis of signature(s);
   b. deploying honeypot(s) and using information collected by it;
   c. evolving signature(s) by learning over time;
   d. interface to exchange information with similar system(s) established by other access provider(s) to evolve signature(s), detecting sender using Sender Information (SI);
   e. considering inputs available from DL-Complaints about complaints and reports and analyze them;
   f. considering inputs available, if any, from any other network element(s) of the access provider system(s);

   (2) provide ways and means for resolving complaint(s) by sharing information related to telephone number(s) of sender(s) against which complaint is made;

2. Every Access Provider shall formulate codes of practice (CoP-UCC_Detect) for system, functions and process prescribed as following: -

   (1) implementation details for detecting Unsolicited Commercial Communications related to suspicious unregistered telemarketing activity using Signature solution, deploying honeypots and other technical measures;
   (2) minimum standards of technical measures to share intelligence information, rules, criteria to detect suspected sources of spam;
   (3) approaches to detect and identify unregistered Unsolicited Commercial Communications sender(s),who are camouflaging themselves by fragmenting their activity across multiple phone numbers;
   (4) approaches for deployment of honeypots to capture Unsolicited Commercial Communications voice call(s);
   (5) approaches to detect and identify source(s) of dictionary attacks;
   (6) timeline(s) for implementation of the functionality referred in code of practice and operationalizing it; such other matters as the Authority may deem fit, from time to time.

3. Report of entities found to be engaged in making or causing to make silent calls, robocalls, abandoned calls or using telephone directory harvesting software to make Unsolicited Commercial Communications, as and when came to notice of the access provider, or as provided for in the regulations for the registered sender(s) with the access providers, on basis of following criteria: -

(a) Ratio of Abandon Calls to total attempted calls for a registered entity exceeding 3% over a period of 24 Hours by an entity using Auto Dialer for Commercial Communications calls;
(b) Ratio of Silent Calls to total attempted calls for a registered entity exceeding 1% over a period of 24 hour by an entity using Auto Dialer for Commercial Communications Calls;
(c) Entity(ies) found to be using telephone number harvesting software for sending Unsolicited Commercial Communications are barred to use their network;