Gmail

rajenderkumarsharma trai <rajendertrai@gmail.com>

Fwd: FW: TRAI consultation paper for 9th NOv 2017

1 message

Sunil Gupta <skgupta2009@gmail.com> Fri, Nov 10, 2017 at 12:38 PM
To: rajenderkumarsharma trai <rajendertrai@gmail.com>

fyi pl.

With Thanks & Regards,
S.K.Gupta,
TRAI

---------- Forwarded message ----------
From: **Ankur Singh** <asingh@mgageindia.com>
Date: Fri, Nov 10, 2017 at 12:16 PM
Subject: FW: TRAI consultation paper for 9th NOv 2017
To: Sunil Gupta <skgupta2009@gmail.com>
Cc: Jitendra Singh <jsingh@mgageindia.com>

Dear Sir,

PFA the suggestion/consultation for Unsolicited Commercial Communication.

Ankur Singh
Senior Manager - Carrier Relations

@: asingh@mgageindia.com | D: +91-22-40556108 | M: +91-98679 06067

mGage
india
Driven by mobile. Powered by insights.

mGage India Pvt Ltd, Unit # 13, 3rd Floor, A Wing, Prism Towers, Mind Space, Malad (West), Mumbai - 400 064.
India
www.mgageindia.com

TRAI COnsultation paper for 9th November.docx
21K

1.) **Categories to be added:**

Transactional
Promotional
Solicited commercial
Govt
Investment messages
2 way communication domestic
ILDO

2.) **Sender ID**:

Today it is getting very difficult to brand a company in allowed6 digitsender ID. for example company named VELTI has only 5 characters but still it is being forced to add one more character which is kind of hampering the branding. Also, the companies like Mahindra & Mahindra, Nishit Desai Law firm etc. cannot be compressed to 6 characters and still be meaningful. Now, if say Mahindra& Mahindra has 10 companies finance/ Automobile/housig/textiles/chemicals etc. then these 6 characters fail to provide the branding. Hence, The sender ID must be of 11 charactersand in that the last 3 characters suffix can be made identifier

e.g. HDFCBANK-AD

The unused characters can be filled with – e.g. if the sender ID is VELTI then the approved sender ID can be VELTI-----AD

Now, the companies which has numerals in their name for eg. Air2web or one97 cannot use any meaningful sender ID. Hence we strongly recommend alpha numeric sender IDs to be approved.

The 11th digit of the sender ID which currently denotes the circle is not required. However, it can be used to identify the category of message. E.g.

- **Transactional** – AT/DT/TT/IT etc
- **Promotional** – AP/DP/TP/IP
- **Solicited commercial** – AS/DS/TS/IS
- **GOVT** – AG/DG/TG/IG
- **Investment messages** – AI/DI/TI/II
- **2 way communication – all media shortcodes and their extension e.g. 56161XXXX must be allowed to be used as sender ID.**
- **ILDO** - AL/DL/TL/IL

However, the sender ID must be allocated by a central repository on producing valid documents say trade license, GST registration etc. along with a declaration of purpose of usage. This information must be accessible to the Telemarketers and the operators to allow whitelisting for only the respective sender IDs for the respective customers.

3.) **Content Originator tracking:**

In current scenario TRAI can track the operator and the telemarketers. These both today are registered with TRAI with an intention of doing business by paying the registration fees. The intent of these organisations is to be in business and be on the right side of the regulatory framework.

The current system has provisions of penalizing only these 2 people in the eco system. However, people who are content originatorsare happy to hop around the market and do all malicious things resulting in penalties on telecom operators and telemarketers (in some cases even blacklisting) and yet are scot free.

The role of Operator and Telemarketer in the whole ecosystem is of a **carrier of the content** being sent. They can put up signature solutions/templates check/keyword filters etc. but still there are incidences where the spammers outsmart the whole logic and intelligence.

To curb this, we need to create an identifier for all such people in the valuechain which identifies the **telemarketer -> aggregators -> resellers -> content originator**.

In this ecosystem only the content originator is the person who is creating and publishing the content rest everyone is mere a career.

TO ADDRESS THIS, we strongly recommend this solution:

i. No operator should give TM resources to anyone who is not registered telemarketer (THIS IS IN PLACE).

ii. ALL the telemarketers must also have telemarketing agreements signed with the aggregators/resellers who are not content originator irrespective of their volume/size etc. and publish the information on the TRAI PORTAL so that, in case of any violation the complete chain can be brought under scanner. Also, this will make the aggregators and resellers more responsible about the business. Without the telemarketing agreement in place if any connectivity is extended at any level then that respective entity must be held responsible for the content origination.

iii. **Content originator** :this can be any enterprise, SME, trust, small shop who wants to send SMS. Since A2P route is co0mpletely commercial hence, it must be mandatory for all such content originator to register and sign up with TRAI along with their PAN, company registration details along with their GST numbers. They must be made to pay a small sum of money say INR 1000/- for this registration in order to track the bank account as well.

Every such entity must be given a unique hash code

The content originator must declare all their sender IDs to be used on the portal along with a brief description.

Every sender ID registered on the portal also must be assigned a unique hashcode which must be extension of Unique ID of the entity identifier.

The content provider must send all its messages using the unique extended hash code assigned for the respective sender ID and not the actual sender ID.

The telemarketer and operator's responsibility would be to whitelist the sender ID only after verifying it from the portal for the respective content originator.

The telemarketer / Operator will replace the extended hashcode with the respective sender ID as per the master registration data.

This will help TRAI to keep a check of all sender IDs being used in the market and have a tight grip on Content originator. In case of misuse that sender ID or all can be provisioned for universal blocking and must reflect real time on the portal.
All operators/telemarketers must be informed about this via automated email.

4.) Cutting short the NDNC registration process:

Moment any one registers /deregisters for NDNC immediately the details must be pinged to all the stakeholders (operators and Telemarketers) **over an API** as it currently happens in the case of media shortcodes.
THE complete incremental data must also be available to be downloaded daily in case of API failure. So that the operators and telemarketers can update their database daily and effective registration/deregistration period can be brought down to under 24 hrs.

Ans1 – The registration and enforcement can be reduced to 24 hrs by implementing real time data processing over API.

Moment any one registers /deregisters for NDNC immediately the details must be pinged to all the stakeholders (operators and Telemarketers) **over an API** as it currently happens in the case of media shortcodes.

The complete incremental data must also be available to be downloaded daily in case of API failure. So that the operators and telemarketers can update their database daily and effective registration/deregistration period can be brought down to under 24 hrs.

Ans2 – The trai application must be mandatorily bundled with the devices for this.

Also, at the time of configuring a mobile for the first time for its settings the customer choice can be asked and can be sent in a templated format to 1909 for registration. Also, this can be a sim hosted feature which can ask for the customer preference over USSD moment a new sim is inserted in the device.

Ans 3 – In case of MNP the new CAF must seek the permission again for NDNC preference.

Ans4- the bulk registration must be allowed either online or via mobile app by uploading company GST /incorporation certificate along with letter of authorization. E.g. while booking a car zoomcar asks the customers to upload their adhar card & driving license via the app. This must be verified by the operator customer center and approve or disapproved or whatever follow up communication can be sent to the enterprise's registered email IDs or in app notification. The backend people verify and the approve or reject the booking.

Ans5 –Additional choices must be scrapped and another category of communication must be rolled out which is **solicited commercial.** The enterprise level opt-ins must be considered for this. Also, a format must be published to seek consent all across to have uniformity and easy verification. As it is mandated for KYC in all other sectors.

Ans6 – After linking the **adhar**number and biometric this will automatically get resolved. Also, in case of enterprises all the details and **eKYC** is there with the operators to initiate the action as per the law of the land.

Ans7 – For Silent calls – the CDRs can be generated by operators or they must put up systems to capture this. In the complaint page this must be given an option about silent calls.

ROBO Calls – Robo call is not a malicious practice as in today's world right from OTP over voice to Prime minister addressing country everything is happening via Robo calls.

Ans 8- Mandated registration of all A2P users described in point 3 will help in tracking down the complete chain of people involved and the content originator as well.

Ans 9 – All the A2P users in any form at any level must be mandated to register and they must be identified by a UID system.

Ans 10 – A central repository must be created as it is done today for Govt exempted Sender ID. The registration of content originator must be charged with INR 1000 at least and a small amount of say INR 100 per sender ID must be charged initially for registration. The payment must be done via online mode or by cheques to track bank account details in case of major escalations. Without registration validation the usage of sender ID must not be allowed. However there must not be any limit on sender ID registration counts.

Ans 11 – a time frame of 3-6 months must be given to all entities to comply. Till then, the business must be allowed to run parallelly with the old system.

Ans 12 –The scrubbing mechanism is running fine it does not need any change as there is no violation on promotional route where already dual scrubbing (one at tm level another on operator level) is happening.

Ans 13 – the sender ID must be allocated by a central repository on producing valid documents say trade license, GST registration etc. along with a declaration of purpose of usage. This information must be accessible to the Telemarketers and the operators to allow whitelisting for only the respective sender IDs for the respective customers.
This will give total control to Content originator to register the sender ID and For TRAI to have complete transparent visibility in it.

Ans 14 - Adding hashcode solution will even resolve the issue of duplicate header identification.

Ans 15 – The current KYC system gives all the necessary details to track down the TMSE.

Ans 16 – Having more categories will help. Also with content originator registration the misuse will subside.

Ans 17- Adding the hash code of the respective sender ID after matching it with central database can speed up the process up as in this case directly the content originator is tracked.

Ans 18 – Multiple medium will definitely add to the ease of complaint resolution if the data is mapped and managed centrally.

Ans 19 – They must not be allowed to complaint as they always have option to register/deregister with 24 hrs TAT as per the process explained earlier over API. Since, now we can track down the content originator in the new system.

Ans 20 – mobile application already has the mobile number mapped to it the complainant just need to feed the date time and content. In case of Voice the calling party number.

Ans 21 – The financial disincentive structure must be relaxed for OAP as well as for RTMS till the Time they are able to furnish all the information of the other resellers/Aggregators (who are also registered now with TRAI and have signed the prescribed agreement with RTMs) and the content originator must be issued notice for misuse.

Ans 22 – unless and until the complete system is designed and implemented to track and identify the content originator the financial disincentives must not change.

Ans 23 – Hashcode tagged to sender ID will help addressing this.

Ans 24 – keyword filters can help here. But it is more important to identify and block the content originators in case of intentional malicious activity.

Ans 25 – Honeypots must be deployed by Operators and keep tracking the errant content providers and accordingly the communication can flow down to RTMs aggregators and resellers to block the content originator.

Ans 26 –Having central repository for all the data will help us identify the content originator and since we will be then able to identify the content originator we can stop misuse of resources.

Ans 27 – We do not support this as this will cause unnecessary delays and technical glitches are bound to happen. Instead as suggested in point 1. the enterprise level opt-in and a unified KYC will help here.

Ans 28 – UNIFIED KYC will mitigate this.

Ans 29 – If we are able to track the content originator and the financial disincentives/penalties/sanctions are made applicable to them the content originator will have to be very careful and will be sending the content responsibly. This will give easy access to the source of UCC and appropriate action can be initiated against them.