Subject: **Fwd: Comments on UCC Consultation Paper**
To: rajender@trai.gov.in

Date: 11/10/17 09:27 AM
From: "Asit Kadayan, Advisor" <advqos@trai.gov.in>

Response to TRAI UCC Consultation from iconectiv &... (272kB)

-------- Original Message --------
From: **Kshitij Lal** <lalk@mnpindia.in>
Date: Nov 10, 2017 8:28:12 AM
Subject: Comments on UCC Consultation Paper
To: advqos@trai.gov.in

Dear Shri Asit Kadyan,

Please find enclosed the comments from our parent company iconectiv and MITS on the consultation paper floated by TRAI on Unsolicited Commercial Communication. These comments are for your kind consideration.

We have given comments on questions that are relevant to us. We would be happy to provide any clarification/ additional information that you may require.

Thanks & regards,

Kshitij Lal

Managing Director
MNP Interconnection Telecom Solutions India Pvt. Ltd.
(iconectiv subsidiary)

Mob: +91 9810297566
Email: lalk@mnpindia.in
Fax: +91 124 4008763

Response to TRAI Consultation paper on Unsolicited Commercial Communication:

Q. 3. In case of Mobile Number Portability (MNP), what process may be needed for retaining the status of customer for preference registration? Please give your suggestions with reasons.

Response: As outlined in the TRAI consultation, there is a delay in de-registration of customer preference from the donor network as well as registration information initiated by the recipient network when a mobile number is ported. This can be achieved by opting for any one the following options

- First option is to get the subscriber's preference from the donor and pass it to recipient using NPC. This can be achieved by further enhancing the UPC validation process for which MITS has recently proposed to TRAI in response to Draft Telecommunication Mobile Number Portability (7th amendment) Regulations, 2017. Per the proposed approach by MITS, donor is required to share details of UPC with the NPC following a request for the same by the subscriber. In that same message from the donor, existing preference of the subscriber can also be added and shared with NPC. On completion of the port request, NPC can share the subscriber's preference details with the recipient for updating the same in the recipient network.

- Second option for TRAI to consider is to enhance the UCC Registration Process, which is detailed in Figure 2.1, to add a step 9b that would download the preferences via a file to the NPC. This new step would download the same file from the National Customer Preference Registry (NCPR) to the NPC. By adding this step to the UCC process, the NPC could then "look up" the number when the porting process was initiated to verify if the customer has indicated his/her preferences. Once the porting process was completed, the NPC would distribute to the recipient network the customer preferences thereby allowing the recipient network to update the customers' preferences immediately.

It should be pointed out that if this additional step was included it would necessitate a modification to the functionality of the existing NPC. However, the adoption of the proposal would eliminate the delay in initiating registration on the recipient network.

Q. 7. What steps may be taken to address the issues arising from robo-calls and silent calls? What are the technical solutions available to deal with the issue? How international co-operation and collaboration may be helpful to address the issue? Please give your suggestions with reasons.

Response: A considerable amount of time has been spent on technical mitigation techniques to Robocalling and Spoofing including White Lists, Black Lists, Smart Phone Applications, Simultaneous Ring, Do Not Originate, Honey Pots, National Do Not Call Registries, etc. However, Robocalling and Spoofing appears to be growing even when these multiple mitigation techniques are used. In the US, there is a technical approach being considered which when deployed, with these various other mitigation techniques, should provide a layer of authentication and verification that would put trust back into the network as well as enabling rapid and efficient traceback for investigation and enforcement purposes. It should be noted that the Federal Trade Commission and local industry bodies explored various approaches to stem robocalling and spoofing. They determined that major changes to the legacy SS7 signaling protocol prevalent in voice network infrastructure was not viable and has thus focused the solution below on next generation IP Multimedia Subsystem (IMS) network interconnection. To be clear, the approach does not require all voice switches to migrate to VoIP, only that the interconnecting trunks between operator networks employ IMS-based VoIP. Furthermore, SMS text messaging generally uses other signaling protocols for Application to Person (A2P) messaging which would require a comparable IP-based approach unless IMS is also adopted for such messaging to consumers.

The approach being considered is entitled the Signature-based Handling of Asserted Information using Tokens (SHAKEN) framework and architecture. The purpose of this industry framework is to provide end-to-end cryptographic signatures for authentication and validation of the telephone identity and related information in an IP-based service provider voice network in order to avoid impersonation of telephone numbers (aka spoofing). The SHAKEN framework and architecture use protocol building blocks developed by the Internet Engineering Task Force (IETF).

TRAI recognizes there has been an increase and proliferation of identity spoofing of phone numbers which has resulted in continuous robocalling for fraudulent purposes. Identity spoofing has the potential to undermine customer’s confidence in the ability of Service Providers to provide a communication service that is simple to use, safe, secure and dependable.

Iconectiv (parent company of MITS), recognized the identity spoofing threat years ago, being an early participant in the US and IETF industry standards groups making significant contributions and investments to create standards and a framework to resolve and close industry vulnerabilities. iconectiv holds leadership positions with the Alliance for Telecommunications Industry Solutions (ATIS) and SIP Forum IP who formed a joint taskforce on Network to Network Interconnect where SHAKEN and related standards committees make substantial contributions to progress both technical and governance direction and resolution. Among our various industry leadership roles, iconectiv also chairs the ATIS Technology and Operations (TOPS) Council which has studied robocalling and spoofing and may prove a constructive vehicle in defining a roadmap for operationalizing SHAKEN as it expands to additional call originators with multi-homed PBXs, plus contact centers, resellers and other entities who would invest to ensure their calls are delivered with full caller ID attestation and unique identification of the originating infrastructure.

- Leadership roles:
    - Board of Directors – ATIS, TIA and SIP Forum\
    - Chair – ATIS TOPS Council
    - Co-chair – ATIS TOPS IP Testbed
    - Editor – ATIS/SIP Forum Task Groups:
        - IP Routing document
        - SHAKEN Governance and Certificate Management document
    -

The standards and specifications being developed in the US are being evaluated by several other countries including Canada and the UK. The international adoption of the SHAKEN/STIR framework would enable the automatic trace back of calls to the switch of origination, regardless of country. The capability exists within the protocols to enable that capability. This would significantly assist the Service Providers, Regulators and Law Enforcement to trace and track robocalls and fraudulent activity.

Q. 23. What enhancements can be done in signature solutions? What mechanism has to be established to share information among access providers for continuous evolution of signatures, rules, criteria? Please give your suggestions with reason.

Response: See answer to Question 7 above as relates to cryptographic signatures. It should be noted that the use of the implementation of signature solutions in the US are not identical to the term and context used by TRAI which appears to refer to traffic “patterns” which might indicates unsolicited commercial calls. This presumes there is sufficient volume of such calls for a statistically meaningful determination that can identify such calls. It is also worth noting that the US industry is investigating techniques to clearly identity when calls are blocked based on deterministic use of reason codes in

the call signaling. Otherwise legitimate commercial callers may have calls blocked and not know the difference between that and other call failures, making it very difficult to address that mis-classification. These legitimate commercial callers also seek transparency with metrics reporting on call blocking and the efficacy of any industry solution. Lastly, they seek a governance process that provides a means to correct any incorrect call blocking. These are all worthy of consideration as TRAI looks to enhance protections from illegitimate nuisance and nefarious calls.

Q. 10. Whether new systems are required to be established for the purpose of header registration, execution and management of contract agreements among entities, recording of consent taken by TMSEs, registration of content template and verification of content? Should these systems be established, operated and maintained by an independent agency or TRAI? Whether agency should operate on exclusive basis? What specific functions these systems should perform and if any charges for services then what will be the charges and from whom these will be charged? How the client database of Transactional Message Sending Entities (TMSEs) may be protected? Please give your suggestions with reasons.

Response: Based on the stated functionality it may be beneficial to build an efficient and scalable centralized system to accommodate the processes mentioned above.

A centralized system takes advantage of support for centralized change and configuration management. Also, centralized management provides automated processes to provision and configure the system and services, monitoring, managing, and reducing cost and effort of operations. It also provides security mechanisms for the detection of anomalous activity both in real-time, as well as reactively during an incident-response event.

In addition to managing the registration of consent and content, some means of proactively ensuring compliance by TMSEs is likely advisable rather than strictly post-incident investigation and ensuing enforcement. With all the mechanisms already in place, TRAI acknowledge that the problem is only getting larger. A technique that ensures TSMEs are always using the constant registry seems worth exploring. A high-level approach could include:

- TSMEs computing and appending a digital signature in the signaling header for their calls and messages that cryptographically identifies the TSME, the registered campaign, and the time of day they scrubbed each campaign against the registry before initiating the traffic.
- Operators could verify the digital signature before delivering that traffic or it could be used solely for investigation of reported incidents in order to ascertain if consumers had opted in or out of said TSME's traffic.

It is recognized that the difficulty is in consolidating documents from all TMSEs to a centralized system, but combining all that data could be accomplished in a phased approach. A centralized approach would be a more efficient and enforceable approach than systems working in a distributed manner.

MITS suggests that such a centralized system could be operated and maintained by an independent agent but that an appropriate Government agency be the procurement organization that selects the agent. For a centralized system to exist, global best practice would suggest it be on an exclusive basis because it would be difficult to manage multiple agencies sharing this information or only having subsets of the information. As an example, the current NPC infrastructure could be utilized to establish such a system. Each of the Telecom Service Providers currently has a provisioning interface to the NPC and the NPC distributes data to each of the Telecom Service Providers. The provisioning interface could be adapted to include each of the required elements as well as utilizing the ability of the NPC to provide distribution to each of the recipients required to have the data.

It is not in the purview of MITS to define the charging methodology but it could be permissible to have a charge for accessing and inputting the data as well as a charge for distribution to the recipients.

The client database of TMSEs would be protected because access would be limited to the agent that was selected. Furthermore, the mechanism to access the information should be via a secure protocol.