

Shri. Asit Kadayan,  
Advisor (QoS),  
Telecom Regulatory Authority of India (TRAI),  
Mahanagar Door Sanchar Bhawan,  
J.L. Nehru Marg, (Old Minto Road)  
New Delhi - 110002, India

**Sub: IBM's Response to the TRAI Consultation Paper on Unsolicited Commercial Communication released on 14th Sept 2017**

Dear Sir,

We thank you for the opportunity to provide our comments in response to TRAI's progress initiative related to initiation of a consultation process on Unsolicited Commercial Communication that needs focused attention to enhance the service quality in our Telecommunications Industry today.

Please find enclosed herewith our comments on the topic with specific responses to the various issues for consultation raised in the paper. We would be pleased to provide further clarifications to our points of view stated here as and when deemed fit by TRAI.

Thanking You

Yours truly,

IBM Global Business Services

## Issues for Consultation

**Q.1 To what extent, time required for registration and enforcement can be reduced? For achieving reduced time lines, what changes in processes or in different entities e.g. PCPR, NCPR, CPDB may be required? Will providing scrubbing as a service for RTM reduces time? Please give your suggestions with reasons.**

### IBM Response:

An efficient registration system should enable i) ease of completion of the registration and ii) the transmission of the registration status to ensure relevant stakeholders are able to receive the updated information in a timely manner

1. The actual process of registration should be enhanced to record the source, timestamp and additional relevant metadata like parent-child, peer or family based relationships that may be relevant in dispute resolutions. The proposed time lag for the registration to become active after a 24 hour delay, as outlined in the paper, is a reasonable recommendation.
2. Post-registration process, the new technology should enable that registration data to be replicated among all sources that are accessed by RTM. This replication can be automated and configured to run several times within the day with business rules (e.g. Overwriting of past registrations with new consent, time sensitivities for certain categories) to ensure single version of the information

Scrubbing as a service should be provided to remove at all points of time to offload filtering requests to the service providing entity, and to restricting the disclosure of the entire numbers database.

---

**Q.2 How to ensure availability of Mobile Apps for registering preferences and complaints and for de-registration for all types of devices, operating systems and platforms? Whether white label TRAI Mobile App may be bundled along with other Apps or pre-installed with mobile devices for increasing penetration of app? For popularizing this app, what other initiatives can be taken? Please give your suggestions with reasons.**

### IBM Response:

Drawing an example from social media platform, a lot of criticism has been received in regards to the ambiguity and inconsistency in enabling users to manage their privacy preferences. At most times, users are left confused in regards to which options, may either completely alienate them out of the sharing economy or on the other hand result in total exposure. On the other hand, the example of consistency needs to be derived from the airline industry whereby most websites of airlines companies or travel aggregators have a fairly consistent layout and appearance.

In order to minimize the guessing for the end consumer, we believe it is imperative for the regulator mandate a consistent privacy management protocol or standard. Our recommendations to achieve the same includes - A common digital platform provided As A Service with APIs that can integrate with individual CSP's apps. The UI within the CSP apps for the registration screens should be simplistic and standardized under regulator guidelines to enable consistency and remove ambiguity. In addition, the embedded tab should enable the users to update and validate their preferences related to their registration.

Our recommendation of maintaining the preferences in the CSP' app is based on the fact that most users manage account, billing and service preferences using native CSP apps. Enabling consistency and simplicity for registration preferences will accelerate the adoption of the enhanced regulations.

**Building a dedicated TRAI App** - A white label TRAI mobile app will need the regulator to invest in technology and resources to ensure smooth functioning and integration of the app with the current infrastructure stack. This will create unnecessary cost and redundant infrastructure for executing a process that can be more easily performed by the CSPs who already have significant penetration with consumers.

The option of a white label app is attractive if it can add value by providing transactional services to the user which are currently not offered by CSPs – e.g. processing of MNP with status tracking, service provider performance and offer comparisons, speed and network tests, location based emergency services data, service outages, complaint and dispute tracking among others.

---

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

**IBM Response:**

Internet and consumer analytics have clearly demonstrated that most industries including fashion, auto, food and travel are subject to trends. This is primarily driven by changing consumer preferences that are influenced by different lifecycle and cultural milestones. This makes it imperative to enable customers to have a system that can process and update preferences in a simplistic manner.

The new platform should be designed to create a digital customer profile that can be controlled, managed and accessed by the consumer. The consumer should have capability to assign access rights to usage or sharing of this data as required. Additionally, the logging of preference update events enables auditability and transparency therefore building additional confidence in the regulatory system and minimize disputes.

The aforementioned recommendation also enables the smooth transition of registered preferences as customers update or acquire additional phone lines or change service providers.

---

**Q.4 How bulk registration may be allowed and what may be the process and documents to register in bulk on behalf of an organization or family? Please give your suggestions with reasons.**

**IBM Response:**

The enablement of bulk registration will require the registration process to be enhanced to include relationship based meta data (as commented in Question 1 above). The requirement is an absolute need and has applicability across users of varying maturity. Some examples include –

1. Ability for parents to limit unqualified solicitations to minors and the elderly
2. Ability for organizations to enable or disable specific service and transactional messages to employees and consumers (e.g. Educational institutions can use the bulk registering feature to provide service messages to students)

The enablement of the process can be done by providing functionality to upload bulk files with predefined templates, through secured channels. Submissions will require the replication of information across all registration databases to ensure all relevant sources have one version of the truth. End consumers should be enabled with the options of being able to review the preferences using the processes and options outlined in Q2 and Q3 above.

**Q.5 Is there a need to have more granularity in the choices to actually capture customers interest and additional dimensions of preferences like type of day, media type(s)?**

**IBM Response:**

Using the current list of DND categories as the baseline, we opine that additional level of granularity needs to be provided to capture customer interests with the additional dimensions mentioned above. The level of granularity will need to be defined based on the following factors – (list below is not all-inclusive)

3. maturity of the underlying mobile technology (e.g. Phone features an capabilities),
4. impact on usage costs (e.g. data usage, SMS cost etc.),
5. scalability vs transaction-time
6. business-need in consideration
7. profiles of the principal beneficiary entities

A word of caution - extreme granularity may be difficult to implement followed by restricted ability related to demarcation of message types, difficulty in detecting violations causing computation, scrubbing service bandwidth overheads.

**What will be impact of additional choices of preferences on various entities like CPRF, PCPR, NCPR, CPDB etc.? Please give your suggestions with reasons.**

**IBM Response:**

Considering the volume of information coupled with the solution considerations outlined in Q1-Q4 above, we recommend a cognitive intelligence system that can gradually mature and factor in additional exogenous data used to validate message content and manage granularity considerations.

**Q.6 Should the scope of UCC regulation be enhanced to include unwanted calls like silent, obnoxious, threatening calls etc. and unauthorized communications.? What role government or constitutional organizations may play in curbing such activities? Please give your suggestions with reasons.**

**IBM Response:**

IBM opines, if possible, that all relevant derivatives of unsolicited communications including silent, obnoxious, threatening calls etc. and unauthorized communications should be captured by the UCC regulations. The standardization of regulations and ownership by a government organizations will 1) provide the consumer a capability to direct its complaints to a centralized authority 2) restrict the unwanted solicitors capability to manipulate the regulation norms.

The app feature outlined in Q2 should enable customers to easily register any calls or messages that are unsolicited. The technology should enable the sharing of this information with the regulator and the CSP to enable corrective actions. The suggested cognitive framework should provide capability to record and analyse these feedbacks in an objective manner that may be used to further enhance the system periodically.

**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.**

**IBM Response:**

In addition to the recommendations above related to reporting and sharing of information between regulators, CSPs and RTM - The registration and authentication process of the new framework should ensure that calls can be made only from some registered numbers. The validation process of the new framework may also ensure that the format of the message / call is approved before distribution. This would considerably help in curbing robo-calls and silent calls.

**Q.8 For robust verification and authentication of telemarketer getting registered, what changes in the process of registration, may be introduced? Please give your suggestions with reasons.**

**IBM Response:**

The new framework should allow the implementation of smart contracts for processing registrations of the different stakeholder entities including Telemarketers. A smart contract enabled registration process may have the feature to tag parent and child entities during the registration process. The registration system should provide certificates to the telemarketers for future robust verification and authentication in the system. These smart contracts may have detailed parameters of registration, as below, to ensure robustness.

Typical Parameters:

1. Demographics - Age Group, Geography Location, Gender, Income
2. User Preferences for TMs and CPs

Resources Parameters:

3. No of SMSes to be sent
4. DND Categories to target
5. No of Calls to be allowed
6. Type of Content to be sent
7. Size of Content

Time Parameters:

8. Start Date of the contract
9. End date of the contract

Commercial Parameters:

10. Transaction values for provider and service enabler
11. Penalty values

The digital registration electronic record should be clearly time stamped and immutable and available for view to end customers to confirm permissions granted for solicitations.

**Q.9 Should registration of other entities such as content providers, TMSEs, Principal Entities, or any other intermediaries be initiated to bring more effectiveness? Whether standard agreements can be specified for different entities to be entered into for playing any role in the chain? Please give your suggestions with reasons.**

**IBM Response:**

Stakeholders / entities should be registered through standard agreement templates / contracts and identifiable for better traceability and governance. This would enable authorized entities only to be involved in the commercial communication.

**Q.10 Whether new systems are required 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 TMSEs may be protected? Please give your suggestions with reasons.**

**IBM Response:**

The tasks related to header registration, execution and management of contract agreements among entities, recording of consent taken by TMSEs, registration of content template and verification of content will warrant the need for newer and smarter technology. Additionally, management and maintenance of the technology will be best served by an independent organization as it will require investment and expertise related to resources and capabilities required for choice of technology.

Enabling TRAI to perform the management and maintenance role will require investments in reskilling and acquisition of technology talent and infrastructure at a significant level. The capabilities of the system to operate 24/7 at high availability as a national utility will also result in upgradation of infrastructure and bandwidth for the same. This would result in a diversion of resources from TRAI's primary objective of improving customer satisfaction by setting up performance standards and norms for telecom stakeholders. Even without the infrastructure management overhead, TRAI will need to add resources to review new streams of data from granular registrations, stakeholder registrations and performance audits of the independent infrastructure agency.

TMSEs should be able to authenticate themselves and operate based on approval from an agency, and they should be able to record consent and verify consent whenever needed. The maintenance and management will require Agencies may need to charge fees of different types to exist in the system, such as a fixed one-time registration fee charged to the TMSE, and recurring fees based on the volume of transactions. Access control can be provided in the system to protect client databases of TMSEs.

**Q.11 Whether implementation of new system should full fledged since beginning or it should be implemented in a phased manner? Whether an option can be given to participate on voluntary basis? Please give your suggestions with reasons.**

**IBM Response:**

Any significant transformation achieves best results when implemented in a phased manner. Phase 1 should be a simplistic proof-of-concept (PoC) that ensures adequate testing of the new system, understanding of issues and

feedback of the system, that can be incorporated before going for further launch. The next production phases of launch should be in sets-of-circles. Likewise, 3 phases may be envisaged to complete the pan-India footprint.

Participation should be mandated to participate to test and comply. However, voluntary participation could be encouraged during a trial period to test the system. In the launch phases, phased introduction of features could be possible. For example, the requirement of processing within 24 hours could be done in stages from 1 week to 3 days to 24 hours. Increasing granularity of message types could be attempted in a phased manner as well.

---

**Q.12 Whether scrubbing as a service model may be helpful for protection of NCPR data? Whether OTP based authentication for queries made by individuals on NCPR portal may be helpful to protect NCPR data? What other mechanisms may be adopted to protect the data? Please give your suggestions with reasons.**

**IBM Response:**

Scrubbing-as-a-Service inbuilt as a check in the new system would be foolproof recommended solution to the above issue. Individual queries on the NCPR portal should also have an OTP based authentication where the OTP is sent to the registered number. That would ensure that only registered entities can perform the queries in the NCPR portal.

The above recommendation is based on the following considerations –

1. SMS based OTP are generally available on phones of all types and do not require advanced technology
2. Scrubbing as a service on a dynamically updated database may reduce any disputes that may result in time lags and provide clear audit logs
3. Databases can be secured using Hardware cryptographic accelerators with tamper-proof cards (HSMs) for key management.
4. Crypto. keys are safe-guarded and never leave container with No ability to install malware programs within the container
5. Application environment isolation via Secure Service Containers that protects data and applications even from system administrators (no SSH)

---

**Q.13 What interface and functionality of NTR system may be made available to Principal entities for managing header assignments of their DSAs and authorized agents? How it may be helpful in providing better control and management of header life cycles assigned to DSAs and authorized entities? Please give your suggestions with reasons.**

**IBM Response:**

The regulation should mandate the registration of intermediate DSAs and authorized agents by the Principal Entities. The agents must register in the system and require to log their activities when engaging in any activity in the system. Agents may be provided a limited duration of access such that access may be revoked or terminated if needed.

---

**Q.14 What changes do you suggest in header format and its structure that may be done to deal with new requirements of preferences, entities, purpose? How principal entities may be assigned blocks of headers and what charges may be applied? What guidelines may be issued and mechanism adopted for avoiding proximity match of headers with well known entities? Please give your suggestions with reasons.**

**IBM Response:**

It is desirable to utilize standard formats (such as based on JSON) and publish them. The header format can be extensible as needed. Limiting the granularity scope can help reduce ambiguity related to proximity match. The header template should enable quick search in a subscriber's handheld.

---

**Q.15 Whether voice calls should be permitted to TMSEs and how these can be identified by the customers? How intelligent network (IN) or IP Multi-media subsystem (IMS) based solutions may be useful for this purpose and what flexibility it may provide to TMSEs in operating it and having control on its authorized entities? Please give your suggestions with reasons.**

**IBM Response:**

IBM does not have any specific points of view here.

**Q.16 What steps need to be initiated to restore the sanctity of transactional SMS? What framework need to be prescribed for those transactional SMS which are not critical in nature? Please give your suggestions with reasons?**

**IBM Response:**

The current technology stack is unable to efficiently review SMS content and filter transactional content from irrelevant data. This is primarily caused due to flexibility in the ecosystem to enable users to define and customize the message templates and use of generic headers. As preventive steps, development of standardized templates and headers will be required as the first step towards restoring the sanctity of transactional SMS. The ambiguity may be further clarified by allocation of a specific phone number series will enable the customer to identify the source and type of message. The standards can be developed into smart filters that can then be further implemented at the CSP network

As a detective measure, analytic tools will need to be used to review and flag messages and providers that deviate from the established mandate.

---

**Q.17 To what extent, present gap between time when UCC complaint was made and time when this was resolved can be reduced? What changes do you suggest to automate the process? Please give your suggestions with reasons.**

**IBM Response:**

80% of delays in dispute resolution are related to inability to stitch the chain of events due to disparate data formats from untrusted data sources. The use of a dynamic shared ledger as a single source of registration data, scrubbing as a service, empowered customers able to manage personal preferences coupled with analytical tools will enable the dispute resolution team to access transaction history on demand.

The actual resolution timings may depend on the nature or type of complaint. The resolution actions can be further expedited by list actions and automate them

---

**Q.18 How the medium of Customer Complaint Resource Functionality (CCRF) with pre-validation of data e.g. Mobile App, Web Portal etc. may be helpful to achieve better success rate in complaint resolution process? Please give your suggestions with reasons.**



**IBM Response:**

A complete CRM functionality may be added to the CCRF where data of the complainant would be pre-validated and tagged to a pre-defined set of complaint type. This would enable correct routing of complaints with automated SLAs for resolution. This CRM-like functionality can be extended to the Mobile App or Web Portal too as a self-service functionality. At advanced stages a chatbot functionality may also be looked into on the Web Portal. The correct tagging of complaints and automated resolution would enable advanced post-facto analysis for accurate reporting.

---

**Q.19 Whether access providers may be asked to entertain complaints from customers who have not registered with NCPR in certain cases like UCC from UTM, promotional commercial communication beyond specified timings, fraudulent type of messages or calls etc.? What mechanism may be adopted to avoid promotional commercial communication during roaming or call forwarding cases? Please give your suggestions with reasons.**

**IBM Response:**

Dynamic registration can be provided for unregistered customers. Filtering mechanisms may be enabled at intermediate nodes during roaming or call forwarding, utilizing processing of standard headers to detect promotional communications. When detected, the header may be modified appropriately, to prevent additional forwarding in the system.

---

**Q.20 How the mobile App may be developed or enhanced for submitting complaints in an intelligent and intuitive manner? How to ensure that the required permissions from device operating systems or platforms are available to the mobile app to properly function? Please give your suggestions with reasons.**

**IBM Response:**

Same response as Q2. Allow multiple options to submit complaints such as Android/Apple phones, complaint desk kiosks, or usage of desktops/laptops to submit complaints, so that users do not submit a complaint about the complaint submission system. Depending on what a user can best access or use, the user may choose the right means to submit a complaint.

---

**Q.21 Should the present structure of financial disincentive applicable for access providers be reviewed in case where timely and appropriate action was taken by OAP? What additional measures may be prescribed for Access Providers to mitigate UCC problem? Please give your suggestions with reasons.**

**IBM Response:**

If the violations are verifiable, the financial disincentives can be automatically enforced and a programmatic review should be possible as well to confirm a violation. Access providers need to request all nodes to register in the system, and log their transactions in the system, so that the UCCs can be verified and traced for appropriate action. If the Access Provider does not have access to intermediate entities, then the (principal) entities that are engaging the intermediate entities should take responsibility for the actions of intermediate entities.

---

**Q.22 Whether strict financial disincentives should be levied for different types of techniques like robocall, auto-dialer calls for UCC? Please give your suggestions with reasons.**

**IBM Response:**

Yes, depending on the nature of the call, these disincentives should be applied. In some cases, a robocall may a legitimate call from a doctor's office reminding a patient of a crucial appointment. Phone users should be given the ability to submit a complaint when they receive UCCs, and when multiple violations are detected from multiple users, then strict financial disincentives must be applied.

---

**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.**

**IBM Response:**

The signature solution capability is equivalent to processing security attacks by detecting patterns, or keywords or phrases. Such a capability needs to dynamically adapt to new methods being used. As new violations are found, the signature solution needs to be adapted to capture new signatures. This should be shared dynamically through a shared network with a shared database across providers.

---

**Q.24 How Artificial Intelligence (AI) can be used to improve performance of signature solution and detect newer UCC messages created by tweaking the content? Please give your suggestions with reasons.**

**IBM Response:**

Cognitive Analytics based Artificial Intelligence may be deployed as APIs into the new system to foster supervised learning may be employed on UCCs flagged by users, so that such UCCs may be analyzed to detect new signatures that need to be processed in the system.

---

**Q.25 How the honeypots can be helpful to detect and collect evidences for unsolicited communications? Who should deploy such honeypots? Please give your suggestions with reasons.**

**IBM Response:**

Honeypots can be deployed to receive and record UCCs, as the message transmitters may not be aware that they are communicating with a honeypot. Different entities such as various access providers can deploy such honeypots. It would be desirable to share information across the entities that deploy honeypots to flag nodes that are engaged in UCCs.

---

**Q.26 Should the data from mobile app or from any other source for registering complaints be analyzed at central locations to develop intelligence through crowd sourcing? How actions against such defaulters be expedited? Please give your suggestions with reasons.**

**IBM Response:**

Analysis can be done at one or more locations so that it is not necessarily centralized. The analysis would be enhanced if done through cognitive analytics solutions of unstructured data. However, only certain entities may be

authorized do perform such analysis when can then be shared across entities that need the information to enable taking action against defaulters.

**Q.27 How the increased complexity in scrubbing because of introduction of additional categories, sub-categories and dimensions in the preferences may be dealt with? Whether Scrubbing as a Service model may help in simplifying the process for RTMs? What type and size of list and details may be required to be uploaded by RTMs for scrubbing? Whether RTMs may be charged for this service and what charging model may be applicable? Please give your suggestions with reasons.**

**IBM Response:**

The complexity is increased but it should be manageable. However, extreme granularity could be discouraged to help ease the computational requirements. Scrubbing as a service will be helpful. A standard data format (such as based on JSON) could be specified by the Scrubbing Service provider, so that RTMs can submit a request based on that. RTMs may be charged based on the volume of transactions and the size of each transaction.

**Q.28 How the cases of false complaints can be mitigated or eliminated? Whether complaints in cases when complainant is in business or commercial relationship with party against which complaint is being made or in case of family or friends may not be entertained? Whether there should be provision to issue notice before taking action and provision to put connection in suspend mode or to put capping on messages or calls till investigation is completed? Please give your suggestions with reasons.**

**IBM Response:**

Traceability of a communication with a log of events related to each communication can help in determining whether it was a UCC or not. A system that securely logs these events can help in processing false complaints in the system. It would be difficult to block submission of complaints of any nature but a high burden of proof and a system that logs the events to provide the proof to dismiss or validate the complaint can help in complaint resolution. It would not be right to assume that an entity is guilty until the proof is provided, but perhaps agreements can have a statement regarding a capping of service when complaints are received, without necessarily fully suspending a connection until a resolution is obtained.

**Q.29 How the scoring system may be developed for UCC on the basis of various parameters using signature solutions of access providers? What other parameters can be considered to detect, investigate and mitigate the sources of UCC? How different access providers can collaborate? Please give your suggestions with reasons**

**IBM Response:**

It may be unwise to share the specifics of a signature solution with all entities, as this would help in creating UCCs that can bypass the signature solution implementations. However, if some access providers decide to work together, then they could selectively share information to help each other via a common secure platform that allows them to exchange information.

**IBM Global Business Services in India/South Asia Contacts:**

**Vishal Awal**

Vice President and Lead Partner  
Communications Leader India/South Asia  
T: +91 98204 55005  
E: vishal.awal@in.ibm.com

**Jitan S Chandanani**

Blockchain Offerings and Engagement Leader India/South Asia  
T: +91 99870 09777  
E: chandan1@in.ibm.com

**Dipayan Ghosh**

Associate Partner  
Telecommunications Industry Practice India/South Asia  
T: +91 97020 55557  
E: dipayan.ghosh@in.ibm.com

**Dilip Krishnaswamy**

IBM Research  
T: +91 90085 53311  
E: [dilikris@in.ibm.com](mailto:dilikris@in.ibm.com)

**Debojyoti Das**

Architect – Blockchain and Cloud Solutions  
T: +91 98306 87434  
E: debojyoti.das@in.ibm.com