Comments on the Telecom Commercial Communications Customer Preference Regulations

June 11, 2018

By **Sandeep Kumar**, **Torsha Sarkar, Swaraj Barooah, Gurshabad Grover**

The Centre for Internet and Society, India

Preliminary

This submission presents comments by the Centre for Internet & Society ("CIS"), India on 'The Telecom Commercial Communications Customer Preference Regulations, 2018' which were released on 29th May 2018 for comments and counter-comments[1].

CIS appreciates the intent and efforts of Telecom Regulatory Authority of India (TRAI) to curb the problem of Unsolicited Commercial Communication (UCC), or spam. Spam messages are constant irritants for telecom subscribers. Acknowledging the same, TRAI has proposed regulations which aim to empower subscribers in effectively dealing with UCC[2]. CIS is grateful for the opportunity to put forth its views and comments on the regulations. This submission was made on 18th June, 2018.

The first part of the submission highlights some general issues with the regulations. While TRAI has offered a technological solution to the menace of UCC, the policy documents has no accompanying technical details. TRAI has not made a compelling case for why Distributed Ledger Technologies (DLTs) should be used for storing data instead of a distributed database. There is no clarity on the technical aspects of the proposed DLTs: the participating nodes in the network, how these nodes arrive at consensus, whether they are independent of each other, are questions that remain unanswered. The draft regulations also mention curbing Robocalls, but technical challenges associated with the same have not been discussed. Spam which are non-commercial in nature remains out of the scope of the current regulations.

The second part of this submission puts forth specific comments related to various sections of the draft and suggests improvements therein.

While CIS appreciates the extension of deadline from 11th June to 18th June, we would like to highlight that the Draft was released on 29th May, and despite the extension, the time to submit comments remains less than a month. Considering the fact that the draft regulations hold significance for the entire telecom industry and nearly 1.5 billion subscribers, TRAI should have granted at least a month's time for the stakeholder's sound scrutiny.

General Comments

Distributed Ledger Technology (DLT)

The draft greatly emphasizes the fact that data regarding Consent, Complaints, Headers, Preferences, Content Template Register, and Entities are stored on distributed ledgers. The

[1] The Telecom Commercial Communications Customer Preference Regulations, 2018 (*hereinafter* TRAI Regulations 2018)

[2] Telecom Regulatory Authority of India (*hereinafter* TRAI), Information Note to the Press (Press Release No. 58/2018), available at <https://www.trai.gov.in/sites/default/files/PRNo5829052018.pdf>

intent is to keep data cryptographically secure with no centralized point of control. However, the regulations do not go into the technical details of the working of these distributed ledgers leading to several potential pitfalls.

As per the draft, every access provider has to establish distributed ledgers for Complaints, Consent, Content, Preference, Header, Entities and so on. There are specific entities mentioned which will act as nodes in the network, and these nodes are preselected.

Whenever a sender seeks to send commercial communications across a list of subscribers, the list is ‘scrubbed’ against the DL-Consent and DL-Preference, to check whether the subscriber has given consent and registered their preference. The sender can only send commercial communication to the numbers which are present in the scrubbed list.

The objective of these regulations is to protect consumers’ rights but the consumer, i.e., the subscriber, is not a node in the distributed ledger. Since the primary benefits of decentralisation are gained when the trust is devolved to the individual subscribers, and the individual users are not clearly specified as participating nodes in the ledger, the justification behind a distributed ledger is unclear.

Additionally, the proposed regime requires the subscriber to place her trust in the access provider to register the complaint, thus offers no tangible benefit over the current regulation. While there are penalties for non-compliant Access Providers (APs), there are no business incentives for APs to expend the extra amount of resources required in for effective implementation of this technology, to act in the users’ interest. This builds a system where APs interests clash with subscribers, but they are nonetheless required to be the guardian of the subscribers’ concerns.

Further, the nodes are entities constituted by the access providers (APs), and there is no mechanism to ensure that they behave independently of each other. In such case, it is wholly possible that all nodes on a distributed ledger are run by the same entity, thus defeating the purpose of establishing consensus. The proposed regulations do not address this scenario.

One solution would be to add subscribers as nodes to the DLT network. But this would be impractical as the technical challenges associated therein, including generating public-private key pairs of each users, computational complexity of the network, are immense. If this is indeed the intention of TRAI, this has not been spelled out clearly in the draft regulations. Additionally, in such a scenario, there would be no requirement for mandating every AP to maintain their own DLT for customer preference and consent artefacts.

Considering the points mentioned above we request TRAI to publish the technical specifications of DLTs, which addresses the following issues:

1. Who can participate in the network other than the entities mentioned in the regulations? Are these participating entities independent of each other? If not, then how will the conflict of interest be resolved?

2. What is the consensus algorithm used in the DLTs?

3. Will the code to implement DLTs be open-source?

Our recommendations are three-fold in this regard:

1. If distributed ledger is used, then mechanisms should be devised to ensure the integrity of the consensus. For this, participating nodes in the network must be independent of each other. Aforementioned points regarding consensus protocol should be taken into consideration as well.

2. In place of DLTs, we recommend use of distributed database with signature-based authentication and encryption of the data to be stored. The immutability and non-repudiation of data can be achieved in this way. Distributed ledgers such as, DL-consent, DL-preference, DL-complaints are instances where authentication of data and subscriber can be done using simplers means such as, OTP verification etc. So, such ledgers need not necessarily utilise DLTs.

3. The regulations should mandate the open-source publication of the implementation of the DLTs. This will enable interoperability, add transparency to the functioning of the regulations, and enable security audits to ensure accountability of the APs.

Broadening the scope of the Regulations to non-commercial communication

The proposed regulations attempts to specifically curb unsolicited *commercial* communications as defined in Regulation 2(bt). But, there are other forms of communication which are unsolicited and *non-commercial*, including political messages and market surveys. [3]

We recommend that the scope of the regulations should be broadened to include both commercial and non-commercial communications. and both of these should be grouped under the category of Institutional Communications. Wherever needed, changes should be made to the regulations dealing with UCC to suit the specific requirements of dealing with unsolicited non-commercial communications as well. At the same time, the regulations should ensure that individual communications are not brought within their ambit.

Technical challenges in combating Robocalls

Robocalls are defined in Regulation 2(ba) and in Schedule IV, provision 3, it has been clubbed with other kind of spam. However, there are some specific technical challenges in regulating robocalls. Right now, ‘block listing’ is a prevalent model where one can identify a number and then block it so that it cannot be used further.[4] But with robocalls, spoofing of other numbers

[3] TRAI, ‘Consultation paper on Unsolicited Commercial Communications’ (*hereinafter* TRAI - Consultation Paper], Page 21

[4] Lily Hay Newman, ‘The Robocall Nightmare is Getting Worse - But Help is Here’, 20th November, 2017, *Wired*, available at <https://www.wired.com/story/robocall-getting-worse-but-help-is-here/>

is easy achievable which makes the blocking of the real identity of caller difficult. The proposed regulations do not adequately address this challenge.

The Alliance for Telecommunications Industry Solutions, with working groups of the Internet Engineering Task Force (IETF), has been working on a different approach to solve this problem. They are working on standards for all mobile and VoIP calling services which would enable them to do cryptographic digital call signing, “so calls can be validated as originating from a legitimate source, and not a spoofed robocall system. The protocols, known as ‘STIR’ and ‘SHAKEN,’ are in industry testing right now through ATIS's Robocalling Testbed, which has been used by companies like Sprint, AT&T, Google, Comcast, and Verizon so far”.[5]

TRAI should take into account these developments and propose a specific regime accordingly. One possible way forward for now could be the banning of robocalls unless there is explicit opt-in by subscribers.

Registration of content-template

The draft envisages a distributed ledger system for registration of content template which would have both a fixed part and a variable part. The content template needs to be registered by the content template registrar, which would be an authorized entity.

Problematically, the content template is defined to include the fixed part as well as the variable part. Further, Schedule I, provision 4(3)(e) mandates that content template registration functions should be utilized to extract fixed and variable portion from actual messages offered for delivery or already delivered. Variable portion of the message contains information specific to a customer, as defined in regulation 2(q)(ii). In addition to privacy concerns with accessing the variable part, there is no functional reason for variable portions to be extracted from the actual message, as only the fixed portion needs to be verified.

The hash[6] of the fixed portion of the message can be used to identify whether a user has received UCC or not. We therefore recommend that the variable portion of the message shall not be made accessible to entities because it is not required for the identification of a message as UCC.

‘Safe and Secure Manner’

Throughout the draft, reference is made to the data collected being stored and/or exchanged in a ‘safe and secure manner’, without any clarification to what this term implies.

We recommend that the term be defined as ‘measures in accordance with reasonable security practices and procedures’ as given in section 43A of the Information Technology Act, 2008 read with section 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[5] Ibid

[6] TRAI Regulations 2018, Schedule I, provision 4(3)(e)

Bulk Registration

In the Consultation paper published by TRAI[7], bulk registration was envisaged as a way to curb UCC wherein one member of the family can register on behalf of the family. Australia has already implemented this mechanism.[8]

In India, evidence suggests that major victims of spam are the elderly and people with limited financial capacities.[9] In such cases, consent and preference registration on behalf of these people by one person, may help in successful control of UCC.

Some telecom service providers argued against this by emphasizing on the individual choice of a subscriber.[10] However, in cases where there is authorization given by the customer, the primary user can register consent on his/her behalf.[11] Similarly, since corporate connections are by definition owned and paid for by corporates, bulk registration in those situations can be also be done.[12]

We recommend that given the situation in India, the provision for bulk registration be incorporated in the regulations for specific scenarios, as mentioned above. An authorization template giving the nominee power to register on behalf of a class can be incorporated to this effect. Also, an opt-out option must be incorporated in case an individual choice differs from the choice registered in the bulk-registration.

Specific Comments

Inferred Consent [Regulation 2(k)(II)(A)]

Comments

Regulation 2(k)(ii)(a) of the Draft defines consent as “voluntary permission given by the customer to sender to receive commercial communication”. However, the draft also includes, “inferred consent”, which is defined as consent that can be “reasonably inferred from the customer’s conduct or the business and the relationship between the individual and the sender”.

[7] TRAI - Consultation Paper (n 3), Page 12

[8] Australian Communication and Media Authority (ACMA), ‘Bulk applications: register, remove or check’, available at <https://www.donotcall.gov.au/consumers/bulk-applications-register-remove-check/>

[9] Debashis Sarkar, ‘5 Common Types of Scam Calls and How to Deal with Them’, *News18*, available at <https://www.news18.com/news/tech/5-common-types-of-scam-calls-in-india-and-how-to-deal-them-1366587.html>

[10] Reliance Jio Infocomm,‘Comments on Consultation Paper on ‘Unsolicited Commercial Communication’ dated 14.09.2017’ (*hereinafter* Jio - Comments) available at <http://trai.gov.in/sites/default/files/Reliance_Jio_Infocomm_Ltd_14112017.pdf>

[11] Bharti Airtel Limited, ‘Response to Consultation Paper on ‘Unsolicited Commercial Communication’, available at <http://trai.gov.in/sites/default/files/Bharti_Airtel_Ltd_10_11_2017.pdf>

[12] Jio - Comments (n 9)

When consent is derived from the customer’s conduct, rather than being given explicitly, it defeats its ‘voluntary nature’. The provision of consent being ‘reasonably inferred’ from the customer’s conduct is also vague, and there is no indication given in the draft as to what kind of conduct would lead to a reasonable inference of implied consent. The definition can also be interpreted to mean that customer’s conduct will be subject to monitoring, which raises privacy concerns.

Recommendations

Consent shall not be be derived from the customer’s conduct unless the person provides it explicitly. We recommend amendment to the definition of ‘inferred consent’ accordingly.

Three years history to be stored in DL-Complaints [Regulations 24(3) and 24(4)]

Comments

Regulation 24(3) and (4) states that the DL-Ledger for Complaints (DL-Complaints) shall record ‘three years history’ of both the complainant and the sender, with details of complaints made, date, time and status of the resolution of the complaint. It is not clear from the regulation whether the mentioned set of data is exhaustive or not.

Recommendations

We recognize that the legislative intent behind drafting Regulation 24(3) and (4) was to curb frivolous or false complaints, which has already been a concern of TRAI.[13] Storing both the complainant and the sender’s history, in such cases, may aid in resolving of these.

We recommend that the language of the regulations may be amended to “three years history *which only includes* details of all complaint(s) made by him, with date(s) and time(s) . . .”, thereby giving a limiting qualification to the broad scope of the term.

Responsibility of the APs to ensure that the devices support the requisite permissions [Regulation 34]

Comments

Regulation 34 mandates that the APs are to ensure that the devices “registered in the network” shall support the requisite permissions of the Apps under this regulations.

In terms of jurisdiction, regulation of the functioning of electronic devices (which can be phones, tablets or smart watches) is outside the scope of the proposed regulations, and probably out of TRAI's regulatory competence.

Even if TRAI can impose the regulation on end devices, this regulation puts the burden on the APs to ensure that devices support the pertinent app permissions. Considering that TRAI

[13] TRAI - Consultation Paper (n 3), Page 48

itself has been weighing legal recourse against device manufacturers on similar grounds[14], it is unclear why TRAI assumes that APs have any legal or technical method to ensure control of a device which has neither been manufactured by them, nor is it under their physical or remote control.

In modern smartphones, the end-user has full control over most app installations and permissions. This practice is consistent with a consumer's autonomy over the device and its functioning. Considering the fact that TRAI has not implemented basic security features in the 'Do Not Disturb' app[15], TRAI is putting at risk the privacy of millions of device owners by legally mandating permissions for an app with the second proviso. The proviso further gives TRAI the power to order APs to derecognise devices from their network. This regulation is draconic and inimical to the rights of consumers, who are at risk of losing network access and connectivity because of their device choice, which is a completely different business and market.

Recommendations

Reporting unsolicited messages or calls is a consumer right, and the regulations are in furtherance of the same goals. TRAI should enable consumer rights by giving subscribers the option to report spam, and has no reason to force users to report spam possibly through legal overreach and privacy invasion. Accordingly, we recommend the removal of Regulation 34.

Additional Suggestions

Consumer and subscriber

The usage of the terms ‘customer’ and ‘subscriber’ in Regulation 3(1) implies that the terms have two different meanings. This interpretation, however, clashes with the actual definition given in Regulation 2(u) and 2(bk) , whereby a customer is a subscriber. This is an inconsistent interpretation.

Either the definition of a ‘customer’ must be clarified or differentiated from that of a ‘subscriber’ in regulation 2, or regulation 3 must be amended to indicate what its actual object of regulation is - the customer or the subscriber.

Drafting misnumbering

There are a few instances of misnumbering of regulations and reference regulations which are non-existent.

[14] ET Bureau, ‘Trai weighs legal action against Apple’, April 06 2018, <https://economictimes.indiatimes.com/news/company/corporate-trends/trai-weighs-legal-action-against-apple/articleshow/63637278.cms>

[15] Anand V, Untitled, Twitter, <https://twitter.com/iam_anandv/status/979625276391923715>

1. Regulations 25(5)(b) and (c) make a reference to regulation 25(3)(a), which does not exist in the given draft. A bare reading of regulation 25 however indicate, that the intention was to refer to regulation 25(5)(a), and as such, this misnumbering should be rectified.
2. Regulation 34 makes a reference to regulation 7(2), which again, does not exist. In such case either regulation 34 or regulation 7(2) must be amended to keep a consistent interpretation.

Ambiguous terms

‘Allocation and assignment principles and policies’ - Provision 4(1)(a) of Schedule I of the regulations indicate that header assignment should be done on the basis of ‘allocation and assignment principles and policies’, without any clarification to the meaning of this term. We recommend an amendment to this provision accordingly.