Response to TRAI’s Consultation Paper on Introducing Calling Name Presentation Service

Date: Dec 11, 2022

To,
Shri Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing),
Telecom Regulatory Authority of India

Dear Sir,

With reference to the Consultation Paper on Introducing Calling Name Presentation (CNAP) services in Telecom Networks, dated Nov 29, 2022, please find enclosed my response to the Consultation Paper.

I hope that my submission will merit your kind consideration and support.

With best regards,

Parag Palsapure
Navi Mumbai
pparag@yahoo.com
+91-9322662040

Background and Summary Of Response:

1. I fully support introducing the CNAP service on telecom networks, as I have been a victim of spam from several unregistered telemarketers bypassing the DND registry. A couple of spammers, when complained via TRAI DND app, even made revenge calls, bombarding me with hundreds of calls from different numbers, registering my mobile number on different websites without my knowledge, so that their telemarketers too bombard me with calls/SMS.
2. There are frequent cases of impersonation, phishing and frauds, where individual mobile callers claim to be calling from a known bank and collect pieces of data through using unsuspecting questions, which can be compiled into comprehensive data about the user’s financial profile, bank/account details, behaviour, naivety and carry out financial frauds.
3. Some mobile OS provider (esp Android) claim to provide spam protection, however I found it be ineffective in curbing the menace of spam calls, phishing and frauds. Additionally, untrusted and potentially rogue Android apps claiming to provide caller’s name / spam protection themselves obtain irrelevant excessive permissions from user. In fact, on obtaining excessive permissions (without which the app refuse to work at all), app makers abuse the personal data.
4. It is therefore necessary, that in the interest of telecom users, users be made aware of the callers. I strongly believe that just presenting the name of caller is not adequate, I recommend a step beyond additional information in a practical and easy way (with potential for generating additional revenue), and is mentioned in my response.
5. It is also necessary that database telecom users (MDN+Caller’s name) need to be protected from being abused for selective targeting users of communities (recognized from names/patterns) and in Social and National interests. I have made some suggestions on making it most difficult to allow such data to compiled by untrusted entities.
6. I hope TRAI will consider the identified potential risks and suggestions to mitigate these in a constructive way. Ofcourse, with a bit of more thought and discussions, improved solutions can be found.

Response to the questions on Consultation:

1. **Whether there is a need to introduce the Calling Name Presentation (CNAP) supplementary service in the telecommunication networks in India?**

Response: In order to minimize incidents of impersonation (i.e. callers using fake names or claiming to calling on behalf of some other entity), spammers, scammers or fraudsters, it is absolutely necessary to introduce the feature of "Calling Name Presentation" on all telecom networks in India, and must be made mandatory for all the mobile and landline services in a phased manner, beginning with mobile services.

CNAP service must present the full name of the entity as registered for obtaining the telecom service for Individual callers, i.e. as mentioned on the CAF (customer Acquisition Form) initially. Launching the CNAP service will provide an opportunity to weed out several impersonators, who utilize telecom services with stolen documents, false/expired addresses/IDs, phones handed over to some other entities within a family/company etc (e.g. prepaid SIM's in possession of temp employees/servant/drivers etc for several years. Therefore a mandate for verification of user details at an appropriate time can be used to eliminate significant amount of inaccurate data.

If the calling party's telecom service is subscribed in the name of non-individual, i.e. a company, proprietary firm, government organization etc, the name of the registered entity must be presented in the first phase. However, just presenting the name of entity as indicated in the CAF is not sufficient, especially for non-individual entities. Caller may not necessarily be identified correctly using the name in the CAF alone.

TRAI should make it mandatory that all ***non-individual entities register the telecom services with proper entity name along with the department/role of individual who primarily will use the service, so that the called party can take informed decision whether to accept or reject calls or develop/use appropriate filters.*** For example, a non-individual should append the name of department, location or name of an individual to the Entity Name as indicated in CAF, so that appropriate and useful details can presented as follows "NameOfCompany MumbaiSalesOffice" or "NameOfCompany - Mr. NameOfPerson" or "NameOfCompany DepartmentLocation NameOfPerson". Such mandate of format of registration of CNAP name will allow a called party to reject unsolicited Marketing calls (and potentially phishing calls) from irrelevant locations (city) but can still accept Service related calls or messages from relevant company, bank or institution from the bank's location or headquarters.

For calls originated from Public Telephone Booths, Name of entity and location/address of booth of the Public Telephone Booth may be presented on the called party's device.

TSPs may be suggested to add different flags as prefixing the CNAP ID with a special character, e.g. a prefix of

"@" or Unverified caller flag for calls which are originated from another network (e.g. VoIP calls, international calls etc) or networks not under jurisdiction of DoT/TRAI. Such tag can also be used fr CNAP data collected from some unregulated third party or crowdsourced / public data, if trustworthy/verified data could not be obtained from the originating TSP's database (fall-back option).

"#" for calls originated from Public Telephone Booths etc.

"~" if the CNAP database / registered entity name is old or unverified (e.g. non-Aadhar KYC, or KYC done over 3 years back using temporary address for prepaid customers / expired ID proof / person known to be dead, excessive abbreviations or improper format used in name, vernacular format etc or any such reasons). Can be used for indicating legacy non-updated name in CAF.

"-" or negative sign indicating an entity against whom more than 10 complaints of DND violations have been registered over the last 3 months or over 20 DND violation complaints over 12 months. This will help people identify potential spammers and reject calls in an informed way.

Using such prefix characters as above, **additional features such as 'Verified' tag** (e.g. prefixed with "*****" and **"Category" tag** (prefixed with "**^**" + CategoryNamePrefix) etc can be explored by Telecom Operators, which ***can provide them opportunity for additional revenue.***

A verified tag on Twitter is considered premium and highly desirable by reputed corporates, banks, government entities, important personalities etc. Vocie Calls or Messages from verified, rather **"TRUSTED" entities** (where the 'category – e.g. regulator approved Bank/FI/Stock broker/Agent, School/College, Govt department, Utility/TelecomProvider, Public Safety office etc) will help telecom subscribers to minimize chances of sharing any sensitive personal data or respond to any impersonating entities, thereby further minimizing chances of financial frauds or criminal activities.

2. **Should the CNAP service be mandatorily activated in respect of each telephone subscriber?**

   Response: CNAP service should be provided free of cost and mandatorily activated for the user by default on subscription of any service, without needing any specific request from customers, in order to protect interests of everyone and for national security. The CNAP service remain active until the telecom service is active (even if only incoming voice/SMS services only are active due to exhaustion of prepaid balance or delayed payment for postpaid services).

   However, customers can ask the telecom operator to NOT PRESENT it with CNAP name of others due to any compatibility issues on called party's handset handset firmware, or for testing apps being developed etc. Telecom operators should provide options via IVR, USSD, call center, Internet website and provider's app to temporarily deactivate and re-activate CNAP service to enable subscriber to deal properly on compatibility of legacy handset/device or apps that work purely on CLI.

   Such deactivating CNAP service should not stop their own registered names to be presented on devices of other called parties.

3. **In case your response to the Q2 is in the negative, kindly suggest a suitable method for acquiring consent of the telephone subscribers for activation of CNAP service**

   Response: Please refer to Response-2

4. **Should the name identity information provided by telephone consumers in the Customer Acquisition Forms (CAFs) be used for the purpose of CNAP? If your answer is in the negative, please elaborate your response with reasons.**

   Response: Please refer to Response-1 above.

5. **Which among the following models should be used for implementation of CNAP in telecommunication networks in India?**

   Response:

Model 2, where each TSP maintains database of own subscribers, provides read-only access to other authorized TSPs on demand, is preferred. Security measures can be deployed by each TSP to minimize abuse and overload of systems, where originating TSPs will respond to query on CNAP ONLY for the relevant caller-ID and ONLY WHEN a call/SMS is verified to have been originated from the originating TSP, so that chances of TSPs gathering subscriber data (for marketing/targeting or any purpose) through multiple / frequent / irrelevant requests can be minimized. Responses can be in encrypted form if transported over Internet. TRAI may further issue rules to ban caching of CNAP data by terminating TSP, responsibly handling and purging CNAP data after it's presentation on terminating TSP's network. (To avoid compilation for targeted harassment, described below)

Model 3 should be highly discouraged, UNLESS this third party is an entity created specifically and regulated by DoT/TRAI in providing centralized 'CNAP' data or "KYC" (Know Your Customer) database similar to Financial Services, or is owned/operated by the association of TSPs and regulated (Model-4, but with very high penalties/cancellation of licenses on violations of any rules) OR a government operated entity such as UIDAI (for individuals). Following are some of the reasons for discouraging Model-3:

1. Highest risk of sensitive data of customers is being handed over to untrusted third party for establishes and operates a centralized CNAP database. This third party may e inexperienced, or have inadequate data security measures (in spite of all claims), or intentionally sells/shares data with additional parties without customer consent, and which can be used to target (for harassment/influencing/advertising or even harm) certain communities/people with certain names/gender etc or enable impersonation. All these can be carried out without the risk of being severely penalized as losing the TSP license which has a much larger impact on promoters than loss of a few thousand dollars as penalty for violations. These selective targeting can pose a serious threat to National Security too and must be discouraged.
2. Risk of data on third party CNAP data going out of sync with TSP's CAF data. Customer may have terminated or modified a service, ported to another TSP, transferred the name to another entity (e.g. due to death of an individual, termination of employee, closure of department/office/entity or any reason etc). This has possibility of providing incorrect or obsolete CNAP to the called parties (even if for a small period), and can also be used as a loophole by some people with wrong intentions, thereby bypassing the whole purpose of providing reliable name or description of the caller.
3. May not provide the sense of trustworthiness to users. Even today, a presented caller-ID and associated name stored in called party's phonebook is considered more trustworthy than some random name provided by TruCaller or other such third party apps which are based on crowdsourced data. Please also see the point related to tagging or prefixes in Response-1 above, and such feature of tagging/verified data may only be possible with TSPs maintaining database of their own subscribers.

TRAI may also consider issuing guidelines for relevant IT and Data Protection Bill that individual data (caller ID + name) be considered sensitive personal data and be protected under the relevant acts/laws.

6. **What measures should be taken to ensure delivery of CNAP to the called party without a considerable increase in the call set up time?**

Response: Use of modern databases (multiple, geographically distributed servers with load balancing) and access of CNAP data over IP network will not introduce significant latency when compared to mobile paging, response from called party. In fact, this CNAP would be faster than apps like TrueCaller which may be querying servers geographically much further with higher transit latency. Benefits of CNAP are significant and with correct implementation, I hope that the increase in call setup time (when both called and calling party are on different networks) will be negligible and well within acceptable limits. In case of excessive delays, selective caching of data related to non-individual IDs (e.g. Corporates/commercial entities/Toll-free nos) may be permitted, as this data is far less sensitive and unlikely to be abused by anyone for ‘targeting’ as mentioned earlier.

7. **7 Whether the existing telecommunication networks in India support the provision of CNAP supplementary service? If no, what changes/additions will be required to enable all telecommunication networks in India with CNAP supplementary service? Kindly provide detailed response in respect of landline networks as well as wireless networks.**

   Response: TSPs should be in a better position to respond to this question.

8. **8 Whether the mobile handsets and landline telephone sets in use in India are enabled with CNAP feature? If no, what actions are required to be taken for enabling CNAP feature on all mobile handsets and landline telephone sets?**

   Response: Handset makers should be in a better position to respond to this question.

9. **Whether outgoing calls should be permitted from National TollFree numbers? Please elaborate your response.**

   Response: As long as CNAP is provided for all outgoing numbers, it would be irrelevant if the toll-free numbers are “incoming only” or have “outgoing call” facility too.

10. **In case the response to the Q9 is in the affirmative, whether CNAP service should be activated for National Toll-Free numbers? If yes, please provide a mechanism for its implementation**

    Response: TSPs should be in a better position to respond to this question.

11. **Whether CNAP service should be implemented for 140-level numbers allocated to registered telemarketers?**

    Response: Will not harm as long as correct CNAP (adequately describing the caller and if possible the purpose) is presented. However, registered telemarketers must continue to follow the DND registry and rules.

12. **--**

13. **Whether the bulk subscribers and National Toll-free numbers should be given a facility of presenting their ‘preferred name’ in place of the name appearing in the CAF? Please elaborate your response.**

    Response: Presenting a ‘preferred name’ for every department or individual who can use the telecom service can be misleading for the called party, and can be potentially abused by the calling party and the **real objective of introducing CNAP will be lost, not just potentially limit the usefulness of the CNAP.** CNAP cannot be targeted only for individuals and give relaxation to commercial entities who are also found to be abusing telecom services for tele-marketing bypassing the DND guidelines. Reproducing relevant parts of Response-1

    TRAI should make it mandatory that all non-individual entities register the telecom services with proper entity name along with the department/role of individual who primarily will use the service, so that the called party can take informed decision whether to accept or reject calls or develop/use appropriate filters. For example, a non-individual should append the name of department, location or name of an individual to the Entity Name as indicated in CAF, so that appropriate and useful details can presented as follows “NameOfCompany MumbaiSalesOffice” or “NameOfCompany - Mr. NameOfPerson” or “NameOfCompany DepartmentLocation NameOfPerson”. Such mandate of format of registration of CNAP name will allow a called party to reject unsolicited Marketing calls from irrelevant locations (city) but can still accept Service related calls or messages from the same company, bank or institution from the bank’s location or headquarters.

Q14: In case the response to the Q13 is in the affirmative, what rules should govern the implementation of such a facility?

Response: As per Response-13

Q15 & Q16: Whether there is a requirement of any amendment in telecommunication service licenses/ authorizations in case CNAP is introduced in the Indian telecommunication network? Please provide a detailed response.

Response: Telecom License must keep pace with the evolution of technology, identify the potential ways different entities can abuse services, put critical telecom infrastructure at risk, abuse personal data of telecom users, identify new security challenges, potential national threats and so on, especially considering that there is effectively no control on the social media, Internet, devices/handsets/apps and how they use telecom and user data. There have been several cases of impersonation and financial frauds.

Therefore, adequate provisions to safeguard the interests of citizens who are telecom users must be introduced in relevant Acts, Laws, Rules, License conditions etc, as and when any risks (potential for abuse/bypass rules) are identified and must take precautionary measures mitigate the risks to our National Security, while encouraging ethical practices to enable economic growth and social development. CNAP data also must be safeguarded, bot just on originating TSP, but also in transit and on terminating device (e.g. handset) where there is potential for misuse too.

Phishing using “missed” calls can be one of the risks (potential method of collecting called party’s data assuming called party will call back on seeing missed call), therefore if any telecom user is making frequent calls to several numbers (in any order, random/sequence/repeats etc), such callers may be identified and outbound calls blocked from making too many calls per hour (robocall phishing origination call via app / attached computer / manual assistance).

Further future rogue apps making missed calls (without customer knowledge/of the intent) to some specific numbers (which collect CNAP data) cannot be ruled out. TSPs should identify risky terminating numbers (which receive several missed calls) and block them proactively.

Other risks may be identified and mitigated.