Dated: January 16, 2023

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

SUB: Our Comments on the consultation paper on the introduction of Calling Name Presentation (CNAP) in telecommunication networks

Dear sir,

Greetings from DeepStrat, a New Delhi-based think tank and strategic consultancy.

We commend TRAI for the release of a comprehensive and insightful consultation paper on the introduction of CNAP in telecommunication networks. We believe that the paper raises many important issues, some of which also impinge on our constitutionally-mandated fundamental rights and serves as the starting point of an important discussion.

In our submission, we have given responses to several issues for consultation keeping in mind four broad contextual points:

1. The Supreme Court judgment in the case of Justice *K.S. Puttaswamy v. Union of India* (2017)
2. Privacy laws in India, including the Draft Digital Personal Data Protection Bill, 2022
3. The practical and technical challenges faced in CAF and KYC verification processes
4. Infrastructural challenges to set up a CNAP.

We will be grateful if you could acknowledge our comments and also consider them in the consultation process that follows.

Yours sincerely,

SAIKAT DATTA
Digitally signed by SAIKAT DATTA
Date: 2023.01.17 17:13:47 +05'30'

SAIKAT DATTA
CEO
DeepStrat | StratDeep Pvt. Ltd.
Contact no.: +919971600417
Email id: saikat@deepstrat.in

Q1. Whether there is a need to introduce the Calling Name Presentation (CNAP) supplementary service in the telecommunication networks in India?

While there is a need to address the issue of increased spam calls, fraudulent calls, etc, our stance is that introducing CNAP supplementary services is currently not a viable or desirable solution. It can only begin to be considered once comprehensive privacy laws are in place in India.

The Hon'ble Supreme Court of India in the case of *Justice K. S. Puttaswamy v. Union of India* (2017)[1] has declared privacy to be a fundamental right under Part III of the Constitution. The Court also ruled that the grounds for restricting the right to privacy have to meet the three-fold test of ***legality, necessity and proportionality***.

The objectives for deliberating CNAP are to address the concerns of telecom users with respect to unsolicited commercial calls from unregistered telemarketers, robocalls, spam calls, fraudulent calls and spoofing. CNAP, however, will mandate disclosure of personal information of *all* end users, regardless of whether they are legitimate users or otherwise. While there is a necessity, there is no reasonable nexus between the objective and the means for achieving it. Therefore, in our view, the proposed solution and the harm it poses, are completely disproportionate and thus fails the Supreme Court's threshold for restricting the right to privacy.

We raise the following concerns to support this stance:

- CNAP would enable the end user to receive the calling name information of the calling party and then make an informed decision about whether to accept the call. In order to achieve accuracy in identifying all callers, *everyone* must be included in a CNAP database. Until a privacy law is in place, this goal is not possible without the caller's personal information being at risk.
- Storing a user's personal information in any database and then disclosing it through a caller id has privacy implications. Further, given the technical complexity of creating such a database, the feasibility of introducing this solution remains impractical. Included in the technical complexity will be the transfer of data between TSPs. This complexity is not proportional to the privacy concerts inherent in the flow of data between different entities.
- The only way around the issue of privacy is to implement CNAP as an Opt-in process. However, then those numbers who are calling as fraudsters/scammers can simply choose to remain anonymous. The problem CNAP is trying to solve in the first place (as stated in point 1) then still exists.

[1] *Justice K. S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, AIR 2017 SC 4161

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

Q2. Should the CNAP service be mandatorily activated in respect of each telephone subscriber?

- No. Mandatory activation would mean that users cannot opt-in. In fact, users might not even be aware that their name is being disclosed. If CNAP is to be considered at all, it must be opt-in. Examples of the risk of mandatory activation include:
- An individual may opt to remain anonymous. Reasons include:
    - Concerns about other aspects of their identity being revealed through their name, such as gender or religion.
    - Concern for whistle-blowers.
    - Concern of being harassed as an employee and revealing business-related identities.
    - Concern of misidentification. For example, if someone's SIM is registered under a name that is not their own.
- The user's name is being used for identity theft or spamming.
- Lack of awareness that personal information is being collected in the first place.

All of these issues support the fact that without a privacy law in place, mandatory activation should not be implemented.

Q3. 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.

While our recommendation is that CNAP services should not be considered at this time, ***if*** they were to be considered once a privacy law is in place, acquiring consent must be clearly articulated to users.

- All information related to how personal data is stored and used must be presented to users before giving them the option to consent.
    - As stated in the Draft Digital Personal Data Protection Bill[2], this includes what kind of data will be processed, how it will be used, and the purpose of the processing operations.
- The option to opt-out at any time must be available, as well as mechanisms for deleting personal information once consent is withdrawn.

[2] *THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022*, MeitY, November 2022, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

Q4. 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.

Legal issues

- The Hon'ble Supreme Court of India in the case of Justice *K. S. Puttaswamy v. Union of India (2017)* had ruled that the grounds for restricting the right to privacy have to meet the three-fold test of legality, necessity and proportionality. CAFs which collect the personal information of *all* end users do not take their explicit consent to disclose the same information on caller id. In the absence of a robust privacy regime, this will be a disproportionate measure for addressing the stated objective.
- Using the information provided in CAFs for the purposes of CNAP also misses the threshold of reasonable expectation of users that this information may be used for displaying their names. An individual may not want to use their names given in the CAFs due to various societal and personal reasons. The Supreme Court has held that the right to privacy includes decisions, choices, information and freedom. Linkage of CAFs with CNAP will strip the users of their right to decide and exercise free choice.

Practical issues

- At present, TSPs use Customer Acquisition Forms (CAFs) to acquire subscribers. The Consultation Paper discusses the two categories of telephone subscribers, which are both subject to different documentary requirements for CAFs. *Individual subscribers* need to submit Proof of Identity (PoI) and Proof of Address (PoA) documents with the CAF. The *bulk subscribers* need to submit a PoA of the entity and PoI of the authorised signatory. Since in the latter case PoI of only the authorised signatory and not the end users is collected, the CAF information for end users under bulk subscribers might be inadequate and at times, inaccurate.
- The current rules allow for one individual to purchase up to nine sim cards by submitting their documentary proofs of identity and address. The end users of these sim cards may be different from the individual who obtained them by giving the PoI and PoA. This can happen in cases of joint Hindu family businesses, or dependents who use their guardian's sim cards, or in the cases of women whose sim cards are linked to a male family member, etc. In such cases the CAF information may not represent the accurate identity of the end user. This would not solve the problems envisaged in the consultation paper.

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

Failure of the KYC process

- At present, the CAF and KYC verification are the basis for acquiring sim cards. Our study[3] has revealed that unlawful actors often have poor or incorrect KYC details. There are multiple stakeholders who seek KYC but there is no standardisation of the KYC data, resulting in multiple KYCs. So a person may have signed up with different details for different KYCs collected by stakeholders.
- Apart from the discrepancies in KYC data, the law enforcement agencies also face numerous problems in investigation through KYCs due to various reasons. There are often long chains of KYCs. For instance, when a person using an identity proof issued in Tamil Nadu, purchases a SIM card in Jharkhand, moves to Rajasthan and uses it to target a victim in Maharashtra. This leads to multiple jurisdictions and conflicting KYCs for LEA investigators.
- The track down mechanism of the police through Base Tower Location depends on KYC. Investigators often find it to be inadequate to track them down and are unable to effectively rely on S. 102 of the CrPC because of KYC norms not being enforced strictly.
- We, therefore, believe that the KYC verification for obtaining sim cards is not the most accurate and robust process. It has been shown to result in inaccurate or inadequate data, and is insufficient to help investigators in tracking down offenders.

Q5: Which among the following models should be used for implementation of CNAP in telecommunication networks in India?

We propose an alternative model based on identifying only telemarketing numbers rather than displaying the name of all users. There will be a separate database, kept with the TSPs, to store the number of the telemarketer and the company that they represent.

Given that this model only identifies the principal entity that the telemarketers represent, it does not come with the risk of compromising the privacy of the average caller and is a **much more appropriate solution** to achieve the objective. Our submission is that there is no need to identify all callers when only a small subset of callers are fraudulent/spam. This will help law enforcement agencies in tracking down the relevant telemarketing agencies.

[3] Datta, Saikat, et al, *Tackling retail financial crimes*, 14/02/2022, Deepstrat, https://deepstrat.in/wp-content/uploads/2022/05/Tackling-Retail-Financial-Cyber-Crimes-In-India-Deepstrat13.05.2022-1.pdf

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

Q6. What measures should be taken to ensure delivery of CNAP to the called party without a considerable increase in the call set-up time?

We recommend that deliberations on caller identification of all users must only begin after a robust privacy law is in place. While we ultimately do not support the use of CNAP service even after this law is in place, should TRAI still wish to consider this option, adequate security and grievance redressal measures in accordance with the proposed Digital Personal Data Protection Bill (DPDPB) are a necessity.

In the event that this option is considered, the following must be done to avoid a considerable increase in the call set-up time:

- Network infrastructure must be optimised to minimise delays and ensure fast and reliable data transfer.
- Use a CNAP server or gateway that can cache frequently called numbers, reducing the need to look up the information in the database.
- The CNAP server or gateway must provide CNAP information in multiple formats, so that it can be easily understood by various device Operating Systems.

1. The CNAP server or gateway must provide a failover mechanism to ensure continuity of service even in case of failures.

- Regularly monitor and maintain the system to ensure that it is running smoothly and efficiently.

Q7. 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. And,

In the consultation paper[4], TRAI points out that there are already concerns about enabling CNAP on different types of phone networks. For example, some legacy wireless networks may require an upgrade to support the CNAP service. The feasibility of implementing the CNAP feature within today's increasingly complex software ecosystem is a major cause of concern. The CNAP database has to be accessible to all service providers, across both landline and wireless networks. This will require a large amount of cooperation and work between TSPs that we do not deem worth the aforementioned security risks.

[4] *Consultation Paper on Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks*, Telecom Regulatory Authority of India, 29/11/2022

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

Q8. 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?

The consultation paper notes that some mobile handsets may already support the CNAP feature, while others will require software upgradation. Similarly, many landline sets may not support this feature. Once the CNAP database is available to all TSPs, the data must be integrated into the software platforms of various phone providers (Apple OS, Android OS, etc) across various model types. Thus, changes to the existing Operating System (OS) software of displaying a caller ID will have to be completely re-wired in a centralised way. Again, the complexity this requires is not proportionate to the aforementioned risks.

Responses to Questions 9 - 12 on the use of a database specifically for telemarketers

1. **Reasonable Classification**

The introduction of the CNAP service for all telecom users is unnecessary given that the concern it is trying to solve involves only a tiny subset of these users. There must be a reasonable classification between the telemarketers who regularly engage in spam calls and the general users of telecom services. There is further concern that the CNAP service would not be enough to identify telemarketing companies in the first case. Before, telemarketers were required to be registered as promotional numbers. However, they now have started outsourcing work by giving individuals SIM cards to retain their personal identity. Thus, the receiver of the call would not even be able to see that it is a telemarketer. Instead of using the CNAP service for all users, the numbers and information of telemarketers should be identified in isolation.

2. **Database Creation for Telemarketers**

In order to identify the source of unsolicited or fraudulent calls, CNAP can display the caller identity of the principal entity which has engaged the telemarketer. The contractual agreement between the principal entity and the telemarketer can be used to build a database which contains the relevant details of both parties. This database needs to be easily accessible to the network and optimised for fast access. Additionally, it must be protected by encryption, securely stored, maintained to protect the privacy of the telemarketers, and comply with the regulatory environment. Proper authentication and authorization mechanisms need to be in place to ensure that only authorised parties can access and update the information.

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

3. Benefits of Telemarketer Caller Identification

The creation of a separate database for telemarketers will be useful in the following:

- Gathering evidence: The CNAP information could be used as evidence in investigations to trace the origin of the calls and to hold the offenders accountable for any unlawful activities.
- Monitoring compliance: CNAP information could be used to monitor compliance with laws and regulations that govern telemarketing, allowing law enforcement agencies to take action against telemarketers who violate these regulations.
- Caller identification: It could help customers to identify the telemarketer and decide whether or not to answer the call, reducing unwanted or unsolicited calls.

4. 140 Numbers

As stated in the consultation paper, registered telemarketers "make commercial calls to telephone subscribers through 140-level series numbers." Therefore, 140 numbers should be subject to the above classification and be added to the aforementioned database. The name of the principal entity associated with that telemarketer can be resolved from this number.

Q16. Whether there are any other issues/ suggestions relevant to the subject? If yes, the same may be furnished with proper justification.

We strongly recommend that the CNAP facility should come into effect after the Digital Personal Data Protection Bill and other privacy laws are enacted and enforced. The model for operationalizing CNAP should meet the data protection and individual privacy standards as envisaged by the Supreme Court.

The objective of the consultation paper is to address the issue of unsolicited commercial calls from telemarketing companies, fraud, spam, robocalls, spoofing, etc. CNAP should not be applicable to all callers, especially not without allowing them the choice of opting-in. A proportionate policy solution to address the problem would be to make a reasonable classification between telemarketing callers and other general callers. The telemarketers should have the requirement of providing information reflecting the principal entity they are calling on behalf of, as per their contractual agreement.

A database with adequate privacy and security measures can be built, in compliance with the upcoming data protection legislation and reflecting the essence of the right to privacy enshrined in the Constitution. This database can be accessed by the TSPs to reflect the names of the telemarketers on the caller id of the end user. This will give the users information about callers

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA

calling for commercial activities and allow them to make an informed decision about receiving the call. It will also help Law Enforcement Agencies in their investigations by providing them access to a database which does not rely on inadequate or inaccurate information provided by the CAFs and verified by KYC.

Even without a privacy law, the decision of the Hon'ble Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India*, needs to be duly followed. Any government action restricting the right to privacy for any purpose should meet the criteria of necessity, legality and proportionality as laid down by the Supreme Court.

https://deepstrat.in | contact@deepstrat.in | +91-11-26717356

CIN: U74996DL2022PTC406180; REGD ADD: M-18, SECOND FLOOR, SAKET, NEW DELHI, PIN-110017, INDIA