Submission of comments on Calling Name Presentation (CNAP) in telecommunication networks

The Telecom Regulatory Authority of India (TRAI), on 30 November 2022, released the consultation paper on the implementation of Calling Name Presentation (CNAP) in telecommunication networks. The paper acknowledges the unanswered genuine calls due to high volume of robocalls, spam, and fraudulent calls. Thus, it is important to display the name of the caller on the receiver's telephone to empower and provide safe telephone communications to consumers.

While the initiative aims to provide users relief from spam and fraudulent calls, concerns have been raised by industry experts about the implementation of this feature. The Department of Telecommunication (DoT) has proposed a model that can be implemented across multi-technology networks and across different telecom service providers, without the need for Internet or smartphones/devices.

However, implementation of this model is not feasible especially considering the fact that that providing CNAP facilities across telecom providers is not a straightforward task. In order to provide implementation solution for CNAP in a technology-neutral and Internet-independent manner, TRAI has proposed four different models.

India Future Foundation (IFF), a not-for-profit organization (working on Digital and Internet Policies to foster and build Digital Ecosystems that guarantee freedom of expression, trust, and safety for its users) puts forward its submission/views on aspects that we feel should be given further consideration before these Rules take the shape of a law. The following feasibility concerns continue to persist across all four models, as proposed by TRAI, for implementation of CNAP:

1. Each Telecom Service Provider (TSP) may be required to develop and maintain a CNAP database of its subscribers. The Telecom Service Providers (TSPs) may also need to upgrade the intermediate network nodes for the passage of CNAP data over the telecommunication network.
2. In the likelihood that CNAP service is introduced in telecommunication networks, the call set-up time is likely to increase. Truecaller, an Internet-based application, provides CNAP services without any delay in call flow and enables caller identification based on Internet connectivity.
3. In India, a large variety of wireless and landline network types are available. While modern networks may readily support CNAP supplementary services, there could be issues with legacy networks and between various network types.
4. In order for CNAP to be implemented, in India, it may be necessary for landline and telephone handsets to undergo software upgrades. This process will involve collaboration between various parties, including manufacturers and service providers, in order to integrate CNAP into future supplies. However, it is currently uncertain how this will affect current products.
5. For bulk subscribers and businesses, it has been suggested that TSPs should verify and approve the "preferred name." However, currently, businesses with toll-free numbers are not authorized to make outgoing calls. To address this, Truecaller is offering a solution called "Truecaller Verified Business Caller ID" which allows businesses to establish their brand identity and communicate safely with customers. Additionally, Truecaller is working on providing a green verified badge for government agencies for communication numbers and helplines.

6. In order to implement CNAP, the Department of Telecommunications (DoT) will need to make changes to existing provisions or add new provisions related to CNAP in the telecom service licenses and authorizations as there is currently no such requirement in place.

Apart from the concerns mentioned above, there are a few challenges in the paper as well. These have been explained in the following section –

1. **Complexity of the Issue**

   Fraudulent calls and scams are a significant concern for both society and industry as they can cause financial harm and mental distress to both consumers and businesses. It can also have a ripple effect on families, employees, and related parties. Therefore, it is crucial to address this issue. However, it is important to note that the complexity of this issue makes it challenging to find a single solution. With the advancement of technology, it is becoming easier for fraudsters to fake calls on legitimate numbers, making it difficult to quickly crack cases. KYC may seem like a plausible solution, but it may not be enough to tackle this complex problem.

   The challenges include –

   - massive scale of SIM provisioning, swapping, and portability,
   - CNAP delivery across network hops, and the need to integrate and synchronize with too many licensed service providers.
   - The cost to the government and carriers to build, run, synchronize and secure systems to support billions of calls daily for billions of Telecom Networks (**TN's)** requires a performant and low latency infrastructure, which will be passed on to end users.
   - Complexity will render coverage, accuracy, and currency unacceptable

CNAP will require not only KYC but also some sort of call authentication/tokenization/certificate authority to address this issue comprehensively. Spoofing may also increase as CNAP can be perceived as "trusted" by consumers.
There are several limitations to implementing CNAP.

- One limitation is that non-Internet solutions may not allow for out-of-band data or API queries from the device, which would make it necessary for the terminating carrier to append the caller's name to inbound calls.
- Another limitation is that the directory of names is too large to be loaded locally on the device.
- Additionally, there are challenges with different handset displays, which implies that engineering will need to be done for the lowest common denominator, meaning feature phones in this case. This is highly dependent on the native Operating Systems (OS) and Original Equipment Manufacturers (OEMs) displays and can often result in truncated, illegible CNAP.

2. **Protection of telecom subscriber's privacy and consumer choice**

   This proposal poses a significant risk to the fundamental rights of Indian citizens, as it limits consumer choice and poses a threat to privacy, which in turn could impact other protected fundamental rights.

It is noteworthy that telecom service providers are already required to display Caller Line Identification (CLI) is the ability of a person receiving a call to view the telephone number of the caller. However, TRAI's proposal to expand this by mandating the disclosure of a telecom subscriber's personal name based on their know-your-customer (KYC) documentation would pose a significant privacy risk to individuals who may prefer not to be identified to the caller for various legitimate reasons, such as risk to life and property, witness protection, whistle-blower protection and risk of retaliation.

Implementation of mandatory CNAP by TSPs would directly violate the exercise of constitutionally protected fundamental rights of citizens. Indian citizens have the fundamental constitutional right to privacy, which has been recognized by the Supreme Court of India in the *Justice K. S. Puttaswamy v. Union of India (2017)*. A mandatory CNAP requirement would be ill-advised, as it would have a chilling effect on individual freedom.

An alternative approach would be to provide individuals with the choice to voluntarily opt-in for CNAP functionality, with the option to withdraw their consent at any time easily.

3. Impact on women's safety

The mandatory nature of the CNAP functionality poses specific dangers for women subscribers, as it risks the unauthorized disclosure of their personal data every time they make a call. This could potentially lead to their contact information being accessed by bad elements in the society and could lead to targeted sexual harassment, spam calls and messages, and so on. The CNAP functionality will impinge on women's informational privacy and autonomy and expose them to exacerbated harms.

4. Rational allocation of public resources

TRAI's proposal to make it mandatory for TSPs to display CNAP raises a fundamental question about the allocation of public resources. Policy decisions should be based on an imminent, significant, and unmet need to justify allocating public resources to a particular problem over other competing demands. The introduction of mandatory CNAP is a proposal that focuses on solving a problem that is already better addressed and solved by private-sector solutions such as third-party caller ID apps. Allocating public resources to this issue could be avoided, and instead they could be better used in other areas that could be enhanced through collaboration with existing solutions, leading to a more effective solution to tackle scams and frauds.

5. Issues with KYC

Telecom service providers are required to conduct mandatory know-your-customer (KYC) compliance checks on users before issuing SIM cards. This process involves collecting and verifying basic user information such as full name, photograph, date of birth, and address, based on officially valid documents such as Aadhar, driving license, PAN, and passport.

However, the accuracy of this information is only about 60%, and errors can occur during manual verification.

Additionally, digital verification of KYC has not been implemented universally. Further, frauds and scams are dynamic in nature, with criminals constantly change their methods to exploit loopholes in the system. It is also important to note that SIMs may not be purchased by the actual user, according to current rules. In cases where the individual purchasing the SIM has fake IDs, the KYC process will also not be able to verify it, meaning that the individual purchasing the SIM may not necessarily be the user of the number.

Further, collecting KYC could lead to problems for certain groups of individuals. These have been discussed in below points –

a. **Small family-run businesses -** Most of the time, phone numbers for business are purchased in the name of the patriarch of the family. These numbers maybe used for personal as well as business purposes. Usage like this, therefore cannot be accurately identified solely by KYC. It is worth noting that currently, India has approximately 633.88 lakh MSMEs. Only using KYC details for caller identification therefore could exclude them from actively participating in economic activities.
b. **Women -** Gender is also an important lens to factor in while considering phone usage and KYC. India predominantly is a patriarchal society, and therefore there continues to be a digital divide in the country with women being 15% less likely to own a mobile phone.[2] Even the ones that do own them, some may have their numbers linked to the male member in the family. For example, it is fairly common for women to get mobiles that are no longer being used by their children or have numbers that have been registered under their husband's name. Caller ID that therefore solely relies on KYC will therefore exclude these women from social interactions over phone. As the caller ID will likely show their husband's or children's details, it might be difficult for them to get on a call with people outside their close circle. This will especially impact their mobility and participation in the economy.
c. **Children:** Children are likely to be using numbers registered with their parents' KYC. Even after reaching adulthood, it is fairly common that they would continue using the same number after becoming an adult and the number would still be linked to their parent's KYC.

The proposed use of KYC for the caller ID system has the potential to lead to confusion and incorrect identification. The private sector currently employs multiple technology solutions to provide accurate caller ID, and the regulator must consider the potential pitfalls of using KYC alone. The responsibility of verification falls solely on the government or the telecom service providers. If verification fails or KYC is inaccurate, victims of scams have no further recourse. A more effective solution would be to combine crowd-sourced verification with KYC. This would allow victims of fraud to alert other users of a fraudster, and the collective experience of multiple individuals would be more reliable than relying on a single reference such as KYC. Algorithms that use crowd-sourced data to "blacklist" numbers would also be more reliable, as numbers would be authenticated by thousands

of victim experiences. It is also worth considering that KYC depends on the individual's willingness and ability to provide correct information at the time of purchase, which can easily lead to false information being collected. Crowd-sourced data, on the other hand, relies on the collective experience of multiple individuals who have faced similar harm.

6. Infrastructure concerns surrounding implementation

The adoption of any of the four models suggested by TRAI will need considerable revamp of the existing infrastructure in use by telecom providers. As mentioned by TRAI, one of the primary considerations in implementing the CNAP facility is likely to increase the call setup time. Even as stakeholders look for technological solutions to reduce the latency time, i.e., time taken to look up the calling name information from a database and supplying it to the provider responsible for displaying it to the subscriber, the current infrastructure will have to be upgraded to enable the CNAP facility. From a review of the four models, it seems that Model No. 1, (in which the CNAP lookup will happen in a local database) is likely to lead to least latency and disturbance in the call setup time.

An associated issue is the prevalence of non-smartphone communication instruments, such as mobile phones without internet connections, landline phones, etc. As of September 2022, there are 1145.5 million wireless subscribers and 26.5 million wireline subscribers. The TRAI has indicated that it wishes for the CNAP facility to be technology neutral and internet independent. In this endeavour, it will have to consider the challenges that telecom providers will face in ensuring transfer of accurate information over intermediate network nodes. While modern networks may readily support CNAP supplementary services, there could be issues with legacy networks and between various network types.

Landline and other telephone handsets in India may require a software upgrade to enable CNAP. Multiple stakeholders including manufacturers and service providers will have to work together to enable CNAP on future supplies and it is not clear how this would apply to current products. For instance, landline providers may need to recall the handsets and provide their customers with new ones that have the CNAP functionality built in.

It is preferable that TRAI provides its inputs on the cost of setting up and maintaining the CNAP database, as different types of network providers will have to adopt different methods to implement the facility. Further, it is currently unclear if these providers would need to bear the cost of setting up and maintaining the database, or if there would be any form of governmental support.

7. Challenges in other jurisdictions

In the USA, the terminating service provider performs a lookup on the database maintained by the originating service provider or a trusted third party. The TSPs pay a nominal fee every time they ‘dip’ into the database. This leads TSPs to supply old data instead of performing a database search or showing the incorrect caller ID.[4] Examples like this point to the fact that the KYC database doesn’t always work and crowd-sourced information may be more reliable moving forward.

Further similar mandates like TCPA, Truth in CallerID Act, Do Not Call (DNC) in the US, lull consumers into complacency and create new opportunities for technically savvy fraudsters.

Conclusion -

Despite the above considerations, in the event, TRAI ultimately decides to implement one of the four proposed options for mandatory implementation of CNAP, then Option 1 should be the clear and preferred choice. This is because it is the only option which could be readily implemented, without the need of complicated regulatory and licensing framework and should purportedly work towards achieving the end-objective as envisaged by TRAI.

Regardless of this, it is advisable for TRAI to keep any such CNAP solution a strict 'opt-in' feature so that the constitutionally protected fundamental rights of citizens are in no way diluted or hampered or limited keeping in mind the fact that CLI is an already-existing mandated mechanism which has an established track-record of working well for most users, and existence of which warrants introduction of CNAP.

TRAI has flagged 16 questions for discussion on the CNAP facility. Some of these questions, with discussion points are –

1. **Should the CNAP service be mandatorily activated for each subscriber? If not, what are suitable methods for acquiring their consent?**

   TRAI says subscribers want to identify the calling party correctly. The menace of spam and scam calls from unknown numbers has made subscribers wary of picking up even genuine calls – if they are from unknown numbers.
   Currently, subscribers can only see the Caller Line Identification (CLI) information, i.e., the telephone number. Along with robocalls, spam, scam, and fraudulent calls, spoofing of CLI information has also become a major concern.
   The native-smartphone apps, such as 'silence unknown numbers' on Apple, or 'caller ID and spam' feature on Android, are not available to regular feature-phone users. **Third-party apps like Truecaller and Bharat Caller ID provide calling name information, but rely on crowd-sourced data. 'The crowd-sourced name identity information may not be reliable, in many instances.'**
2. **Where should the information for the database be sourced? Should it be from the Customer Acquisition Forms?**

   Under the Unified Access license regime currently in play, TSPs are mandated to ensure 'adequate verification of each and every customer'. They thus get their customers to fill Customer Acquisition Forms (CAF) which have their name, address, etc. and submit relevant documentary proof to the TSP. Similarly, bulk subscribers submit proof of address of their company, firm, etc. and proof identity of the authorised personnel to the TSP. The CAF database can act as the CNAP database.

3. **How to reduce latency and ensure minimal addition to the call set up time?**

   The CNAP service is likely to cause a slight increase in the call set up time. 'It appears that in the case of Model No.1 and Model No.4 (in which CNAP lookup will be performed in a local

CNAP database), the increase in call set up time would be lesser than that in case of the Model No. 3 (in which the CNAP lookup will be performed on a centralized CNAP database).'

4. **How to implement CNAP service for both offline and online mobile phone users, and for landline phones?**

   In another letter to TRAI in July 2022, DoT has indicated that CNAP service should be **technology neutral and Internet independent.** 'In case CNAP service is introduced, the manufacturers of mobile handsets and landline telephone sets may have to enable the CNAP feature in their future supplies.'

5. **Whether the CNAP service should be apply to entities, such as telemarketers, registered under the TCCCPR, 2018?**

   Entities registered under TCCCPR, 2018 are assigned a telephone number in the 140-level series. 'For displaying the name identity of the principal entity to the called party, suitable provisions will have to be made to store the name identity of the principal entity in the CNAP database.'

6. **What amendments will be needed in the telecom service licenses/authorisations, if CNAP was to be introduced?**

   Currently, TSPs are mandated to show only the CLI information – under the Unified Access Service License (UASL), NLDO License and ILDO License. However, there is no obligation to display the caller's name. DoT may need to amend existing provisions or include new provisions in these licenses to implement the CNAP.

7. **Whether the existing 2G, 3G, 4G, 5G mobile networks, and modern (Next Generation Network) and legacy (based on circuit-switched tech) landline networks are capable of implementing CNAP services? If not, what technical changes/additions are needed?**

   'While the modern networks might readily support CNAP supplementary service, some legacy networks might require an upgrade to support the CNAP service. Besides, there could be issues related to the passage of CNAP at the points of interconnection (POI) between various types of networks.'

8. **Some international precedents for CNAP:**

   USA: the terminating service provider performs a lookup on the database maintained by the originating service provider or a trusted third party.
   Canada: the calling party name information is sent from the originating service provider to the terminating service provider.
   Turkey: service providers are allowed to use the sender's name, commercial name, a public institution or a non-governmental organization's name, trademarks, and patents as CLI, provided that the respective subscribers possess official documents to prove their legitimate right to use these names.