
	<p style="text-align: center;">BHANJA INSTITUTE FOR RURAL DEVELOPMENT ଭଞ୍ଜ ଗ୍ରାମ୍ୟ ବିକାଶ ପ୍ରତିଷ୍ଠାନ/ ଭଞ୍ଜ ଗ୍ରାମୀଣ ବିକାଶ ସଂସ୍ଥାନ <u>Bhanja Mandap, Kullada, Ganjam, Odisha-761131</u> Cell-9437619050 & email- birdkld90@gmail.com <u>Regd. Voluntary Consumer Organization</u> under SR Act-1860/IT Act-1961/FCRA-1976/CAG of TRAI</p>	
---	--	--

CONSULTATION PAPER (CP)

BIRD Comments on the TRAI CNAP Consultation Paper

1. Background

Bhanja Institute For Rural Development (BIRD) expresses its gratitude to the Telecom Regulatory Authority of India (TRAI) for inviting comments on the Consultation Paper on Calling Party Name Presentation Facility (CNAP) in Indian Telecommunications Network.¹

2. About BIRD

BIRD in its 25 years of existence, has come a long way from being a grassroots consumer centric organisation headquartered in Kullada village of Ganjam district of Odisha state ,

BIRD has been working towards improving the regulatory environment through evidence-based policy and governance-related interventions across sectors and national boundaries. It has conducted various studies and events in the telecommunications (telecom) sector, such as Demystifying Reality from Myth for 5G in India²; Coding and Enforcing Mobile Internet Quality of Standards in India³; Consumer Broadband Labels for Greater Transparency & Informed Consumers;⁴ Towards Effective Choice: A Nation-Wide Survey of Indian TV Consumers;⁵ among many others. Currently,.

3. Recommendations to TRAI

BIRD has approached the proposal of introducing CNAP to examine its effects on consumers. There are some issues in the TRAI's consultation paper that need thorough examination from a consumer perspective. Therefore, we urge the regulator to undertake comprehensive cost-benefit analysis of its proposal on all stakeholders, before reaching a conclusion. These issues are

¹https://traai.gov.in/sites/default/files/PR_No.78of2022.pdf

²5G in India

³Coding and Enforcing Mobile Internet: Quality of Standards in India - ccier

⁴Project Launch Meeting "Consumer Broadband Labels: For Greater Transparency & Informed Consumers" - ccier

⁵<http://cuts-ccier.org/pdf/research-report-towards-effective-choice-a-nation-wide-survey-ofindian-tv-consumers.pdf>

discussed in the subsequent sections. We have engaged with different consumer groups on key issues arising out of the consultation paper.⁶

4. Broad issues

1. Need for conducting a Regulatory Impact Assessment for the Telecom Sector:

Regulatory Impact Assessment (RIA) is a systemic evidence-based approach for assessing positive and negative effects of proposed and existing regulations and non-regulatory options, on diverse stakeholder groups.⁷ It is based on collection and analysis of quantitative and qualitative information, thereby affording regulators substantial and high-quality inputs from a wide range of affected and interested parties. Regulators can base their decisions on sound rationales, by assessing costs and benefits likely to flow from proposed regulations.⁸

RIA helps regulators in deciding whether and how a regulation can deliver the most benefits to the society. It compares costs and benefits of different possible ways of resolving an issue to identify and consider the most efficient course of action before a decision is made.⁹ Thus, it helps in sound and objective decision making, promoting regulatory certainty while minimising legal challenges. It enhances stakeholder confidence in regulatory decisions through public consultations, and commitment to transparency and non-discrimination.¹⁰

Regulators across sectors are realising the benefits of RIA, and Information Communications and Technology regulators in at least 43 countries now conduct RIA before regulatory decisions are made.¹¹ Several multilateral organisations like the International Telecommunications Union (ITU) have been promoting the use of RIA in the telecommunications sector for quite some time now.

In addition, several ICT regulators are using RIA to design approaches for addressing issues which are similar to issues that TRAI is dealing with. For instance, the US Federal Communications Commission (FCC) is exploring different approaches to reduce robocalls¹² and deploying broadband infrastructure.¹³

In order to fully benefit from the RIA framework, it is essential that it is not a one-off exercise. RIA needs to be seamlessly integrated with the regulation making process, and must not be considered as an additional burden/ compliance requirement. Further, while the changes brought

⁶ Some of the Consumer organisations and groups with whom we have engaged include Cashless Consumer, Consumer Voice, Money Life, Consumer Care Society, Himachal UpphogktaSanrakshan Parishad Shimla, Patiala Consumers & Telephone Subscribers Forum, Tamil Nadu Consumer Protection & Environmental Research Centre(TNCPERC), BIRD-CAG.

⁷<https://www.oecd.org/gov/regulatory-policy/43705304.pdf>

⁸<https://digitalregulation.org/wp-content/uploads/D-PREF-TRH.1-2-2020-PDF-E.pdf>

⁹<https://www.oecd.org/gov/regulatory-policy/BRP-brochure-2022-web.pdf>

¹⁰<https://digitalregulation.org/wp-content/uploads/D-PREF-TRH.1-2-2020-PDF-E.pdf>

¹¹<https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.439.51.en.702.pdf>

¹²<https://www.federalregister.gov/documents/2022/07/18/2022-13436/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor>, <https://www.federalregister.gov/documents/2022/07/18/2022-13878/advanced-methods-to-target-and-eliminate-unlawful-robocalls-call-authentication-trust-anchor>,

<https://www.fcc.gov/document/fcc-affirms-three-call-limit-robocalls-residential-lines>,

¹³<https://www.brookings.edu/interactives/tracking-regulatory-changes-in-the-biden-era/>

by technology and innovation across sectors hold great potential to enhance prosperity and well-being, they also entail significant risks and potential adverse effects. These potential effects and risks which can arise as issues for consumers, with the introduction of CNAP have been discussed in the next section.

5. Specific Issues

These issues are categorised under four themes, which are as follows:

1. Issues with displaying the name of Consumers
2. Consent, Privacy and Protection of Data of Consumers
3. Existing Market-Based and Regulatory Solutions
4. Other Issues for Consumers to be considered

5.1 Issues with Displaying the Name of Consumers

It has been noted that the Department of Telecommunications (DoT) has provided a note to TRAI in September 2022, which pointed out that the introduction of CNAP aims to empower telecom consumers to take informed decisions while receiving incoming calls. It will further reduce the harassment of subscribers from unknown/ spam callers, as they will be able to clearly identify the caller (by having access to name and not just number) before picking up the calls.¹⁴

While the aim of introducing such a facility is guided by existing concerns of telecom customers, the implementation raises some concerns, especially from the consumer's perspective. The CNAP facility as it is currently proposed will create additional issues for consumers which are discussed in this section.

1. Protection of identity of consumers in distress, victims of abuse, whistle-blowers, and journalists.

There might be various scenarios wherein consumers may not wish to have their identities revealed on others' devices. These could include calls by victims of domestic abuse, activists, journalists, auditors, investigators, watchdogs, whistle-blowers, or those bound by professional secrecy. Also, consumers making one-off innocuous or inquiry related calls to e-commerce delivery personnel, cab aggregator drivers, booking agents, other intermediaries and aggregators, may have no option but to give up their identity even before the call is picked up. This one-size fits all approach, of displaying identity of all callers, bereft of nuances, may not necessarily be an optimal solution.

Furthermore, TRAI's proposal to expand CNAP with an unhindered mandate to disclose personal name of telecom consumers based on their know-your-customer (KYC) documentation, will pose significant privacy risk to individuals who may prefer not to be identified to the caller

¹⁴https://traai.gov.in/sites/default/files/CP_29112022_0.pdf

due to a variety of legitimate reasons. These privacy risks have been discussed in subsequent sections.

2. Reliability of name provided in the Customer Acquisition Form, which is proposed to be mandatorily displayed.

TRAI proposes to rely on information provided by consumers in Customer Acquisition Forms (CAF) at the time of subscribing, for name reveal to call recipients. The CP also intends to explore if the CNAP service be mandatorily activated in respect of each subscriber, or if an implementable method for acquiring consent of subscribers for activation needs to be designed.

However, the concerns around reliability, safekeeping, and verification of information provided in CAF have cropped up from time to time. It is possible that such information is not consistent with information recorded during other customer due diligence exercises. Responses to Right to Information (RTI) queries to TRAI, on the reliability of CAF have not been encouraging as they claim to not have relevant information to confirm veracity of KYC details. The Telecom Analytics for Fraud management and Consumer Protection (TAF-COP) portal is yet to be fully operationalised.¹⁵

The KYC details are collected by TSPs (Telecom Service Providers), as self-declarations from subscribers. TSPs are required to fulfil mandatory KYC compliance checks of users prior to the issuance of SIM cards. KYC involves collecting and verifying basic user information (full name, photograph, Date of Birth, address, etc.) based on certain officially valid documents (e.g., Aadhar, driving licence, PAN, passport, etc.). The KYC information declared by the consumers is not completely accurate. The manual verification of KYC can be filled with errors. Digital verification of KYC has not been implemented universally and can also give rise to privacy and exclusion concerns.¹⁶ Further fraud and scams as phenomenon are dynamic in nature, with criminals continuously changing their modus operandi to find loopholes in the system.¹⁷ KYC in turn is a static set of information, once the data is collected, it is rarely changed or modified. Given these constraints, KYC may not provide the most accurate information on the caller ID feature.

3. Difference between subscriber and user of the number, resulting in possibility of display of wrong name

There are some cases in which the person filling in the CAF might be different from the person using the number. This may lead to the revelation of a wrong name. This is further compounded by the fact that sims may not be purchased by the actual user. As per current rules, any individual can obtain up to 9 SIM cards by providing their proof of identity and proof of address. For example, an individual could purchase a sim using their IDs and then give their sim to their parents, siblings, or someone else who would not be in the KYC database. In case the individual purchasing the sim has fake IDs, the KYC information collected by the TSP's will also not be

¹⁵ <https://tafcop.dgtelecom.gov.in/index.php>

¹⁶ <https://www.medianama.com/2023/01/223-explained-astr-sim-facial-recognition/>

¹⁷ <https://www.biometricupdate.com/202301/pushback-against-sim-registration-in-philippines-as-india-adds-facial-recognition-checks>

sufficient to verify the same. The KYC, therefore, overlooks that an individual purchasing the sim may not necessarily be the user of the number.

Additionally, if a customer's phone or sim gets stolen, and is misused, the KYC information will not be sufficient proof for protecting the consumer. CNAP will legitimise these existing stolen or fraudulent SIM cards obtained through identity theft and will display names of victims of identity theft. In this way the CNAP facility might give more protection to fraudsters, who will continue to use the stolen IDs for the purpose of committing more fraud.

While the problem of unsolicited calls does exist, it is a complex problem that cannot be solved by simply relying on KYC information, due to many related issues. In this context, the DoT has launched multiple measures such as Do Not Disturb, Telecom Commercial Communication Customer Preference Regulation (TCCCPR) 2018, etc. to address this problem. It might be more useful to focus on these and other existing measures to address the problem of unsolicited calls, in collaboration with industry players and consumer bodies.

4. Collecting only KYC details can lead to unintended consequences for certain groups of individuals.

These groups include:

a) Small family-run businesses: Most of the time, phone numbers for business are purchased in the name of the patriarch of the family, or 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 MSMEs¹⁸. Only using KYC details for caller identification therefore could exclude them from actively participating in economic activities as it will affect the autonomy of the person who owns the enterprise. These activities might include government subsidies, loans from developmental banks and financial institutions, especially if it is a women-led business.

b) Women: Gender also is 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.¹⁹ Even the ones that do own them, some may have their numbers linked to the male family member. 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. This might make it difficult for them to get on a call with people outside their close circle. The effect of this might be women losing their own agency and autonomy, by being attached to the identity of the male head of the household. Personal identity and autonomy have been seen as important factors for societal and individual growth of a person.²⁰

c) Children: Children are likely to be using numbers registered with their parents' KYC. Even after reaching adulthood, it is common that they would continue using the same number after

¹⁸<https://www.ibef.org/blogs/msme-sector-imperative-to-lift-indian-economy>

¹⁹<https://www.orfonline.org/expert-speak/indias-gendered-digital-divide/>

²⁰https://www.researchgate.net/publication/329776846_PERSONAL_AUTONOMY_AS_A_KEY_FACTOR_OF_HUMAN_SELF-DETERMINATION

becoming and the number would still be linked to their parent's KYC. The issue of losing autonomy and identity this way would also apply to children. About 2.2% of India's population lives with some kind of physical or mental disability, as per the National Statistics Office report. While the country only has a seven per cent disability gap in ownership, persons with disabilities are **30 per cent less** likely to be aware of mobile internet. by its their livelihoods KYC it be accessible and like others

d) Persons with dis-Abilities: PWD as neglected and disadvantages group of society also is an important lens to factor in while considering phone usage and KYC. As per 2011 Census, the total population of India is 1.23 billion, in which about 2.1 per cent (over 21 million people) suffer from one or the other kind of disability. Of the total disabled population males and females are respectively 12.6 and 9.3 millions.

5.2 Consent, Privacy and Protection of Data of Consumers

1. Display of name without effective and informed consent.

As mentioned in the previous discussion points, there might be various scenarios where users, rightfully, may not wish to have their identities placed on record on others' devices. Thereby, display of name without effective and informed consent of consumers may raise concerns around privacy and data protection. The Digital Personal Data Protection Bill, 2022 (DPDPB) which is being debated currently, has evolved over the years as a result of a felt need to have a comprehensive law to protect privacy of individuals, and empower them to make an effective choice for sharing personal information and data.

It is important for individuals to be aware of the potential privacy implications of using supplementary services like CNAP, and then be able to give informed consent on whether or not they want their name to be displayed when making calls.

Consequently, it might be useful to think about limiting obligations of caller name display to specific service providers of a certain threshold, and further, natural persons may be given the option to opt into such systems. Similarly, it might be useful to explore options wherein the caller presses additional codes after dialling the caller's number to allow display of the caller information.

2. Privacy and data protection risks with respect to the database from which names will be sourced for display, leading to difficulty in fixing responsibility and accountability in case of breach.

To operationalise caller name presentation, TSPs may need to dip into each other's database. Sharing and passage of data through different points of interconnection between multiple networks, may make data susceptible to leaks. Alternatively, creation of a centralised database wherein details of all consumers are stored, or its clones with all service providers, may end up acting as honeypots for malicious actors, with increased likelihood of data leaks and breaches, resulting in increased spam for users. In such scenarios, it might be difficult to fix responsibility

and hold service providers to account. This might particularly be problematic in a scenario when the country lacks a robust personal data protection law.

3. Mandatory implementation of CNAP facility may lead to violation of fundamental rights of consumers

It is important to note that TSPs are already currently mandated to display caller line identification (CLI). TRAI's proposal to make it mandatory for telecom service providers (TSPs) to mandatorily display Calling Name Presentation (CNAP) presents a material risk to the constitutionally protected fundamental rights of Indian citizens. The caller's name is considered personal information, and the disclosure of this information (along with caller's number) without the caller's consent could be considered a violation of their privacy.

Indian citizens are entitled to fundamental constitutional right to privacy which has been duly recognised by the Hon'ble Supreme Court of India in *Justice K. S. Puttaswamy v. Union of India (2017)*. Preserving this constitutionally protected right to privacy is an essential prerequisite to ensuring and preserving exercise of other constitutionally protected fundamental rights of individuals e.g., right to free speech. As an alternative, what could be considered is an 'opt-in' approach wherein individuals are provided a choice to voluntarily and expressly 'opt-in' for such a CNAP functionality (with an option to withdraw their consent at any time in an easy manner) vis-à-vis all or specific call recipients. Such a voluntary and express 'opt-in' would not only preserve consumer-choice but would also ensure that the constitutionally protected fundamental rights are respected and given necessary and due policy protection both in letter and in spirit.

4. Risks of identity spoofing and misuse of data.

These above listed concerns on privacy and data leakages, coupled with disclosure of personal information like name and contact number, without customer consent, in absence of an overarching data protection law, could also exacerbate risks related to violation of privacy, misuse of information, and identity spoofing. The caller's name may be used for malicious purposes, such as identity theft (through call back scams etc) or spamming, if it is displayed to unauthorised parties. Young users of telecom services and senior citizens may particularly be at risk in such scenarios. Consequently, it might be useful to wait for the data protection law to be operationalised before acting on TRAI's proposals.

Spoofing could very likely increase as CNAP can be perceived as misguidedly 'trusted' by consumers.

5.3 Existing Market-Based and Regulatory Solutions

1. Utility of existing market-based solutions which help display and mark suspicious callers based on crowd-sourcing.

The CP notes that at present, there are several market based solutions for the issue of robocalls, spam calls, fraudulent calls, and caller identity spoofing. At present, smartphone users can make use of native smartphone tools and third-party apps to identify calling party name, location, and mark spam calls. For instance, Apple provides a 'silence unknown numbers' feature on its

handsets. Google app allows phone users to mark incoming calls as spam. Third-party apps like ‘Truecaller’ and ‘Bharat Caller ID & Anti-spam’ also provide calling party name identification and spam identification facilities.

Despite the fact CP assumes that given these market-based solutions use crowd sourced caller information, the same is likely to be unreliable. It does not support its assumptions with evidence. Moreover, these assumptions have been made when Truecaller has launched a feature to connect users with government officials in India.²¹ It has also been pointed out that 50% of Truecaller’s subscribers in India are women who use the service as a first line of defence against harassment.²²

Furthermore, it is not clear if any study has been undertaken with respect to reliability of crowd sourced caller names. Moreover, there is lack of data on perspectives of consumers (benefits and challenges experienced) and stakeholders on crowd sourced caller information and other market innovations²³. It is also ironic that one hand a movement to give power back to consumers by reducing information asymmetry is gaining ground, while on other, information sourced from consumers is being summarily disregarded. It might make sense to trust consumers’ judgement more often.

This kind of database will be useful to examine if scarce state capacity and public resources should be invested to design regulatory intervention on an issue on which the industry is already making a lot of progress.

In addition, it is not clear if the solutions in place have been effective and is there a need to push for their greater adoption through awareness generation and capacity building, or is there a need for a new solution. While potential exists to enhance reliability of such crowd sourced data, availability of additional information may aid call recipients to make informed choices about picking up the call.

As discussed in previous points, the KYC information may not necessarily be accurate, and TSPs may find it difficult to verify such information. Crowd-sourced verification coupled with KYC could help in solving this problem. It might be a better idea for the regulator to join forces with the market players, for addressing concerns related to their solutions, and generating awareness and building capacity of consumers, on using them.

2. Need to explore innovative solutions and best practices

²¹<https://www.hindustantimes.com/technology/truecaller-launches-feature-to-connect-users-with-govt-officials-check-details-101670392360930.html>. Also see, “The government’s CNAP database is under consultation, and telcos and involved parties are likely to take at least 12 months—or more—to come to a consensus for India to have an ‘official’ caller ID service. This gives Truecaller time to diversify its offerings with other services, such as the ‘smart SMS’ service that it launched last year to identify spam links and scams in a phone’s SMS inbox”, at <https://www.livemint.com/companies/news/truecaller-rolls-out-digital-directory-of-indian-government-11670335550463.html>

²²https://www.business-standard.com/article/companies/public-interest-outweighs-concerns-over-privacy-says-truecaller-ceo-122033000013_1.html

²³ For instance, Truecaller has introduced a feature called Call Reason option, which helps users send a note with their outgoing calls. See, <https://www.businesstoday.in/interactive/longread/truecaller-will-its-over-dependence-on-india-come-back-to-bite-it-190-25-10-2022>

Having reviewed practices in countries like the United States of America,²⁴ Canada²⁵, Turkey²⁶, the CP lays out different models for CNAP.²⁷ But, in the proposed models, incorrect identification, due to unreliability of CAF based on KYC information is likely to lead to more confusion in the ecosystem. Current private sector interventions use multiple technology solutions to provide accuracy for the caller ID system. An instance of this is AI powered call assistant, which helps users identify who is calling and why, and filter spam calls.²⁸

In the USA unwanted calls, including illegal and spoofed robocalls, are the FCC's top consumer complaint and is among top consumer protection priority.²⁹ To address these issues, FCC has taken certain steps that include empowering phone companies to block by default illegal or unwanted calls based on reasonable call analytics before the calls reach consumers. It also possesses significantly greater enforcement capabilities, when compared with the Indian regulator.

Also to require phone companies to implement caller ID authentication to reduce illegal spoofing, an industry-standard caller ID authentication technology is used, which is a set of technical standards and protocols that allow the authentication and verification of caller ID information for calls carried over Internet Protocol (IP) networks. It is a carrier-based Caller ID authentication that requires carriers to digitally sign calls originated by their customers. This means that calls travelling through interconnected phone networks can have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers.³⁰

Such solutions, which utilise technology and combine it with a structure wherein, the government can work with market forces and consumer bodies to ensure benefits for consumers should be explored for the Indian telecom sector.

3. Potential of the proposed solution to reduce fraud calls.

The CP discusses the concerns which consumers have raised regarding the absence of calling party name presentation facilities. They prefer not to attend calls from unknown telephone numbers, as most of such calls are unsolicited commercial communications (UCCs) from unregistered telemarketers. As a result, even genuine telephone calls go unanswered. Concerns

²⁴ The terminating service provider performs a lookup on the database maintained by the originating service provider or a trusted third party, using the calling party's telephone number to obtain name information for presenting it to the called party.

²⁵ The calling party name information is sent over the telecommunication network from the originating service provider to the terminating service provider

²⁶ 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.

²⁷ The CP suggests four models: 1. Each TSP establishes and operates a CNAP database in respect of its subscribers; 2. The terminating TSP seeks CNAP data from the originating TSP; 3. A third party establishes and operates a centralized CNAP database; and 4. Each TSP maintains a CNAP database to keep a copy of the centralized database established and operated by a third party.

²⁸ <https://www.telegraphindia.com/business/trucaller-plans-to-bring-artificial-intelligence-powered-call-assistant-to-india/cid/1905845>

²⁹ <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>

³⁰ <https://www.fcc.gov/call-authentication>

have also been raised with respect to robocalls, spam calls, fraudulent calls, and caller identity spoofing, which may end up in consumer harassment or harm.³¹

While the CP points to the problem of spam, fraud, and spoof calls in general, it doesn't explain if a particular category of consumers face this problem more than others. Similarly, it is not clear if a specific kind of problematic calls are more prevalent than others. Such nuanced data will be crucial to design targeted measures to address the problem, rather than taking a one size fits all approach.

It is also not clear how mere display of caller name will address the issue of fraud, spam, and robo calls. While it may give some additional information to call recipients, it may not necessarily be sufficient to distinguish genuine calls from other callers, without picking up the call.

4. Effectiveness of other existing regulatory solutions to address the problem of fraud calls.

The CP makes certain assumptions regarding the problem at hand and existing practices, without showcasing relevant evidence. It also makes some recommendations without necessarily comprehensively examining their potential impacts or effectiveness. It further seems that several existing regulatory and market-based solutions to address the problem have not been reviewed decisively. These are some such issues, which require further investigation, through interaction with consumers and other stakeholders.

Also, one of the triggers for CP has been rise in UCC by unregistered tele-marketers in form of calls and SMS, and related customer harassment and financial frauds. TRAI and DoT, along with regulators like Reserve Bank of India, Securities and Exchange Board of India, Ministry of Consumer Affairs, have formulated the Joint Committee of Regulators'³² Action Plan to Curb Financial Frauds using Telecom Resources.³³ All of these regulators are also independently and collectively making efforts to address the problem of UCC. The impact of such existing regulatory and market based solutions to identify, prevent, and block such calls has not been detailed in the CP. TRAI has also been leveraging distributed ledger technology and artificial intelligence to curb unsolicited commercial communication.³⁴ Such initiatives may have greater chances of success, in the longer term.

5.4 Other Issues for Consumers to be considered

1. Possibility of call drops, delay in call set up time, and deterioration in quality of services for consumers.

³¹https://traai.gov.in/sites/default/files/CP_29112022_0.pdf

³² The committee consists of TRAI, Reserve Bank of India, Securities and Exchange Board of India, Ministry of Consumer Affairs. Officials from Ministry of Home Affairs and DoT participated in its recent meeting dated 10 November 2022.

³³https://traai.gov.in/sites/default/files/PR_No.75of2022.pdf

³⁴<https://www.financialexpress.com/industry/hassled-over-pesky-telemarketing-calls-ai-to-rescue-traai-to-crack-down-on-spam-calls-smses/2895082/>

The CP acknowledges that in case the CNAP service is introduced, through one of the models suggested by it, there is a likelihood of a slight increase in the call set up time.³⁵ Moreover, there could be issues related to passage of CNAP at the points of interconnection between various types of networks. These might adversely impact consumer experience and also impose cost on the industry.

While the CP suggests that its proposed models may increase call set up time, it does not consider the adverse impact of such delays on consumers who might already be facing call drops and sub-optimal quality of telecom services. This should be taken into consideration given the rising instances of call drops and service quality-related issues.³⁶

There might be other concerns with the models such as data concentration, security and privacy issues, and possibilities of misuse of caller identification, through mechanisms like identification spoofing.³⁷ Some of the models may also increase the cost of doing business with service providers.

2. Possibility of increase in price of telecom services, given the likelihood of passing off the cost by telecom service providers, to the consumers.

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. But as discussed above, the models of CNAP as proposed have other issues which would affect the consumers.

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.³⁸ 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.

³⁵ The time taken between the moment the calling party finishes dialing the telephone number of the called party and the moment the called party's telephone starts ringing

³⁶<https://www.zeebiz.com/economy-infra/telecom/news-telecom-dept-dials-service-provider-on-call-drops-and-service-quality-issues-discusses-interventions-214961>

³⁷<https://www.iiitb.ac.in/faculty-articles/caller-id-raises-privacy-security-questions>

³⁸https://www.trai.gov.in/sites/default/files/PR_No.67of2022.pdf

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. The cost incurred by TSPs is most likely to be transferred onto the final consumers.