CUTS Counter Comments to TRAI Consultation Paper on Caller Name Presentation in Telecom Services

Background

CUTS is thankful to the Telecom Regulatory Authority of India (TRAI) for providing us an opportunity to submit counter comments on its Consultation Paper on Caller Name Presentation in Telecom Services. We had submitted our comments and also reviewed comments submitted by other stakeholders on the Consultation Paper. Based on our review and further analysis, CUTS is pleased to submit its counter comments on the Consultation Paper.

The comments and recommendations have been classified into specific and broad issues:

Specific Issues and Recommendations

A. Direct Issues and Risks to Consumers

1. Risks of Cyber Attack and Data Protection

A number of submitted comments, including by Cellular Operators Association of India (COAI), Internet Freedom Foundation (IFF), Cyber Cafe Association of India (CCAOI), AP & Partners and others, have discussed the concerns around privacy with implementation of CNAP, especially in the context of the absence of a Data Protection Law in India. COAI, which has emerged as the official voice for the Indian telecom industry, has highlighted the biggest concern with CNAP would be the protecting privacy and confidentiality of subscriber information.

According to COAI, the proposed model of CNAP would involve creating a database of name and mobile number of the entire country's subscribers and with certain third parties, such as handset manufacturers and operating system providers having access to the same. A central database should be avoided since it increases the threat surface to privacy risks, and makes the data extremely prone to misuse and leakages. In this context a consumer group, Bhanja Institute For Rural Development (BIRD), also discussed in their comments, the issue of privacy and data protection risks with respect to the database from which names will be sourced for display. They point out that it would lead to difficulty in fixing responsibility and accountability in case of breach. One of the service providers, Vodafone Idea Limited (VIL), have raised similar concerns and pointed out that the database will be akin to storage of sensitive information in Aadhaar database.

Moreover, large datasets have been honeypots for cyber-attacks.[1] There have been many instances, such as the JustDial (a local search service platform) data breach in 2019, in which data of more than 100 million users was compromised and put in public domain, which included names, mobile numbers, email IDs, date of birth, gender and addresses.[2] Another such instance where data of 22 million users was compromised, and put up for sale, was the Unacademy (an online education platform) data breach in 2020.[3]

As per reports, India saw the highest number of cyberattacks on government agencies worldwide[4]. This included the cyberattack on data systems of All India Institute of Medical Sciences (AIIMS)[5]. Another report presents that on an average 29,500 records were breached in India by March 2022.[6] Specifically, telecom service providers have increasingly faced risk of cyber-attacks,[7] with multiple cases of breaches of information.[8]

Recommendation: We believe that the apprehension of such security issues with subscriber data in the proposed CNAP database is justified. Such a model would make consumer data susceptible to leaks and end up acting as honeypots for malicious actors, creating issues misuse of sensitive data, and of spam and frauds for the consumers.

2. Violation of Privacy of Individual Consumers

Many stakeholders including VIL, Airtel, AP & Partners and others, have insisted that a data privacy legislation should be a precondition for CNAP implementation, so that the rights of users can be protected and there can be an assessment of its impact on individual privacy. VIL mentioned that name is a confidential piece of data for a subscriber and there would be segments of consumers who may not want their names to be shared. Privacy violation is a possibility with the mandatory CNAP feature, which would disclose the name of the caller to the receiver even in cases where the caller does not wish to disclose their name (for example, in case of a person inadvertently calling a wrong number leaving her name exposed). Moreover, as the CNAP feature will be mandatory, such consumers will not have opt-out option.

1 https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html
2 https://www.policybazaar.com/corporate-insurance/articles/biggest-cyber-breaches-in-india/
3 ibid.
4 https://www.livemint.com/technology/tech-news/india-saw-the-highest-number-of-cyberattacks-on-govt-agencies-in-2022-report-11672389099189.html
5 https://scroll.in/latest/1038702/how-aiims-is-working-to-restore-services-after-hackers-crippled-its-computer-systems
6 https://analyticsindiamag.com/the-ridiculous-17-5-cr-for-a-data-breach/
7 https://thehackernews.com/2022/10/telstra-telecom-suffers-data-breach.html
8 https://cio.economictimes.indiatimes.com/news/corporate-news/tpg-telecom-joins-list-of-hacked-australian-companies-shares-slide/96224289

Herein, the New Indian Consumer Initiative (NICI) in their comments highlight the important issue that should be considered is the protection of the identity of certain groups of consumers, such as those in distress, victims of abuse, whistle-blowers, and journalists. These individuals may need to make anonymous or confidential calls to seek help or report abuse, and the introduction of CNAP could put them at risk if their name is displayed.

It should be noted that display of consumer names and numbers, would create issues and risks for consumers, of frauds, phishing, vishing, identity theft, which have been increasing at alarming rates. Indian consumers have been reported to be most vulnerable to fraud on social media sites.[9] Data reports of the last two years have shown that there have been over 9 lakh incidents of phishing, One Time Password (OTP) compromise and 42% Indians have experienced financial fraud.[10] Reports also suggest that Indian businesses are concerned about the increasing fraud and phishing cases,[11] and more than 95% of Indian companies/organisations saw new types of frauds happening in the past two years.[12] Vishing and phishing have also been included by Reserve Bank of India (RBI) in the top fraud instruments in India.[13]

Recommendation: We believe that the proposed CNAP poses a myriad variety of risks to consumers and their privacy, in absence of a comprehensive privacy and data protection law.

3. Violation of consent of Consumers due to Mandatory Implementation

Largely, firms and associations have demanded that CNAP should not be a mandatory feature as proposed. IFF argues that CNAP should be introduced as an alternative and voluntary 'opt-in' service. Users should be allowed to voluntarily 'opt-in' for such a CNAP functionality (with an option to withdraw their consent at any time in an easy manner). 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.

One of the service providers, Reliance Jio, also advocated for opt-in CNAP service, for consumers who opt to share their names details can be allowed to receive the name

9 https://www.financialexpress.com/money/indian-consumers-most-vulnerable-to-fraud-on-social-media-sites-apps-report/2911302/

10 https://timesofindia.indiatimes.com/business/india-business/over-9-lakh-incidents-of-phishing-otp-compromise-reported-in-last-two-years-42-indians-have-experienced-financial-fraud/articleshow/93361388.cms

11 https://www.outlookindia.com/business/fraud-cases-continue-to-rise-globally-97-of-indian-firms-consider-customer-experience-paramount-says-report-news-244639

12 https://economictimes.indiatimes.com/news/company/corporate-trends/new-fraud-incidents-reported-by-over-95-of-indian-companies-surveyed-by-pwc/articleshow/95535739.cms

13 https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

details. Moreover, COAI submitted that CNAP would be suitable as an optional and supplementary Value-Added Service (VAS) service.

Jio also said it is safe to assume that mandatory CNAP activation will not survive legal scrutiny.

It should be noted that similar provisions of mandatory consumer responsibility of KYC (Know Your Customer) identification, in the draft Telecom Bill 2022, were criticised on the grounds of proportionality, and in violation of fundamental rights of privacy of the subscribers.[14] The provisions under the recent draft Digital Personal Data Protection Bill, 2022, of duties and obligations of data principals have also been criticised by stakeholders.[15]

Offering more perspective, the Internet Service Providers Association of India (ISPAI), National Centre for Human Settlements and Environment (NCHSE) BSNL, and others have argued that providing CNAP service should not be made mandatory even on the service providers and device manufacturers.

Recommendation: We believe that the mandatory implementation of CNAP could be violative of consent and right to privacy of consumers.

4. Issues to consumers due to unreliability of Information

A financial service provider, Paytm has highlighted that the KYC process undertaken by telecom service providers (TSPs) is not watertight. There are two broad issues which make KYC information of consumers provided in the Consumer Acquisition Form (CAF) unreliable:

a. Fraudulent KYC

Instances of fraudulent KYC or cases where fraudulent persons manage to forge identity documents to obtain multiple SIMs/connections have been seen.[16] Paytm argues that unless the existing KYC process is not strengthened and re-verification of suspected connections are done, the entire purpose of CNAP may be defeated.

b. Multiple KYC creating difference between subscriber and user

Meanwhile, Truecaller, which already offers a similar service albeit through a crowdsourcing model has also said since several people purchase SIM cards using forged identity cards, the proposal to use SIM registration data to display callers' names might be fraught with inaccuracies since the identity of the actual user of a mobile

[14] https://www.medianama.com/2022/10/223-discussion-draft-telecom-bill-2022-kyc-requirements/
[15] https://internetfreedom.in/read-our-consultation-response/
[16] https://www.bgr.in/telecom/vi-blocks-nearly-8000-sim-cards-issued-on-fake-identity-proof-1250015/

number may not be the same as the subscriber. This is especially so because in India one could legally own up to nine mobile phone numbers.[17]

It has also been observed that in families, numbers for which the KYC details were provided by one member, were often provided on phones to aged parents or young children and the like. Many small enterprises often used one or other of the personal mobile numbers of the founders, for official purposes. A discrepancy based on gender is also observed in India, as there exists a digital divide, with mobile ownership being 30% higher among men than women[18] and women only constitute one-third of Internet users.[19]

BIRD, the consumer group has made a similar submission that KYC information is unreliable, and would lead to issues such as difference between subscriber and user of the number, resulting in possibility of display of wrong name. Also, collecting only KYC details can lead to unintended consequences for certain groups of individuals such as women, children, small businesses, and elderly people. These have been discussed in a subsequent section.

Recommendation: We also agree that CAF information in its current form, may not be fool proof, and thus should not be the basis for display of caller identity as proposed under the CNAP feature. It might be useful for the regulator to commission an evidence-based study to examine reliability of CAF information, and understand shared usage of mobile phones.

5. Issues for Law Enforcement, women safety, and other disadvantaged groups

An industry representative, Reliance Jio said that the presentation of a user's name at the time of calling can "lead to various social and criminal issues", such as social media stalking. Therefore, CNAP might result in more cases of cybercrime. As per reports, there has been a 63.5% increase in cybercrime cases in 2019 as compared to 2018, out of which, in 60.4% of cases, fraud was the motive followed by sexual exploitation (5.1%) and causing disrepute (4.2%).[20]

From the submissions of Jio and Internet and Mobile Association of India (IAMAI), we understand that there can be myriad reasons for the customers not being willing to share their name with the called party. A few of these can be potential fraud and risk of abuse, misbehaviour, social media stalking etc. We are already witness to multiple cases where

17 https://swarajyamag.com/tech/solution-looking-for-a-problem-government-proposes-caller-name-presentation-of-all-incoming-phone-calls

18 https://scroll.in/latest/1039064/digital-divide-mobile-ownership-30-higher-among-men-than-women-in-india-shows-oxfam-report#:~:text=In%20India%2C%2061%25%20men%20had,digital%20divide%20in%20the%20country.

19 https://indianexpress.com/article/india/women-constitute-one-third-of-internet-users-in-india-study-8305984/

20 Digital India Sees 63.5% Increase In Cyber Crime Cases, Shows Data (ndtv.com)

the abuse and inappropriate behaviour starts the moment the party is speaking to a person of the opposite sex, which can only increase when the name is also available.

Therefore, obtaining the consent of subscribers before activating such a facility is very crucial. Various studies[21] show that both men[22] and women[23] are prone to online harassment, with women[24] being more vulnerable. Display of phone numbers of women, will make them even more vulnerable to such harassment.

The National Centre for Human Settlements and Environment (NCHSE) have forwarded a similar viewpoint. They add that these risks are further exacerbated due to weak laws which give benefit leeway to cybercrimes.

As per the recent National Family Health Survey Report[25], only about 54% of women aged 15-49 years have a mobile phone that they themselves use. The use of CAF, which would display the name of the subscriber and not the user (as discussed in earlier section) may unnecessarily discriminate against such hitherto disadvantaged groups.

In their comments BIRD has discussed the issues of losing autonomy of vulnerable groups such as women, children, elderly. The Consumer Protection Association Himmatnagar also makes a reservation against CNAP that there are some vulnerable groups to whom the mandatory activation of CNAP can be up to some degree harmful, such as for women and girls.

Recommendation: Through these submissions we understand and agree that CNAP can potentially harm consumers, like women and exacerbate risks of cybercrimes.

B. Indirect Impact to Consumers

1. Utility of crowd-sourced data

A service provider, Truecaller, offering a similar caller ID facility, albeit on crowd-sourced data, highlighted that such data can be more reliable than the data declared by customers in Customer Acquisition Form. The crowdsourced information displays the caller ID of the actual user of a mobile number. This crowdsourced data is based on

21 https://www.thehindu.com/news/national/8-out-of-10-indians-have-faced-online-harassment/article19798215.ece
22 https://mediaindia.eu/society/both-men-and-women-vulnerable-to-online-harassment-in-india/
23 https://www.mumbailive.com/en/culture/83-of-women-in-india-experience-online-harassment-63054
24 https://www.newindianexpress.com/world/2020/oct/06/58-per-cent-young-women-face-online-harassment-abuse-report-2206631.html
25 http://rchiips.org/nfhs/NFHS-5Reports/NFHS-5_INDIA_REPORT.pdf

community feedback and a combination of Artificial Intelligence[26] and Machine Learning[27] tools.

From the submissions of Truecaller, we understand that the crowd-sourced data is collaborated from multiple signals including a community of active users who regularly vet and update information in real time, adding tremendous value to spam identification systems.

It might be useful for the regulator to examine other benefits of the crowd-sourced model used by Truecaller. Currently, it has 235 million users in India.[28] The identity of the caller displayed by Truecaller has even helped law enforcement agencies to identify criminals.[29] Globally, Truecaller analyses 60 billion incoming calls every month[30], and presents global[31] and country specific data of spam calls.[32] In other countries as well, the Truecaller model has been used to detect scams and frauds[33] and identify criminals[34].

Additionally, there has been research which suggests that primary information that is complemented by both follow-up feedback and collective confirmation leads to improved outcomes for the public.[35] This is the essential principle of crowd-sourced information, therefore, it's utility should be examined.

Recommendation: We believe that there is merit in examining the model of crowd-sourced data, as used by Truecaller to address the issues of spam and robo calls, unsolicited commercial calls (UCCs) in India. While the model may also be prone to misuse and pose certain privacy risks, it would be prudent to improve the shortcomings of the solutions by addressing risks rather than exploring a new solution like CNAP, which has potential to exacerbate consumer issues and risks. It might also be useful for the regulator to commission an evidence-based study to examine reliability of crowd sourced information.

26 https://www.indiatoday.in/cryptocurrency/story/ai-to-help-truecaller-users-in-india-know-why-someone-is-calling-them-2313655-2022-12-26

27 https://www.indiatimes.com/technology/apps/truecaller-is-challenging-whatsapp-with-a-new-instant-messaging-feature-of-its-own-354182.html

28 https://www.truecaller.com/blog/impact/though-truecaller-has-its-roots-in-sweden-india-has

29 https://www.orissapost.com/truecaller-helps-delhi-police-nab-fraud-occult-practitioner-read-full-story/

30 https://www.washingtonpost.com/world/the_americas/from-cheap-loan-offers-to-fake-kidnapping-brazil-leads-the-world-in-telephone-harassment/2019/12/02/b4234e7a-0fb4-11ea-bf62-eadd5d11f559_story.html

31 https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021

32 https://www.truecaller.com/blog/insights/truecaller-insights-2022-us-spam-scam-report

33 https://www.nytimes.com/2021/02/14/podcasts/the-daily/scam-call-centers.html

34 https://punchng.com/my-daughters-life-has-been-destroyed-mother-of-teenager-allegedly-abducted-defiled-by-policeman/?fbclid=IwAR1fKHLwt-s2DKO6x9umD4-qeJMIHRjw0JX0tH3TNxX66Divv_Pp_dC91sQ%22%20%5Ct%20%22_blank

35 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377042

COAI, VIL submitted that it is pertinent to throw light on the fact that there are similar services from crowd sourcing apps, such as Truecaller, Whoscall, CallApp, Showcaller, etc. that are already readily available which are being used by the subscribers. Truecaller has been downloaded 500 million times.[36] On Google play store, the download rate of these apps (Whoscall, CallApp, Showcaller) are 5Cr+, 10Cr+, 1Cr+ respectively. Thus, the CNAP service would only render duplication of a feature/service that is already in use, which would further cause a dilemma to the party receiving the call.

COAL, VIL have also added that information on a crowdsourced basis would be the closest match to the real user and their names with which they are known to their friends, family and social/professional circles. TRAI has also launched a few apps that work on information gathered on a crowd-sourced basis. This raises a pertinent question of why TRAI is introducing a completely new model, which doesn't utilise the existing models, as this would also add to the existing regulatory burdens considering scarce capacity.

2. Cost of CNAP and likelihood of passing it off to the consumers

The industry representatives and Truecaller have quoted studies which mention that India is the second-largest telecommunications market in the world with 1145.5 million wireless subscribers and 26.5 million wireless subscribers. Many stakeholders and service providers such as COAI, Airtel, Jio, VIL have submitted that CNAP implementation will involve cost and huge development in both Network and IT systems and processes. Moreover, all the proposed models involve substantial latency.

The NCSHE have pointed out that the only option to implement CNAP is to request the manufacturing company to upgrade the hand sets and land line telephone set and if it is not possible the alternative is to change the set. We understand from ISPAIs and the other submissions that there is a cost associated with the implementation of CNAP, which needs to be reviewed, as it is likely to be passed on to the customers.

The Consumer Protection Association Himmatnagar has advocated that CNAP should be implemented without financial burdens on the consumers. COAI, Airtel, VIL and others have pointed out the various techno-commercial challenges. Most likely the earlier feature-phone handsets (like 2G handsets) will not support CNAP. Even the recent smartphones would require software updates. Even such software upgrades would be challenging for the smartphones which have crossed software upgrade cycles as provided by handset manufacturers. Consumer Guild also added that software upgradation will be required in all mobile and landline sets.

[36] https://www.truecaller.com/blog/news/500-million-downloads-150-million-daus-truecaller

Industry players like Jio have submitted that CNAP facilities is a good to have supplementary value-added services (VAS) service. However, in a country where over 375 million users (over 350 million mobile nonbroadband users and over 25 million wireline users) are unlikely to possess a CNAP enabled device, in addition to a sizable portion of the wireless broadband users that may not be possessing CNAP enabled devices as well, it can safely be said that it should not be a mandatory service. If implemented as proposed, CNAP will not have the intended impact.

Recommendation: In the view of a telecom service provider, VIL, current third-party solutions effectively solve any customer concerns. Hence, the implementation of CNAP has limited additional benefits and adds to the regulatory burden and costs of telecom service providers in India. As discussed, these costs are most likely to be transferred to the final consumers. Therefore, a need-based assessment of CNAP, using data from evidence-led studies should be conducted.

VIL also recommends alternate ways of providing caller name information which are existing 3rd party apps i.e., through a Common Mobile App (CMA) which will integrate the subscriber name database from all TSPs in a secured way. Such alternatives should also be explored. Therefore, instead of mandating CNAP, the government should look to improve anti-spam regulation, which is a widespread problem currently faced by users in India.

Broad Recommendations

Need to conduct RIA, Cost Benefit Analysis and undertake need based assessment of the CNAP feature

BIRD, COAI, IAMAI have joined CUTS in recommending that TRAI must carry out the Regulatory Impact Assessment (RIA) and detailed cost benefit analysis before deciding whether to adopt CNAP in India. RIA would also play a role in determining which model of CNAP or alternative should be implemented to deal with the issue of addressing fraud/spoofing/UCC.

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.[37] 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.[38]

[37] https://www.oecd.org/gov/regulatory-policy/43705304.pdf
[38] https://digitalregulation.org/wp-content/uploads/D-PREF-TRH.1-2-2020-PDF-E.pdf

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.[39] 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.[40]

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.[41] 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 robocalls[42] and deploying broadband infrastructure.[43] Herein, RIA will be extremely useful in assessing the need for CNAP and undertaking a cost-benefit analysis of the proposed facility. It would also be useful for the regulator to commission an evidence-based study to examine reliability of CAF information, crowd sourced data, and to understand shared usage of mobile phones.

Consumer Unity & Trust Society (CUTS) expresses gratitude to Telecom Regulatory Authority of India (TRAI) for inviting counter comments on the Consultation Paper on 'Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks'. CUTS looks forward to TRAI accepting the above suggestions and assisting in its efforts to empower consumers and lead to effective and optimum regulation. We would be glad to make an in-person presentation of our submission before TRAI.

For any clarifications/further details, please feel free to contact:
Shiksha Srivastava (sva@cuts.org), Yatika Agrawal (yta@cuts.org), Research Associates at CUTS International. We are thankful for the support of Amol Kulkarni (amk@cuts.org).

39 https://www.oecd.org/gov/regulatory-policy/BRP-brochure-2022-web.pdf
40 https://digitalregulation.org/wp-content/uploads/D-PREF-TRH.1-2-2020-PDF-E.pdf
41 https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.439.51.en.702.pdf
42 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,
43 https://www.brookings.edu/interactives/tracking-regulatory-changes-in-the-biden-era/