ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Look Who's Calling: India Needs a Right to Know Who Is Contacting You

INDIAN EXPRESS

1 August 2026 · SCIENCE & TECH · POLITY · GS2 · GS3

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Look Who's Calling: India Needs a Right to Know Who Is Contacting You

The Indian Express 1 August 2026 GS2 GS3

INTERVIEW ANGLE

"CNAP draws caller names from telecom KYC records, which means the state and telecom operators are jointly deciding what name appears on every citizen's phone screen. What safeguards would you build so that a system designed against spam does not become a general-purpose identity-disclosure infrastructure?"

Every fact web-verified against primary sources

THE LIFT LINE

Every unanswered call from a number you do not recognise is a small tax that fraudsters have levied on everyone else. CNAP does not block the fraudster; it takes away the anonymity that made the fraud worth attempting.

WHY THIS EDITORIAL MATTERS FOR YOUR EXAM

Digital consumer rights, telecom regulation and privacy are converging into a recurring GS2/GS3 theme, and CNAP is a clean case study in which a privacy-protective and a privacy-intrusive reading of the same measure are both defensible, exactly the kind of tension examiners want candidates to hold rather than resolve too quickly.

GS Paper 2: Government policies and interventions; consumer rights; e-governance; statutory and regulatory bodies.

GS Paper 3: Awareness in the field of IT; cyber security; money laundering and its prevention.

For **Prelims**, fix the CNAP and CLIR acronyms and TRAI's role as the recommending regulator.

CONCEPT	MEANING	WHY UPSC TESTS IT
CNAP (Calling Name Presentation)	A service displaying the caller's verified name, drawn from telecom KYC records, on the recipient's device	The core mechanism of this reform
CLIR (Calling Line Identification Restriction)	The facility allowing a caller to withhold identity presentation	The privacy opt-out, and the point at which the default question arises
TRAI	Telecom Regulatory Authority of India, the sector regulator that recommended CNAP	The institutional actor behind the reform
Purpose limitation	The data-protection principle that data collected for one purpose should not be used for another	The central safeguard this editorial argues must be legislated alongside CNAP

BACKGROUND AND CONTEXT

India's telecom subscriber base is among the world's largest, and its spam and fraud-call problem is correspondingly large: Truecaller recorded roughly 4,168 crore spam calls across 2025. TRAI recommended CNAP following a consultation process, the DoT framework was approved in October 2025, and a staged nationwide rollout was targeted from March 2026, beginning with 4G and 5G users. Successive interventions have taken a blocking approach: the Do Not Disturb registry, operator-side filtering obligations, and a substantial private market in third-party caller-identification apps that crowdsource spam labels. CNAP takes a different approach, using the KYC information telecom operators already collect at the point of subscriber verification to display a verified name to the recipient.

APPROACH	MECHANISM	LIMITATION
Do Not Disturb registry	Recipients opt out of marketing calls	Poor compliance; ineffective against fraud calls, which never intended to comply
Third-party caller-ID apps	Crowdsourced spam labelling	Depends on private databases of uncertain provenance and accuracy
Operator-side filtering	Network-level blocking of flagged numbers	Reactive; fraudsters cycle numbers faster than blocking adapts
CNAP	Displays verified KYC-derived name at call presentation	Creates an identity-disclosure infrastructure with uses beyond spam

THE CORE ARGUMENT / ISSUE

Why blocking has failed, and what it cost

The blocking paradigm assumes a finite adversary who can be enumerated and excluded. Fraud calling does not work that way: numbers are cheap, cycled rapidly, and often spoofed. The predictable result is that blocking never catches up, and recipients adopt the only reliable defence available to them, which is to stop answering unknown numbers entirely. That adaptation is individually rational and collectively costly, since it degrades the phone network's usefulness for every legitimate caller who happens to be unknown to the recipient.

Why identity disclosure is structurally different

Displaying a verified name does not block anything. What it does is remove the anonymity that makes high-volume fraudulent calling economically viable. A fraud operation depends on being unidentifiable both to the person it is defrauding and to anyone investigating afterward. Attaching a KYC-verified name to the call attacks both, and does so without requiring the network to correctly predict in advance which calls are fraudulent, which is the prediction problem blocking approaches keep failing.

The architectural objection, taken seriously

The concern is not that CNAP will fail; it is that it will work, and that a functioning nationwide identity-disclosure layer attached to the telephone network is a capability with obvious secondary applications. Identity infrastructures built for narrow purposes have historically expanded, and the expansion is typically incremental and individually reasonable at each step. The safeguard against this is not technical but legal: an express statutory purpose limitation confining CNAP-derived data to call presentation, enforceable independently of the executive's own restraint.

The default question

CLIR lets a caller withhold their name. That is a genuine mitigation, but it is an opt-out. Under an opt-out design, the default is disclosure, and privacy is available only to those who know the facility exists and take the trouble to invoke it, a population that skews toward the already-informed. Data-protection principle generally favours privacy-by-default, and the question of whether CNAP's default is correctly set deserves more scrutiny than it has received.

HOW TO THINK ABOUT THIS (ANALYTICAL FRAME)

Distinguish an intervention that predicts bad behaviour from one that removes the conditions enabling it. Blocking-based approaches must correctly identify which calls are fraudulent, a prediction problem the adversary is actively working to defeat. Identity disclosure does not predict anything; it changes the payoff structure so that fraudulent calling is less attractive regardless of whether any particular call is

detected. When evaluating any enforcement or regulatory design, ask whether it depends on winning a prediction contest against an adaptive adversary, since designs that do tend to degrade over time while designs that alter incentives tend not to.

THE DIAGRAM IN WORDS

Picture the phone network as a doorway with no peephole. Currently, every knock is anonymous, so residents have learned to ignore knocking altogether, which frustrates the postman and the neighbour as much as the intruder. The blocking approach installs an ever-growing list of people not to admit, which the intruder defeats simply by using a different name each time. CNAP installs a peephole. It does not decide who may enter; it lets the resident see who is there, and, just as importantly, it means the intruder knows they can be seen. The remaining question is who else can look through the peephole, and what they are permitted to do with what they see.

WAY FORWARD

1. **Legislate express purpose limitation** confining CNAP-derived identity data to call presentation alone, enforceable independently of executive discretion.
2. **Reconsider the CLIR default**, evaluating whether privacy-by-default would better align the system with data-protection principle without materially weakening its anti-fraud function.
3. **Establish independent oversight** of access to the telecom KYC databases feeding CNAP, with published access logs and audit provisions.
4. **Build an accuracy-correction mechanism**, since a system displaying verified names must have a fast, low-friction route for individuals to correct a wrong or outdated name.
5. **Evaluate outcomes on fraud incidence, not call volume**, so the system's success is measured against the harm it was built to address rather than against a proxy metric.

PYQ LINKAGE AND PRACTICE

UPSC has tested data protection, telecom regulation, cyber fraud and digital consumer rights across GS2 and GS3, and CNAP offers a specific, current instrument through which the privacy-versus-security trade-off can be examined concretely rather than abstractly.

Practice question: "An intervention that removes the conditions enabling harm is more durable than one that attempts to predict and block the harm itself." Examine this claim with reference to India's Calling Name Presentation rollout and the failure of blocking-based approaches to spam and fraud calling. (250 words, 15 marks)

Interview angle: CNAP draws caller names from telecom KYC records, which means the state and telecom operators are jointly deciding what name appears on every citizen's phone screen. What safeguards would you build so that a system designed against spam does not become a general-purpose identity-disclosure infrastructure?

Sources: The Indian Express, Telecom Regulatory Authority of India, Department of Telecommunications

KEY ARGUMENTS AT A GLANCE

India's spam and fraud call problem is fundamentally an information-asymmetry problem, the caller knows who they are reaching while the recipient knows nothing about the caller, and Calling Name Presentation (CNAP) addresses that asymmetry directly in a way that blocking and do-not-disturb registries, which treat the symptom, do not.

✓ SUPPORTING

- The scale of the problem, with roughly 4,168 crore spam calls recorded across 2025 (Truecaller) and 79 per cent of businesses reporting that customers avoid answering calls from unrecognised numbers (Truecaller-TTBS State of Business Calling 2026), indicates that the existing blocking-based approach has failed and has imposed a secondary cost: legitimate unknown callers, including hospitals, delivery services and government agencies, now go unanswered.
- Identity disclosure is the structural precondition for accountability; a fraudulent caller operating behind an anonymous number faces no reputational cost, whereas a caller whose verified name appears on the recipient's screen is identifiable both to the recipient and, in the event of fraud, to investigators.
- CNAP draws names from telecom KYC databases already collected under existing subscriber-verification requirements, meaning it uses information the system already holds rather than requiring a new data-collection regime.

⚠ COUNTER

A system that displays a verified name on every call creates a general-purpose identity-disclosure infrastructure whose uses will not remain limited to spam prevention; the CLIR opt-out mitigates this but places the burden on the individual to actively protect their own anonymity, which is the inverse of a privacy-by-default design.

→ WAY FORWARD

Pair the CNAP rollout with statutory purpose limitation restricting the use of CNAP-derived identity data to call presentation alone, a privacy-by-default review of the CLIR opt-out

> mechanism, and independent oversight of how telecom KYC data feeding the system is accessed.

✍️ MAINS ANSWER FRAMEWORK

QUESTION

Examine caller identity disclosure through CNAP as a consumer-rights and digital-trust measure, and assess the privacy safeguards necessary for such a system to remain proportionate. (250 words)

INTRODUCTION

India's rollout of Calling Name Presentation (CNAP), which displays a caller's verified name drawn from telecom KYC databases on the recipient's screen, reframes the spam-call problem from one of blocking unwanted contact to one of correcting the information asymmetry that makes spam and fraud calling viable in the first place.

BODY

The scale of India's problem, roughly 4,168 crore spam calls in a year and nearly eight in ten Indians reporting that they now refuse calls from unknown numbers, indicates that blocking-based approaches, do-not-disturb registries, operator-level filtering, third-party spam-identification apps, have not solved it. Worse, they have generated a secondary harm: because the rational response to an unidentifiable caller is non-answering, legitimate unknown callers including hospitals, emergency services, delivery personnel and government agencies now face a population trained not to pick up.

CNAP addresses the underlying asymmetry rather than the symptom: a caller who must appear under a verified name faces both immediate recipient scrutiny and post-hoc traceability, which changes the economics of fraudulent calling substantially. The serious objection is architectural rather than technical. A system that attaches verified identity to every call creates infrastructure whose usefulness extends well beyond spam prevention, and history suggests that identity infrastructures built for a narrow purpose tend to acquire additional ones. The Calling Line Identification Restriction (CLIR) opt-out provides a mitigation, but it is an opt-out rather than an opt-in, meaning disclosure is the default and privacy requires affirmative action, which inverts the privacy-by-default principle that data-protection law generally favours.

CONCLUSION

CNAP is a well-targeted response to a genuine and large-scale harm, but its proportionality depends on safeguards external to the technology itself: statutory purpose limitation confining CNAP-derived identity data to call presentation, independent oversight of access to the underlying KYC databases, and a reconsideration of whether disclosure or restriction should be the default state.

📰 RELATED DAILY ARTICLES

1 Aug **Current Affairs Today, August 1, 2026**

1 Aug **Samudra Manthan: India Bets Rs 84,084 Crore on Offshore...**

1 Aug **No Blanket Ban: The Supreme Court Takes Up Pellet Guns...**

1 Aug **Regulating the Way Down: India Issues Its First...**

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

📖 Read Full Article on Ujiyari →

https://ujiyari.com/editorials/2026/08/ie-cnap-right-to-know-caller-2026/