ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

THE STRANGER ON THE VIDEO CALL: TRUTH-DEFAULT, TRANSPARENCY AND INDIA'S DIGITAL ARREST SCAMS

Dr. Janet Paul[1], Pandu Aravind[2],
[1]*Principal, Alpha Gen School, Tekkali*
[2]*English Teacher, Alpha Gen School, Tekkali*

Article DOI: https://doi.org/10.36713/epra31251
DOI No: 10.36713/epra31251

ABSTRACT

On 28 August 2024, the eighty-two-year-old chairman of one of India's largest textile groups answered a telephone call that kept him under fake police custody, on camera, for two days and cost him seven crore rupees. This article reads India's digital arrest epidemic through two connected bodies of work: Timothy Levine's truth-default theory and Malcolm Gladwell's popularisation of it in Talking to Strangers (2019). It argues that these frauds succeed not because their victims are foolish but because the scam weaponises three ordinary features of human communication: our default to belief, our faith in appearances, and the coupling of behaviour to engineered circumstance. It ends with what the psychology of deception cannot explain, which is the entirely rational unease Indian citizens feel when the state appears to come calling.

KEYWORDS*: Digital Arrest, Cyber Fraud, Truth-Default Theory, Malcolm Gladwell, Timothy Levine, Deception Detection*

On the morning of 28 August 2024, S. P. Oswal, chairman and managing director of the Vardhman Group and a Padma Bhushan awardee, took a phone call from a man who introduced himself as an officer of the Central Bureau of Investigation. Oswal was told that his name had surfaced in a money-laundering investigation connected to Naresh Goyal, the arrested founder of Jet Airways, and that he was being placed under "digital arrest". For the next two days he lived inside a production staged entirely for an audience of one. He was instructed to keep Skype running on his phone even while he slept. He received a document laying out seventy rules of "24x7 surveillance", a fabricated order in a case titled *Justice Dhananjaya Y Chandrachud vs Shri Paul Oswal*, and, as the centrepiece, a video hearing before a man impersonating the Chief Justice of India. The "court" directed that his funds be moved into accounts controlled by the "investigation" for verification. He transferred seven crore rupees. Police later recovered Rs 5.25 crore, in what was reported at the time as the largest recovery in an Indian cybercrime case, and arrested two men in Guwahati (TNM Staff).

The obvious question is the wrong one. To ask how a man who has read balance sheets for sixty years could believe a judge inside a Skype window is to assume that detecting the fraud was a matter of intelligence, and that the rest of us, suitably warned, would have switched the phone off. The research on human deception detection points the other way. The better question is what equipment any of us actually possess for discovering that the confident stranger on a video call is not who he says he is. The uncomfortable answer is: very little, and the scammers know it with more precision than their victims do.

A REVIEW OF THE LITERATURE

Three bodies of work meet in this article, and they have rarely been introduced to one another.

The first is the experimental literature on deception detection, which is one of psychology's longer-running humiliations. Decades of laboratory work have failed to find the behavioural signature of lying that police manuals and common sense both promise. A meta-analysis by DePaulo and colleagues of more than a hundred candidate cues found the classic tells, gaze aversion, fidgeting, nervous speech, to be weakly related or unrelated to actual deception (DePaulo et al.). Judgement studies fare no better: across hundreds of experiments, observers separate lies from truths at rates scarcely distinguishable from chance, and professionals such as police officers and customs inspectors improve little on students, though they are considerably more confident (Bond and DePaulo; Vrij). Levine's contribution was to reinterpret this failure as design rather than defect. His truth-default theory proposes that belief, not evaluation, is our resting state; that suspicion requires a trigger; and that the arrangement is adaptive, because most communication is honest (Levine, "Truth-Default Theory" 378-92). *Duped* consolidates two decades of this experimental programme.

The second body of work is Gladwell's book and the argument around it. *Talking to Strangers* carried Levine's theory, together with research on the illusion of transparency and on the coupling of behaviour to context, to a very large general readership. Its reception was divided: admirers found the synthesis masterly, while critics found the method loose, the cases selectively arranged and the theory pressed harder than the evidence allows (Ferguson). This article takes that criticism seriously and uses the book accordingly, as a lens with unusual reach, kept honest by the primary research beneath it.

The third is the criminology of fraud victimisation. Whitty's stage model of the online romance scam, built from interviews with victims, describes a choreography that will look familiar throughout this article: a credible approach, the gradual escalation of requests, the manufacture of urgency, and the deliberate isolation of the victim from anyone who might break the spell (Whitty). Button and Cross document how cyber fraud victims cut across lines of education, income and age, and how poorly the stereotype of the gullible victim survives contact

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

with the data (Button and Cross). Cross has shown, further, that the stereotype is not idle: the anticipation of ridicule and blame measurably suppresses reporting, which in turn flatters the official statistics (Cross).

On digital arrest itself, scholarship is only beginning. The phenomenon has so far been mapped mainly by journalists, courts and policy analysts (Rej), and the first psychological treatments have now appeared: Robert and colleagues, in a recent perspective article, read the scam through obedience research and authority bias, arguing that its victims are psychologically rather than technologically vulnerable (Robert et al.). What is missing, and what this article attempts, is a connection between the scam and the deception-science tradition proper: an account in which digital arrest appears not as an exotic new crime but as an industrial application of the oldest findings in the field, staged, in India, against a particular experience of the state.

An Epidemic of believing

The scale of the phenomenon is now a matter of parliamentary record. In 2024, Indians filed 1.23 lakh complaints of digital arrest fraud on the National Cybercrime Reporting Portal and lost Rs 1,935.51 crore to it, the Minister of State for Home Affairs informed the Rajya Sabha in March 2025. The trajectory is steep: reported losses were Rs 91.14 crore in 2022 and Rs 339 crore in 2023, and the first two months of 2025 alone added a further Rs 210.21 crore (Team Inc42). The real figures are certainly higher, since shame keeps an unknown share of victims from filing at all. The alarm has reached the top of both the executive and the judiciary. Prime Minister Narendra Modi devoted a section of his Mann Ki Baat broadcast in October 2024 to the scam, telling listeners that “there is no such thing as ‘digital arrest’” and that “no investigative agency will ever contact you by phone or video call for enquiries”, and observing that “people from every class and age group” have lost “lakhs of rupees earned through their hard work, out of sheer fear” (“Modi Raises”). By July 2026 the Supreme Court, hearing a suo motu case on the scams, had urged the Union government to define digital arrest as a distinct criminal offence with enhanced punishment, and the Solicitor General told the court that legislation covering digital arrests and deepfakes was being drafted (Roy). Days later the court directed the Reserve Bank of India to put in place a standard operating procedure for banks, along with grievance redressal and money restoration mechanisms for victims (Shrivastava).

The scam itself did not appear from nowhere. It is the refinement of earlier waves of telephone fraud, the courier parcel supposedly held at customs, the mobile number about to be disconnected, each round of which taught its operators which pretexts opened a conversation and which closed it. What distinguishes the digital arrest variant is its scale of organisation: call-centre operations working from scripts, costume and set dressing for the video stage, and networks of mule accounts waiting at the far end. This is not an opportunist’s trick. It is an industry with a product, and the product is manufactured belief.

Public commentary, meanwhile, still runs mostly on a single explanation: gullibility. The victim, in this telling, is insufficiently alert, insufficiently modern, insufficiently intelligent, and the remedy is another round of awareness messaging. The difficulty is that the victim profile refuses to cooperate. The defrauded include senior doctors, serving and retired civil servants, software professionals, academics and, in Oswal, one of the country’s most experienced industrialists. If susceptibility were a function of education or intelligence, the epidemic would look very different. Something else is being exploited, and it is not stupidity.

The Science of the Truth-Default

The most useful account of that something comes from the communication scholar Timothy Levine, whose truth-default theory holds that human beings are built to assume, passively and without deliberation, that the people communicating with them are honest. Doubt is not our resting state. It must be triggered, and even when it is triggered we tend to explain our suspicions away until they become impossible to sustain. Levine’s experiments, in which observers try to identify students who have cheated in a trivia game, find again and again that people, including trained interrogators, perform barely better than chance; the fullest statement of the theory and its evidence is his book *Duped*. His findings sit on top of one of the most replicated results in social psychology: a meta-analysis of more than two hundred studies by Charles Bond and Bella DePaulo found that people distinguish lies from truths at an average accuracy of 54 per cent, a whisker above tossing a coin (Bond and DePaulo). The figure barely moves for police officers, customs inspectors or judges. Expertise changes the confidence of the judgement, not its accuracy.

Malcolm Gladwell built *Talking to Strangers* around Levine’s idea, and his summary of it is usefully blunt: “We start by believing. And we stop believing only when our doubts and misgivings rise to the point where we can no longer explain them away” (Gladwell 74). His case studies are the spies and fraudsters of recent American history, Ana Montes inside the Defense Intelligence Agency and Bernie Madoff inside the financial establishment, and his point is that the people they deceived were not the credulous but the well-informed, experienced professionals whose doubts were repeatedly raised and repeatedly explained away. The counterexample proves the point. Harry Markopolos, the financial analyst who deduced Madoff’s fraud nearly a decade before it collapsed, was the rare man with no truth-default to exploit. He was also ignored by every institution he warned, and he ended the affair armed and checking his door, convinced that no one else would see what he saw. Gladwell offers him not as a model but as a caution: the person constitutionally incapable of being fooled is also constitutionally incapable of being believed.

Neither Levine nor Gladwell, and this is the hinge of the argument, treats the truth-default as a defect. A person who trusted nothing could not maintain a marriage, a business or a queue at a bus stop. Deception is rare in ordinary life, so a default to belief is efficient almost all of the time. The price of a workable society is that the rare predator gets a free run.

The digital arrest scam industrialises that free run. Its script is engineered so that no single step trips the trigger that converts belief into suspicion. The opening call is mundane: a courier parcel, a telecom notice, a bank alert. The escalation to “police” arrives with verifiable-sounding case numbers and real public names, in Oswal’s case that of Naresh Goyal, lifted from the news. Each new demand is only slightly more unusual than the last, and the fiction itself supplies the explanation for every misgiving: of course the matter is secret, it is a money-laundering case; of course the money must be moved, the accounts must be audited; of course you cannot consult your lawyer, that would be tipping off. The victim's doubts do rise. What the script removes is any moment at which they can no longer be explained away. Levine's theory predicts exactly this vulnerability, and the scam behaves like a machine built by people who have read him.

The Theatre of transparency

The second exploited assumption is the one Gladwell calls transparency: the belief that what people are is legible in how they look and behave. "When we don't know someone, or can't communicate with them, or don't have the time to understand them properly," he writes, "we believe we can make sense of them through their behaviour and demeanour" (Gladwell 152). The belief is ancient and it is false. In one of the book's most memorable passages, researchers who coded the facial expressions of actors in an episode of *Friends* found the emotions perfectly readable from faces alone, which is precisely why real life misleads us: we expect the world to perform feeling the way television does. Real liars are frequently calm, and real innocents frequently twitchy. Gladwell's exhibit is Amanda Knox, who spent nearly four years in an Italian prison substantially because her odd demeanour after her flatmate's murder was read as guilt.

Seeing a person, in other words, does not sharpen our judgement of them, and can corrupt it. Gladwell reports an American study in which bail decisions made by an algorithm working only from the case file outperformed those of judges who had the defendant standing in front of them. The face supplied information, and the information was wrong. It is worth holding that finding up against the intuition, shared by every victim of a video-call fraud, that a thing witnessed on screen has been verified.

The digital arrest scam runs the same error in reverse. Where Knox was a mismatched innocent, punished because she did not look the part, the scammer is a matched liar, rewarded because he looks it exactly. Transparency is not merely assumed by the victim; it is manufactured by the criminal. The uniform is correct. The precinct visible behind the "officer" is correct. The letterhead, the seal, the case caption, the seventy-point surveillance order served on Oswal, all of it is costume and set design for the victim's demeanour-reading machinery, which duly votes yes. The video call, which feels like verification, is the heart of the trick: seeing, we believe, is believing. But video transmits performance, not truth, and performance is now cheap to fabricate. In Oswal's case a human impersonated the Chief Justice; the Supreme Court's insistence, in the same breath as its digital arrest recommendations, that Parliament legislate on deepfakes recognises that the next impersonator need not be human at all (Roy).

Coupling, or the scene of the crime

The third and least noticed of Gladwell's ideas is coupling: the finding that behaviour is tied to particular places, instruments and circumstances far more tightly than our character-based explanations allow. His central example is the fall in British suicides that followed the replacement of coal gas in domestic kitchens, evidence that removing the means from the moment prevents the act rather than displacing it. The criminological implication is that context is not the backdrop of conduct but a component of it.

Read with this idea, the digital arrest scam is a study in the engineering of circumstance. Nothing about its stage set is accidental. The call arrives unannounced, at home, where institutional theatre is least expected and least checkable. The victim is immediately isolated: Oswal was ordered to keep Skype on "even during sleep" (TNM Staff), and victims are routinely forbidden from telling family members, colleagues or lawyers, on pain of aggravating their "case". The camera never blinks, reproducing the psychology of actual custody: watched continuously, the victim begins to behave as though the authority were real, and compliance deepens by the hour. Urgency forecloses reflection. And at the end of the pipeline sit instant payment rails and networks of mule accounts, which move the money out of reach in minutes. Every element couples the victim to the one environment in which the fraud can breathe.

The policy consequence follows directly, and it is the same one Gladwell draws from the gas ovens: change the environment, not the sermon. Awareness campaigns ask citizens to out-argue their own truth-default in real time, which the evidence suggests they largely cannot do. Decoupling, by contrast, dismantles the stage. Some of this is already under way. Lakhs of SIM cards, devices and bank accounts, and thousands of fraudulent video-calling identities, have been blocked ("Modi Raises"); the Department of Telecommunications has disconnected some 3.9 million mobile connections linked to cyber fraud ("Sanchar Saathi"); citizens can report suspicious calls through the Chakshu facility on the Sanchar Saathi portal and dial the 1930 cybercrime helpline ("Chakshu"). The Supreme Court's directions to the RBI point the same way: standard procedures that slow suspicious first-time transfers, and restoration mechanisms that make the pipeline less profitable (Shrivastava). A standalone offence, as the court urges, would complete the redesign (Roy): naming the crime lets the system count it, prosecute it as itself rather than as a patchwork of impersonation and extortion provisions, and build victim compensation on a settled footing. None of these measures asks the citizen to become a better lie detector. That is their virtue. Fraud that operates from compounds beyond Indian jurisdiction cannot reliably be arrested; its stage, its props and its payment pipeline are all within reach.

What psychology cannot explain

It would flatter the theory, though, to stop here, and it would repeat the central weakness of Gladwell's book. *Talking to Strangers* habitually universalises encounters that are structured by power, most damagingly in its reading of the death of Sandra Bland, where the language of mutual misunderstanding quietly levels a confrontation between an armed officer and a citizen who had every reason to fear him. An Indian account of the digital arrest scam must not make the mirror-image mistake. Truth-default and transparency are universal human equipment, but the scam's stage set is local, and what it stages is the Indian state.

The threat "you are under arrest" lands with particular force in a country where an encounter with an investigating agency is widely experienced as unpredictable, protracted and ruinous regardless of guilt, where process itself can function as punishment. The fraudsters did not create that fear; they rent it.

The counterfeit CBI works because the real one is feared, and the fake court order compels because the real summons does. Nor is arrest the only lever. For a certain class of victim the deeper threat is disgrace: the name in the newspaper, the neighbours' knowledge, the stain of a case regardless of its outcome. The scripted insistence on secrecy, ostensibly a condition of the "investigation", is aimed squarely at this respectability, and it does double work, since the same shame that keeps the victim from calling a lawyer during the fraud keeps many from filing a complaint after it. There is a quiet institutional admission inside the Prime Minister's reassurance that no agency conducts enquiries by video call: the state found it necessary to teach citizens what its own lawful conduct looks like, because they could not tell ("Modi Raises"). A complete account of the epidemic therefore needs political sociology as much as psychology. The victims believed a story about their state that the state's own conduct has made believable. Deception researchers cannot fix that, and neither can the RBI.

The distribution of the harm is not universal either. The scam disproportionately finds the elderly, the recently online, and households where a single frightened person controls the family savings, and it finds them in their own homes, outside the institutional settings where a second opinion is natural. Awareness campaigns are not useless here; the Prime Minister's formula of "stop, think, take action" is sound advice compressed to three words ("Modi Raises"). But advice presumes a moment of calm in which to apply it, and the entire architecture of the scam, the urgency, the isolation, the camera that never blinks, is built to abolish that moment. Education addresses the citizen the scam has already been designed around.

Caution and Humility, Institutionalised

Gladwell ends his book with advice: "The right way to talk to strangers is with caution and humility" (262). As a personal maxim this is thin armour against a professional script rehearsed on thousands of victims, and the evidence reviewed here suggests that no private vigilance will reliably beat a well-built con. But the maxim scales. Caution and humility can be institutionalised: in payment systems that pause where fraud concentrates, in telecom networks that strip the scam of its props, in verification channels that let a frightened citizen check a claim of authority in one call, and in a legal category that names the crime. Levine would add a warning of his own: the answer cannot be to abandon the truth-default, because a society that stops believing strangers stops functioning. The default is worth defending precisely because it is worth exploiting.

The last word belongs to the book's bleakest observation. "Because we do not know how to talk to strangers," Gladwell writes, "what do we do when things go awry with strangers? We blame the stranger" (346). In fraud, with grim irony, the stranger we blame is usually the victim, whose foolishness makes a more comforting story than our shared design. The Rs 1,935 crore lost in 2024 was not lost to stupidity. It was lost to an industry that has studied how human beings believe one another and built, around that knowledge, a stage, a costume and a script. Until the stage is dismantled, every one of us is one unexpected phone call away from the stranger who knows exactly how we trust.

WORKS CITED

1. *Bond, Charles F., Jr., and Bella M. DePaulo. "Accuracy of Deception Judgments." Personality and Social Psychology Review, vol. 10, no. 3, 2006, pp. 214-34.*
2. *Button, Mark, and Cassandra Cross. Cyber Frauds, Scams and Their Victims. Routledge, 2017.*
3. *"Chakshu: Report Suspected Fraud Communication." National Government Services Portal, Government of India, services.india.gov.in/service/detail/chakshu-report-suspected-fraud-communication. Accessed 10 Aug. 2026.*
4. *Cross, Cassandra. "No Laughing Matter: Blaming the Victim of Online Fraud." International Review of Victimology, vol. 21, no. 2, 2015, pp. 187-204.*
5. *DePaulo, Bella M., et al. "Cues to Deception." Psychological Bulletin, vol. 129, no. 1, 2003, pp. 74-118.*
6. *Ferguson, Andrew. "Malcolm Gladwell Reaches His Tipping Point." The Atlantic, 10 Sept. 2019. Medium, medium.com/the-atlantic/malcolm-gladwell-reaches-his-tipping-point-5920f45915ca.*
7. *Gladwell, Malcolm. Talking to Strangers: What We Should Know about the People We Don't Know. Little, Brown, 2019.*
8. *Levine, Timothy R. Duped: Truth-Default Theory and the Social Science of Lying and Deception. U of Alabama P, 2019.*
9. *---. "Truth-Default Theory (TDT): A Theory of Human Deception and Deception Detection." Journal of Language and Social Psychology, vol. 33, no. 4, 2014, pp. 378-92.*
10. *"Modi Raises 'Digital Arrest' Scam in Mann Ki Baat; Lakhs of Bank Accounts Blocked, Says PM." The Week, 27 Oct. 2024, www.theweek.in/news/india/2024/10/27/modi-raises-digital-arrest-scam-in-mann-ki-baat-lakhs-of-bank-accounts-blocked-says-pm.html.*
11. *Rej, Abhijnan. "India's Digital Arrest Scams." The Interpreter, Lowy Institute, 10 Sept. 2025, www.lowyinstitute.org/the-interpreter/india-s-digital-arrest-scams.*
12. *Robert, S. James, et al. "Digital Arrest in the Cyber Age: A Psychological Perspective on Fear, Authority, and Consciousness." Frontiers in Psychology, vol. 17, 2026, doi.org/10.3389/fpsyg.2026.1726740.*
13. *Roy, Debayan. "Supreme Court Calls for Separate Offence on Digital Arrests, Harsher Punishment against Accused." Bar and Bench, 28 July 2026, www.barandbench.com/news/supreme-court-calls-for-separate-offence-on-digital-arrests-harsher-punishment-against-accused.*
14. *"Sanchar Saathi: DoT Disconnects 3.9 Mn Mobile Connections over Cyber Fraud." Business Standard, 6 Feb. 2026, www.business-standard.com/technology/tech-news/sanchar-saathi-dot-disconnects-3-9-mn-mobile-connections-over-cyber-fraud-126020600513_1.html.*
15. *Shrivastava, Amisha. "Digital Arrest Scams: Supreme Court Issues Directions for Prevention, Compensation and Grievance Redressal." LiveLaw, 4 Aug. 2026, www.livelaw.in/top-stories/digital-arrest-scams-supreme-court-issues-directions-for-prevention-compensation-greivance-redressal-544292.*
16. *Team Inc42. "Indians Lost INR 1,935 Cr to Digital Arrest Scams in 2024: Govt." Inc42, 14 Mar. 2025, inc42.com/buzz/indians-lost-inr-1935-cr-to-digital-arrest-scams-in-2024-govt/.*
17. *TNM Staff. "How an Indian CEO Lost Rs 7 Crore to Scammers Who Pretended to Be ED, CBI and CJI." The News Minute, 2 Oct. 2024, www.thenewsminute.com/news/how-an-indian-ceo-lost-rs-7-crore-to-scammers-who-pretended-to-be-ed-cbi-and-cji.*

18. *Vrij, Aldert. Detecting Lies and Deceit: Pitfalls and Opportunities. 2nd ed., John Wiley, 2008.*
19. *Whitty, Monica T. "The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam." British Journal of Criminology, vol. 53, no. 4, 2013, pp. 665-84.*