Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The Evidentiary Black Hole: Ephemeral Messages in Corporate Fraud Investigations

Abhigyan Shrivastava[a]

[a]Uttar Pradesh State Institute of Forensic Science (UPSIFS), Lucknow, India

Received 28 May 2026; *Accepted* 29 June 2026; *Published* 03 July 2026

The foundation of corporate governance is built on a deceptively straightforward idea: the preservation of truth through documentation. For decades, fraud investigations could trace a predictable, if painstaking, electronic trail: archived emails, server logs, corporate hard drives. That world has been fundamentally disrupted. The mass adoption of self-destructing messaging platforms WhatsApp, Signal, Telegram, and Wickr, equipped with end-to-end encryption (E2EE) and features such as 'View Once' and disappearing chats, has introduced a crisis into white-collar investigations. This article examines how ephemeral communication has been co-opted by bad actors to construct a technological sanctuary for corporate malfeasance. Viewing the problem first through the lens of US regulatory crackdowns by the SEC and the DOJ, it then pivots decisively to the Indian legal landscape. It diagnoses the evidentiary challenges confronting SEBI and the CCI, evaluates admissibility standards under the Bharatiya Sakshya Adhiniyam 2023 and the Information Technology Act 2000, and approaches the crisis through the eyes of a litigator walking into court empty-handed. By erasing real-time intent before any investigation can begin, auto-deleting media creates an 'evidentiary black hole' that can only be closed through a combination of technical safeguards and legislative reform.

Keywords: *ephemeral messaging, corporate fraud, electronic evidence.*

INTRODUCTION

Imagine a driver is stopped at a red traffic light. As it turns green, he speeds up to cross the street. But a split second later, the traffic system glitches and the light suddenly turns red again. A police officer stops him and accuses him of running the red light. The driver has zero proof that he is innocent. He has no dashcam, and there are no street cameras around. Also, the traffic light computer failed to record the quick green flash. When asked to prove he did not break the law, the driver is totally stuck. He has no supporting evidence at all.

This normal traffic problem is exactly like the big crisis happening right now in corporate fraud investigations. The main rule of checking for bad behaviour is that crimes always leave a trail. Now that the rule is falling apart. For decades, investigators from places like the Securities and Exchange Board of India (SEBI), the Competition Commission of India (CCI) and the US Securities and Exchange Commission (SEC) could just read old emails and computer hard drives to figure out fraud and catch bad executives.[1]

Now that the clear trail is gone. Apps like WhatsApp and Signal let bosses and traders send secret text and voice messages that leave zero trace. Features like WhatsApp Disappearing Messages easily beat normal saving methods. At first, people loved these apps because they protected privacy. But now bad actors use them as a safe spot for corporate crimes. By erasing the evidence before an investigation can even begin, disappearing messages create an evidentiary black hole.

THE MECHANICS OF TRANSIENCE: HOW EPHEMERAL MESSAGING WORKS

From Permanent Archives to Vanishing Conversations: For decades, enterprise communication was working around the principle of persistence. When an executive sends an email via Microsoft Outlook or a message over a corporate network, that data is indexed across local relays, backed up on physical or cloud-based servers, and retained under strict schedules mandated by Section 128(5) of the Companies Act 2013.[2] Even a maliciously deleted inbox can be forensically reconstructed; metadata survives, database files linger in unallocated disk clusters, and mirror copies sit on corporate Exchange servers. Ephemeral

[1] Stuart P Green, *Lying, Cheating, and Stealing: A Moral Theory of White-Collar Crime* (OUP Oxford 2007)
[2] Companies Act 2013, s 128(5)

messaging inverts this reality. These platforms are based on two interlocking mechanisms that together defeat conventional forensic investigation.

First, end-to-end encryption (E2EE) ensures that a message is encoded on the sender's device and can only be decoded on the recipient's device. No one in between, not the internet service provider, not the corporate IT department, and not the platform itself (whether Meta's WhatsApp or the Signal Foundation) holds the keys to read what was sent.[3] This is not a flaw in the system; it is the system's purpose. The consequence for investigators is that even a lawful preventing order directed at the server returns nothing intelligible.

Second, automated deletion removes the message at the endpoint. Whether through WhatsApp's 'View Once' feature, which prevents a photo, video, or document from being saved, forwarded, or even screenshotted without using a secondary device or Signal's configurable self-destruct timers, the application executes an overwrite command once the message is read or the time limit to view is passed.[4] Telegram's secret chats operate identically, leaving no trace on Telegram's own servers.

Why Deletion is not Recovery: The Forensic Reality: In ordinary digital forensics, a deleted file is not truly gone. The operating system removes its directory pointer and marks the storage space as available, but the data payload itself waits until new information physically overwrites it.[5] Standard recovery tools exploit this window to reconstruct deleted files from unallocated clusters.

Ephemeral messaging closes that window entirely. Many applications perform secure wiping protocols or clear the relevant flash memory blocks on deletion. The message never existed on the company's server in a readable format, and on the other hand, for the end user's device, the link to it was not merely removed, as it was overwritten, leaving absolutely no trace of it anywhere. Because many applications perform repeated overwriting on deletion, standard imaging procedures conducted by the Central Forensic Science Laboratory (CFSL) under the IT Act 2000 are ineffective.

---

[3] 'Secure by design' (*WhatsApp Security*) <https://www.whatsapp.com/security/> accessed 24 May 2026
[4] 'About view once' (*WhatsApp Help Center*) <https://faq.whatsapp.com/general/chats/about-view-once> accessed 24 May 2026
[5] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn, Academic Press 2011)

THE MODUS OPERANDI OF ZERO TRACE CORPORATE MISCONDUCT

Understanding this technology explains how easily it becomes a weapon. In the past, major conspiracies left massive paper trails. During the Satyam accounting fraud, for instance, investigators managed to rebuild the entire corporate fraud case simply by digging through the company's internal emails and messages.[6] Similarly, investigators broke open the LIBOR (London Interbank Offered Rate) manipulation scandal in the West by digging through saved Bloomberg (The Software) chats. Those saved chats let investigators establish mens rea, the criminal intent that is the basis of any prosecution and prove that conspirators had a meeting of the minds.

Nowadays, corrupt people in big companies have figured out how to work across two separate tracks at the same time. Routine HR emails, board minutes, and official updates go through monitored corporate accounts, making everything look perfectly compliant on the surface. Meanwhile, the actual illegal activity, like price fixing, sharing insider secrets, and plotting to fake the accounts, happens over WhatsApp disappearing messages, Signal groups with burn-on-read timers, or Telegram secret chats. The official record is clean. The whole point of using these apps is to operate without leaving a single digital trace. Indian regulators have seen this split-channel tactic over and over again in cartel and insider trading cases.[7]

HOW REGULATORS PUSH BACK: A COMPARATIVE VIEW

The US: When Fines Run into Billions: The US led the first regulatory crackdown. Under SEC Rule 17a-4 and CFTC Regulation 1.31, broker-dealers must keep business messages in a non-erasable format for three years. In late 2021, regulators swept Wall Street for 'off-channel communications,' finding that traders routinely used WhatsApp and Signal on personal phones to share market secrets. This resulted in unprecedented fines totalling billions of dollars. At the same time, the DOJ's 2023 Compliance Guidelines added that if executives use auto-delete apps, their firm loses all cooperation credit, as prosecutors will assume the data was wiped to cover up corporate crimes.[8]

---

[6] Ayushi Mendhiratta, 'M/S Satyam Computer Services Ltd vs Directorate of Enforcement' (*Lawful Legal*, 19 July 2025) <https://lawfullegal.in/m-s-satyam-computer-services-limited-vs-directorate-of-enforcement/> accessed 24 May 2026

[7] *In Re: Cartelisation in Industrial and Automotive Bearings* CCI Suo Motu Case No 05/2017

[8] *Evaluation of Corporate Compliance Programs* (US Department of Justice Criminal Division, 2024)

The Indian Regulatory Landscape: SEBI, CCI, and the IT Act: India's response operates through a more complex system: the IT Act 2000, SEBI's regulations, the CCI's investigative powers, and national cybersecurity directives. In India, the situation is different because WhatsApp is not just a casual app anymore. It is the dominant way everyone talks and handles business across the entire corporate ladder.

SEBI and Insider Trading: Under the SEBI (Prohibition of Insider Trading) Regulations 2015, listed companies are required to maintain a Structured Digital Database (SDD) recording every person with whom Unpublished Price Sensitive Information (UPSI) or insider secrets is shared.[9] SEBI was forced to act because people were leaking sensitive financial data on WhatsApp groups before companies could officially announce it, an issue known as the 'WhatsApp Leaks' scandal. In Shruti Vora v Securities and Exchange Board of India, SEBI stepped in to find out who was circulating the confidential financial numbers of big-name companies in private WhatsApp groups right before they were set to go public.[10] Because end-to-end encryption (E2EE) blocked them completely, SEBI used its search and seizure powers under Section 11C of the SEBI Act, 1992[11] to launch early morning raids. They confiscated cell phones from over twenty-four traders and read the unencrypted messages straight from the unlocked devices before users could delete them.

Where direct digital evidence was unavailable, SEBI pressed circumstantial inference. In SEBI v Kishore R Ajmera, the Supreme Court held that SEBI may establish insider trading on the 'preponderance of probabilities' through circumstantial evidence where direct proof is absent.[12] That doctrine is valuable, but it is perpetually stretched thin when the very digital footprints needed to build a circumstantial chain have already been automatically erased.

CCI and cartelisation: The Competition Commission of India has come to rely heavily on seized WhatsApp conversations to establish the meeting of the minds that Section 3 of the Competition Act 2002 requires before cartelisation can be found. In the Beer Cartel probe and the Industrial and Automotive Bearings case, the Director General of the CCI used WhatsApp exchanges between senior executives as primary evidence of price fixing.[13] The

[9] SEBI (Prohibition of Insider Trading) Regulations 2015, reg 3(5)
[10] *Shruti Vora v Securities and Exchange Board of India* App (L) No 28/2020
[11] *Ibid*
[12] *Securities and Exchange Board of India v Kishore R Ajmer* (2016) 6 SCC 368
[13] *In Re: Alleged anti-competitive conduct in the Beer Market in India* (CCI Suo Motu Case No 06/2017

CCI has taken a clear stand: talking over casual chat apps does not give you a pass. Those messages are still treated as solid legal evidence. According to the CCI, casual WhatsApp messages about price fixing hold the same legal weight as official board resolutions. The real issue is the disappearing messages feature, which leaves no digital trail. Because of this, the regulator has to count on whistleblowers using the leniency program as a much more uncertain route for an investigation.

The IT Act 2000 and CERT-In directions: Under the broader Information Technology Act 2000, Section 69 grants the government the power to intercept and decode any information transmitted across digital networks. But against end-to-end encryption, these government powers hit a dead end. Because WhatsApp and Signal do not have access to the decryption keys, it is technically impossible for them to turn over plain, readable text. This tension gave rise to Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, which requires significant social media intermediaries to enable traceability of the 'first originator' of a message.[14] The rule triggered constitutional litigation in WhatsApp LLC v Union of India, with platforms arguing that mandating traceability necessarily breaks E2EE, violating the fundamental right to privacy recognised in Justice K S Puttaswamy (Retd) v Union of India.[15]

Separately, CERT-In, acting under Section 70B of the IT Act, issued its 2022 Cybersecurity Directions requiring corporate entities, data centres, and service providers to retain all ICT system logs for a rolling 180-day period. The use of self-deleting messaging applications on corporate infrastructure directly sabotages this compliance obligation, placing enterprises in the position of simultaneously violating their cybersecurity duties and their communications governance obligations.

A LITIGATOR'S PERSPECTIVE: WALKING INTO COURT EMPTY-HANDED

The Evaporation of Intent: Understand how big this problem really is, you must look at it from a prosecutor's perspective, standing in a courtroom knowing exactly what happened but having almost no evidence that can be used in court. In criminal and quasi-criminal corporate matters, establishing mens rea (Mental Intention) is not optional. A prosecution

[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4(2)
[15] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2019) 1 SCC 1

must show not merely that the accused acted, but that they acted with deliberate wrongful intent. In the past, email records showing executives agreeing to leak confidential pricing data functioned as undeniable evidence.

With ephemeral messaging, that anchor is gone. Without message logs, prosecutors must try to prove a conspiracy solely through circumstantial evidence. This means pointing out that two companies raised prices simultaneously or two traders copied each other's market moves at the same time. Indian courts and tribunals do permit this approach: in V K Kaul v SEBI, the Securities Appellate Tribunal affirmed the use of circumstantial evidence to establish insider trading.[16] Defence counsel, however, exploits the absence of direct communication brilliantly. They frame simultaneous price movements as organic market competition or coincidence. Without the vanished WhatsApp conversation to link the parallel conduct to a shared criminal purpose, the litigator cannot establish even a prima facie case, a case that, on its face, discloses a cause of action. The theory exists, but the evidence does not.

The Admissibility Wall Under the Bharatiya Sakshya Adhiniyam 2023: If a piece of electronic evidence does survive a screenshot taken by a co-conspirator before a 'View Once' message vanished, for instance the litigator faces a second obstacle: the strict admissibility framework now codified under Section 63 of the Bharatiya Sakshya Adhiniyam 2023 (BSA), which replaces and substantially mirrors Section 65B of the Indian Evidence Act 1872.[17] The Supreme Court in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal settled any doubt: a certificate confirming the integrity and operating status of the computer source is a mandatory condition precedent for the admission of secondary electronic evidence.[18]

Consider what this means for that screenshot. Because of auto-delete features, the original message on the sender's device is gone, having already been automatically overwritten. The litigator must now procure a Section 63 BSA certificate for a photograph of a screen, taken on a third party's personal phone. Defence counsel immediately challenges: the screenshot could be a fabrication, a digitally altered image, because without the primary source, its hash value cannot be verified against an original. The critical evidence gets dismissed purely on

[16] *Mr V K Kaul v SEBI* (2012) 116 SCL 24
[17] Bharatiya Sakshya Adhiniyam 2023, s 63; Indian Evidence Act 1872, s 65B
[18] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors* AIR 2020 SC 4908; *Anvar P V v P K Basheer & Ors* (2014) 10 SCC 473

procedural rules rather than the facts of the case. The application's automated deletion saves the defendant, doing more work for them than their own legal team.

THE AUTO-DELETE DEFENCE: WHY DIGITAL FORENSICS AND COURTS ARE FALLING BEHIND

In the United States, when a lawyer faces intentional evidence destruction, they can use a well-known remedy: Federal Rule of Civil Procedure 37(e). In WeRide Corp v Kun Huang, the court handed down a case terminating sanctions because the defendants deliberately ignored a preliminary injunction. The judge found that their continued use of auto-deleting communication platforms was a purposeful effort to keep critical evidence beyond the reach of investigators.[19]

India's framework relies on penal provisions rather than civil discovery sanctions. Section 201 of the Indian Penal Code 1860, carried forward as Section 238 of the Bharatiya Nyaya Sanhita 2023, criminalises the destruction of evidence to screen an offender.[20] Under Section 114(g) of the Indian Evidence Act, which is now Section 119(g) of the BSA, courts can draw an adverse inference. This means that if a party decides to hide or withhold evidence, the judge can assume that the missing data would have hurt their case.[21]

The problem is that an executive facing a SEBI or CCI investigation needs only to say that the 24-hour disappearing timer on their WhatsApp was activated months ago as a matter of routine digital hygiene an entirely plausible, even legally defensible position given Section 8(7) of the Digital Personal Data Protection (DPDP) Act 2023, which obliges Data Fiduciaries to delete personal data once its purpose is fulfilled.[22] The deletion was not triggered by knowledge of the investigation, as it ran automatically. Proving the specific criminal intent, the mens rea required under Section 238 BNS[23] becomes, in this framing, almost impossible. The Latin phrase suppressio veri, suggestio falsi (hiding the truth is the same as lying) perfectly captures why this behaviour is wrong. However, while the moral issue is clear, the

[19] *WeRide Corp et al v Huang et al* (2019) No. 5:2018cv07233 - Document 352 (Nd Cal)
[20] Indian Penal Code 1860, s 201; Bharatiya Nyaya Sanhita 2023, s 238
[21] Indian Evidence Act 1872, s 114(g); Bharatiya Sakshya Adhiniyam 2023, s 119(g)
[22] Digital Personal Data Protection Act 2023, s 8(7)
[23] Bharatiya Bharatiya Nyaya Sanhita 2023, s 238

law requires prosecutors to prove a deliberate intent to destroy evidence, which is impossible when an app's software deletes everything automatically.

The Tech Trap: Controlling Apps That Delete the Evidence: The goal is not to ban modern communication tools but to take their unfair advantage of their untraceability when used for corporate purposes. Indian enterprises must move away from consumer-grade, unmanaged instances of WhatsApp, Signal, and Telegram toward enterprise-grade platforms. Tools like Symphony, Slack Enterprise Grid, and purpose-built compliance overlays support what practitioners call 'managed ephemerality.'

This model allows messages to expire on user devices to prevent data leaks from lost or stolen phones. But before the payload disappears, a business-level interface captures the data at the network layer and stores a permanent plain-text copy in a secure WORM (Write Once, Read Many) archive. As a result, users get an automated clean-up tool, while corporations maintain a legally defensible record that follows SEBI's document preservation rules.

Along with archiving, companies must use Mobile Device Management (MDM) and Data Loss Prevention (DLP) tools. On company phones, MDM software blocks unapproved apps like personal WhatsApp, Signal, or Telegram. DLP protocols go further by disabling copy-paste functions. This stops executives from lifting text from secure databases and pasting it into personal, disappearing chats. By fencing the data, these controls force evidence to stay within archivable corporate networks.

When a statutory body, such as the Serious Fraud Investigation Office (SFIO), the Enforcement Directorate (ED), or the CFSL, enters an environment where these controls were absent, investigators must pivot to specialist reclamation techniques. If a device is seized unlocked during a dawn raid, live RAM dumps can extract unencrypted text payloads from active memory before the application executes its overwrite sequence.[24] Where messages have already been purged from the endpoint, investigators look for cloud backup gaps: many users inadvertently leave automated backups active on Google Drive or iCloud. Under Section 94 of the Bharatiya Nagarik Suraksha Sanhita 2023 (formerly Section 91 of the Code

[24] Casey (n 5)

of Criminal Procedure 1973), law enforcement can subpoena those backup caches, which often contain unencrypted database files preserving communication history.[25]

Fixing the Rules: Closing the Legal Loopholes on Auto-Delete Apps: Technology alone cannot seal the black hole if the law continues to allow executives to walk away by invoking data hygiene. Two legislative reforms are essential.

First, India must codify a mandatory statutory presumption under **Section 119(g) of the BSA.[26]** Based on the common law maxim omnia praesumuntur contra spoliatorem (all things are presumed against the destroyer), this rule should automatically apply to any executive caught using unapproved, disappearing chat platforms during a SEBI or CCI investigation. Once unauthorised app use is proven, the burden of proof must shift to the executive to demonstrate that the deleted messages contained nothing illegal. This permanently shifts the disadvantage from the regulator to the wrongdoer.

Second, regulatory boards must establish a clear boundary between DPDP Act data minimisation and corporate preservation mandates:

The Record Carve Out: Communications regarding financial disclosures, UPSI, mergers, or pricing must be excluded from DPDP minimisation obligations and subject to the Companies Act's strict eight-year retention rule.

Banning the Defence: Activating auto-delete features on these records should be treated as automatic evidence destruction (per se spoliation). This eliminates the 'data hygiene' loophole, empowering compliance teams to enforce corporate rules without conflicting legal obligations.

CONCLUSION

The rise of ephemeral messaging applications WhatsApp, Signal, Telegram, Wickr has irrevocably altered the landscape of corporate fraud investigation. Platforms that were designed to protect ordinary users from data exposure have been turned into instruments for dismantling the evidentiary foundations upon which market integrity depends. By treating corporate data as a transitory resource rather than a permanent record, features like

[25] Code of Criminal Procedure 1973, s 91; Bharatiya Nagarik Suraksha Sanhita 2023, s 94
[26] Bharatiya Sakshya Adhiniyam 2023, s 119(g)

E2EE, 'View Once', and disappearing messages have introduced an evidentiary black hole that threatens to shield white-collar crime from SEBI, the CCI, and the ED.

While that traffic light glitch happens by accident, corporations are not passive victims. Instead, they are often the deliberate architects of these convenient digital loopholes. However, the regulatory response, including billions in SEC fines, SEBI's dawn raids, and the CCI's device seizures, signals clearly that the era of using technological fragmentation as a legal shield is ending.

But unlike a driver facing a random traffic glitch, corporations deliberately design these convenient digital loopholes. Global enforcement through billions in SEC fines, SEBI's dawn raids, and CCI device seizures signals clearly that using tech fragmentation as a legal shield is officially over.