

UPSC & STATE PCS CURRENT AFFAIRS · [UJIYARI.COM](https://ujiyari.com)

EDITORIAL ANALYSIS

Jack Dorsey Is Wrong on Bitchat and India's Takedown Order

 HINDUSTAN TIMES

8 August 2026

POLITY

SECURITY & DEFENCE

GS2

GS3

CURATED & WRITTEN BY

**Bharat Choudhary**

UPSC Educator & Content Creator

 linkedin.com/in/epicbharat

ALSO FROM THE CREATOR

BharatNotesFree UPSC notes, MCQs, PYQ analysis. **100% Free.**bharatnotes.com → **ADVERTISE****Advertise with Ujiyari**

Reach thousands of UPSC aspirants daily.

 epicbharat@gmail.com

Jack Dorsey Is Wrong on Bitchat and India's Takedown Order

 **Hindustan Times**

8 August 2026

GS2

GS3

 Every fact web-verified against primary sources

THE LIFT LINE

A state can have a legitimate reason to act and still choose the least transparent way to do it. Both things can be true at once.

WHY THIS EDITORIAL MATTERS FOR YOUR EXAM

Answers on internet governance and free expression tend to default to naming Section 69A. This editorial forces the harder distinction: the actual order here used Section 79(3)(b), a different and less procedurally safeguarded route, to achieve a public-order-based blocking outcome, and knowing which provision was actually used, and why that choice matters, is what separates a Prelims-level answer from a Mains-level one.

GS Paper 2: Indian Constitution: significant provisions and basic structure; separation of powers between various organs; issues and challenges pertaining to the federal structure; role of technology in governance.

GS Paper 3: Cyber security and challenges in security through communication networks; role of media and social networking sites in internal security challenges, cyber security basics.

CONCEPT	MEANING	WHY IT IS TESTABLE
Section 69A, IT Act, 2000	Empowers the Central Government to block public access to information/apps on grounds including sovereignty, defence, security of the state and public order, subject to a review committee process	The IT Act's dedicated, more procedurally safeguarded blocking provision
Section 79(3)(b), IT Act, 2000	Conditions an intermediary's safe-harbour protection on removing unlawful content when directed; used here to order GitHub to disable Bitchat repositories	The provision actually invoked in this case, narrower procedural safeguards than 69A
Mesh network (Bluetooth)	A network where devices relay data directly to each other without a central server or internet connection	Explains why conventional blocking methods (serving notice to a server) do not work on Bitchat
I4C (Indian Cyber Crime Coordination Centre)	Body under the Ministry of Home Affairs that issued the Bitchat blocking order	Institutional actor, examinable as a Prelims fact
Safe harbour	Legal protection shielding an intermediary (like GitHub) from liability for user-uploaded content, conditional on compliance with valid takedown directions	The lever that makes intermediary-directed blocking orders effective even without reaching the underlying technology directly

BACKGROUND AND CONTEXT

The trigger was a directive issued by the **Indian Cyber Crime Coordination Centre (I4C)**, under the **Ministry of Home Affairs**, ordering GitHub to disable public access to three code repositories hosting **Bitchat**, an open-source messaging application associated with **Jack Dorsey**, within three hours of the order.

Bitchat uses **Bluetooth Low Energy mesh networking** to relay encrypted messages directly between nearby devices, without requiring an internet connection, mobile network access, a phone number or a central server. This design allows communication to continue even when conventional connectivity is suspended, which is exactly the circumstance in which it saw increased use.

The order came during a sustained period of protest at **Jantar Mantar, Delhi**, over the **2026 NEET-UG examination paper leak**, in which the National Testing Agency cancelled the examination and referred the matter to the CBI. Authorities suspended mobile internet in a **1.5 km radius** of the protest site and shut **17 Delhi Metro stations**; reporting documented protesters turning to Bluetooth mesh apps to stay in contact once conventional connectivity was restricted.

The order itself invoked **Section 79(3)(b) of the IT Act, 2000**, read with **Rule 3(1)(d) of the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021**, a provision that conditions an intermediary's safe-harbour protection on compliance with a lawful takedown direction, rather than **Section 69A**, the Act's dedicated content-blocking provision.

THE ANALYSIS

- 1. The legal route chosen matters as much as the outcome.** Section 69A carries a review committee process for blocking orders; Section 79(3)(b), the provision actually used here, does not carry an equivalent safeguard, even though this order pursued a public-order and security rationale similar to what 69A is designed for.
- 2. Bitchat's architecture is a genuinely hard case for any state.** With no central server, a conventional takedown notice has nothing to be served to; blocking has to target the code repository, app-store listing or device level, a blunter instrument that is harder to confine to only the misuse it targets.
- 3. The civil-unrest context is specific, not generic.** This was not a blanket judgement about mesh-network technology; it followed weeks of documented protest activity in which internet suspensions were already in effect and Bitchat use rose specifically in response to those suspensions.
- 4. The proportionality question is unresolved by the order itself.** A technology's use by some protesters to evade monitoring does not establish that blocking the repository for all users, the great majority using it entirely lawfully, was proportionate; the order's own text cites risk of misuse rather than documented instances of it.
- 5. The order's practical effectiveness is itself in question.** Reporting indicates Bitchat remained available on major app stores after the GitHub order, since open-source code is easily mirrored elsewhere, which raises a separate question about whether this specific instrument achieves what it sets out to.
- 6. The transparency gap is the strongest structural critique.** Digital-rights groups argue that using Section 79(3)(b) for a public-order-based blocking outcome functions as a way to achieve a 69A-style result without 69A's procedural safeguard, a pattern that, if it recurs, would matter well beyond this single case.

DATA AND INSTITUTIONS VAULT

PRELIMS-GRADE FACTS:

Blocking order issued by: Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs

Legal basis: Section 79(3)(b), IT Act, 2000, read with Rule 3(1)(d), Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 (not Section 69A)

Target: three GitHub repositories hosting Bitchat, ordered disabled within three hours

Bitchat: open-source, Bluetooth Low Energy mesh-network messaging app associated with Jack Dorsey; works without internet, mobile network, phone number or central server

Context: 2026 NEET-UG paper leak protests, Jantar Mantar, Delhi; mobile internet suspended in a 1.5 km radius; 17 metro stations shut

Critics: Internet Freedom Foundation, Software Freedom Law Centre (SFLC.in)

WATCH THE TRAP: DO NOT WRITE THAT THIS ORDER WAS ISSUED UNDER SECTION 69A; THE ACTUAL PROVISION WAS SECTION 79(3)(B), A NARROWER INTERMEDIARY-LIABILITY ROUTE WITH WEAKER PROCEDURAL SAFEGUARDS, AND THAT DISTINCTION IS THE EDITORIAL'S CENTRAL LEGAL FACT.

THE DEBATE

Argument FOR the state's action. A democratically elected government has a legitimate duty to respond when a communication technology is credibly used to evade lawful monitoring during organised civil unrest. The order targeted a specific tool in a specific context, using an existing statutory provision, not a blanket ban on encrypted communication or an extra-legal emergency power, and mislabelling this as authoritarian collapses a meaningful distinction between targeted, lawful regulatory action and general suppression.

Argument AGAINST treating the order as unproblematic. The provision actually used, Section 79(3)(b), lacks the review committee safeguard that applies to Section 69A even though the order pursued a similar public-order rationale, and blocking an entire open-source code repository catches the overwhelming majority of lawful users along with whatever misuse motivated the order, a proportionality concern that a general capability for misuse does not resolve. The order's apparent limited practical effect, given that the app remained available on app stores, also raises the question of what was actually achieved.

Balanced verdict. The state's underlying interest in responding to organised evasion of lawful monitoring during a public-order crisis is legitimate and should not be dismissed as inherently authoritarian. But legitimacy of purpose does not settle the separate question of procedure: routing a public-order-based blocking decision through a provision with weaker transparency and review safeguards than the dedicated blocking provision available for exactly this purpose is a real institutional gap, independent of whether Bitchat itself deserved to be blocked.

HOW TO THINK ABOUT THIS

The transferable pattern: **when a state has more than one legal route to the same outcome, ask which route was chosen and what procedural safeguard that choice avoided, not only whether the outcome itself was justified.**

Legitimacy of purpose and adequacy of procedure are two separate questions, and a state can satisfy the first while failing the second. When a government reaches for a general-purpose provision (intermediary liability, emergency powers, a residuary clause) to achieve an outcome that a more specific, more accountable provision was designed for, the choice of route deserves as much scrutiny as the **substantive** decision itself, because it reveals whether the safeguards built into the specific provision were being deliberately avoided.

This same structure recurs in preventive detention law, where states sometimes invoke broader public-order provisions rather than more specific, more procedurally safeguarded ones; in financial-intermediary regulation, where a general compliance direction can achieve what a more specific, appealable order would otherwise require; and in content regulation more broadly, wherever multiple statutory routes exist to the same practical outcome with different procedural protections attached.

DIAGRAM-IN-WORDS

TWO ROUTES TO THE SAME OUTCOME

SECTION 69A (IT Act)

dedicated blocking provision
grounds: sovereignty, defence,
security, public order

|

REVIEW COMMITTEE

procedural safeguard

|

v

more accountable

blocking route

SECTION 79(3)(b) (IT Act)

intermediary safe harbour
condition: comply with
lawful takedown direction

|

NO EQUIVALENT

REVIEW STEP

|

v

THIS ORDER

(Bitchat, July 2026)

|

v

GitHub directed to disable

3 repositories within 3 hours

|

BITCHAT ARCHITECTURE

no central server to notify

(Bluetooth mesh network)

|

blocking targets repo/app-store

level instead, catches lawful

users along with any misuse
|
app remained on app stores
(limited practical effect)

CRITIQUE: same public-order rationale as 69A, weaker safeguard

TAKEAWAY BOX

The state may have had good reason to act. It still chose the provision with the weaker safeguard to do it.

Order issuer **I4C** (Ministry of Home Affairs); legal basis **Section 79(3)(b) + Rule 3(1)(d)**, NOT Section 69A; target **Bitchat** (Jack Dorsey, Bluetooth mesh-network app), **3 GitHub repositories**, 3-hour compliance window; context **2026 NEET-UG paper leak protests**, Jantar Mantar; **1.5 km** internet suspension radius, **17** metro stations shut; critics **Internet Freedom Foundation, SFLC.in**.

if a technology has a large majority of lawful users and a small minority of users evading lawful monitoring, and the state cannot technically separate the two, does proportionality require accepting some risk of misuse, or does it justify blocking the tool for everyone?

UPSC has examined internet shutdowns, free expression versus state security, and IT Act blocking powers in various forms; this editorial supplies a live case distinguishing between two different statutory blocking routes with different procedural safeguards, a distinction not usually tested with this specificity.

“A state’s authority to block a communication technology during civil unrest does not, by itself, settle whether the procedure chosen to exercise that authority was adequate.” Discuss with reference to the blocking of Bitchat in India in 2026.

Sources: Hindustan Times, PIB, Ministry of Home Affairs

Source: Jack Dorsey Is Wrong on Bitchat and India's Takedown Order — Ujyari.com | Free UPSC & State PCS Editorial Analysis

• KEY ARGUMENTS AT A GLANCE

Rahul Sagar defends the Indian government's order to block Bitchat, Jack Dorsey's peer-to-peer mesh-network messaging app, arguing the state has a legitimate duty to curb technologies deployed to evade lawful monitoring during civil unrest, and that labelling this regulatory action "authoritarian" misrepresents lawful authority exercised by a democratically elected government to protect public order.



SUPPORTING

- The order was issued not under Section 69A of the Information Technology Act, 2000, the general content-blocking provision, but under Section 79(3)(b) read with Rule 3(1)(d) of the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021, a narrower intermediary-liability route through which the Indian Cyber Crime Coordination Centre (I4C) directed GitHub to disable access to Bitchat's code repositories.
- Bitchat is technically distinctive: it is an open-source app using Bluetooth Low Energy mesh networking to relay encrypted messages device-to-device, without requiring internet connectivity, mobile network access, phone numbers or a central server, which is precisely what made it attractive to protesters coordinating during localised internet suspensions.
- The order followed weeks of sustained demonstrations at Jantar Mantar in Delhi over the 2026 NEET-UG paper leak, during which authorities suspended mobile internet within a 1.5 km radius of the protest site and closed 17 metro stations, and reports documented protesters turning to Bluetooth mesh apps, Bitchat among them, once conventional connectivity was cut.
- A server-less, mesh-network app is a genuinely harder case for content moderation than a conventional platform: there is no central server to serve a takedown notice to, so blocking has to happen at the app-store, repository-hosting or device level instead, a blunter instrument more likely to catch the large majority of lawful users in the same action.



COUNTER

Section 79(3)(b) blocking orders in India have drawn sustained criticism, including from the Internet Freedom Foundation and the Software Freedom Law Centre, for functioning as a less transparent, less procedurally safeguarded route than Section 69A, whose blocking orders are at least subject to a review committee process; critics argue this specific order effectively achieved a 69A-style outcome, blocking access to a communication tool for reasons of public order and security, without going through 69A's comparatively more accountable procedure. A technology's use by some protesters to evade lawful monitoring does not by itself establish that blocking the underlying code repository for all users, the vast majority using it for entirely lawful

purposes, was a proportionate response, and reporting suggests the app remained available on major app stores even after the GitHub order, raising questions about what the action actually achieved.

**WAY FORWARD**

Whatever the correct policy outcome on Bitchat itself, the deeper institutional question, whether Section 79(3)(b) intermediary-liability orders should be permitted to achieve public-order and security-based blocking with less procedural transparency than Section 69A requires for the same underlying purpose, needs a clear answer, either by routing such orders through 69A's review mechanism or by building an equivalent transparency and review requirement into 79(3)(b) itself.


MAINS ANSWER FRAMEWORK
QUESTION

A state ordered a decentralised, server-less messaging application blocked during a period of civil unrest, citing risks of evasion of lawful monitoring. Examine the constitutional and technological questions this raises for the scope and transparency of intermediary-blocking powers in India. (250 words)

INTRODUCTION

In July 2026, India's Cyber Crime Coordination Centre (I4C) directed GitHub to disable access to the code repositories of Bitchat, Jack Dorsey's open-source, Bluetooth mesh-network messaging app, after it was used by protesters at Delhi's Jantar Mantar to coordinate during localised internet suspensions. Rahul Sagar's defence of the order, and the criticism it has drawn, together frame a live question about the scope and transparency of India's intermediary-blocking powers.

BODY

The order was issued under Section 79(3)(b) of the Information Technology Act, 2000, read with Rule 3(1)(d) of the 2021 Intermediary Guidelines, rather than the more familiar Section 69A, which is the IT Act's dedicated content-blocking provision and carries a review committee process. Sagar's defence rests on distinguishing a general ban on a communication technology, which would raise serious free-expression concerns, from a targeted response to a specific tool credibly linked to evading lawful monitoring during a public-order crisis, exercised through an existing legal provision rather than an extra-legal power.

Bitchat's architecture makes this a genuinely hard case: as a server-less, Bluetooth mesh-network app, there is no central server to which a conventional takedown notice can be served, so any blocking action has to target the app-store listing, code repository or device level instead, a blunter tool than blocking a conventional server-based platform. The order followed weeks of protest over the 2026 NEET-UG paper leak, during which authorities suspended mobile internet in a 1.5 km radius of Jantar Mantar and shut 17 metro stations, and Bitchat saw a documented rise in use once conventional connectivity was restricted.

The counter-argument, made by digital-rights groups including the Internet Freedom Foundation, is that Section 79(3)(b) orders lack the review committee safeguard that applies to Section 69A blocking orders, even though this order achieved a functionally similar public-order-based blocking outcome, and that blocking an entire code repository catches the large majority of lawful users along with any bad actors, a proportionality concern that a general capability for misuse does not resolve on its own.

CONCLUSION

The stronger position holds two things at once: a state facing organised evasion of lawful monitoring during civil unrest has a legitimate interest in addressing it, and the procedural route chosen to do so, Section 79(3)(b) rather than the more accountable Section 69A, deserves scrutiny independent of whether blocking Bitchat itself was justified. Defending the underlying authority to act is not the same as defending the specific procedure used to exercise it.

RELATED DAILY ARTICLES

13 Aug **Current Affairs Today, August 13, 2026**

13 Aug **Himachal Pradesh Levies 60 Paise/Litre "Widow and...**

13 Aug **NIA Raids Chennai and Madurai in Andaman Sea...**

12 Aug **Tamil Nadu Assembly Demands Permanent Freeze on Lok...**



CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

[linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)[Read Full Article on Ujiyari →](#)<https://ujiyari.com/editorials/2026/08/ht-bitchat-takedown-state-authority-2026/>

ALSO FROM THE CREATOR

BharatNotes

Free UPSC study platform — subject-wise notes across all 4 GS papers, Prelims MCQs, Mains answer frameworks, PYQ analysis & progress tracking. **100% Free • No Login Required.**

[Start Preparing → bharatnotes.com](https://bharatnotes.com)

🚩 OPPORTUNITY

Advertise with Ujiyari

Reach **thousands of serious UPSC & State PCS aspirants** daily through our PDFs, website, and social channels.

Ideal for: Coaching institutes • EdTech platforms • Book publishers • Exam prep apps

[✉ epicbharat@gmail.com](mailto:epicbharat@gmail.com)

Write to us for rates & media kit

Free UPSC & State PCS Current Affairs · ujiyari.com · bharatnotes.com