



UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

Code as Contraband: When the State Takes Down an Architecture, Not a Post

THE HINDU

27 July 2026 ·

POLITY

SCIENCE & TECH

GS2

GS3

CURATED & WRITTEN BY

**Bharat Choudhary**

UPSC Educator & Content Creator

[in linkedin.com/in/epicbharat](https://www.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](mailto:epicbharat@gmail.com)

Code as Contraband: When the State Takes Down an Architecture, Not a Post

The Hindu

27 July 2026

GS2

GS3



INTERVIEW ANGLE

"If an application is designed so that lawful interception is technically impossible, is publishing that code protected expression or an act of frustrating the law?"

✓ Every fact web-verified against primary sources

THE LIFT LINE

Every takedown until now has been about a message. This one is about a mechanism. Directing GitHub to disable BitChat's repositories, the Indian Cyber Crime Coordination Centre named no unlawful post; it named an architecture that cannot be intercepted. The order therefore asks what Indian intermediary law was never drafted to answer: can the State prohibit a communications tool for what it makes possible, rather than for what has been done with it?

WHY THIS EDITORIAL MATTERS FOR YOUR EXAM

This is a constitutional law problem wearing a technology costume, and it is the kind of question examiners now favour because it cannot be answered from either discipline alone. GS2 supplies the source of executive power, the difference between a [statutory](#) safeguard and an administrative shortcut, and the standard of judicial review applied to digital restrictions. GS3 supplies the grounding on encryption, mesh networking and lawful interception that makes the legal argument concrete rather than abstract.

It also teaches a transferable idea. Most regulation assumes a [chokepoint](#): a licensee, a platform, an office with a compliance officer in it. Decentralised systems remove the chokepoint by design. When that happens, the State's instinct is to regulate the next thing upstream, which here is the code itself. Whether that instinct is constitutional is the question of the decade for technology law, and it will recur with virtual private networks, peer-to-peer payments and open-weight artificial intelligence models.

GS Paper 2: government policies and interventions and issues arising out of their design and implementation; separation of powers between various organs; transparency and accountability in governance; statutory and executive bodies.

GS Paper 3: basics of cyber security; developments in science and technology; challenges to internal security through communication networks; role of media and social networking sites in internal security challenges.

For **Prelims**, hold these precisely: the distinction between **Section 69A** of the **Information Technology Act, 2000** (an express blocking power, operationalised by the **Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009**) and **Section 79** (conditional safe harbour for intermediaries); **Rule 3(1)(d)** and the traceability requirement in **Rule 4(2)** of the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**; the **Indian Cyber Crime Coordination Centre (I4C)** under the Ministry of Home Affairs; and the **Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017**, later superseded by the **Telecommunications (Temporary Suspension of Services) Rules, 2024**. For **Mains**, argue how the proportionality doctrine should apply when the object of regulation is an architecture rather than a message.

BACKGROUND AND CONTEXT

On **23 July 2026**, the **Indian Cyber Crime Coordination Centre (I4C)**, under the **Ministry of Home Affairs**, directed **GitHub** to remove repositories hosting **BitChat**, the Bluetooth mesh messaging application built by **X co-founder Jack Dorsey**. The stated ground was that the application could be exploited to coordinate unlawful assemblies and to **circumvent** lawful restrictions imposed by competent authorities in situations involving public order. The context matters: repeated internet shutdowns near protest sites had already pushed protesters towards Bluetooth-enabled messaging platforms, and BitChat was the most capable of them.

BitChat is a decentralised peer-to-peer messaging application running over **Bluetooth mesh networks**. It needs no internet connection, no servers and no phone numbers. Each device acts as both client and server, automatically discovering peers and relaying messages across multiple hops to extend reach beyond the range of any single link. Its claimed properties are censorship resistance, surveillance resistance and infrastructure independence, and it remains functional during internet outages, natural disasters, protests and in low-connectivity regions. Those are the same properties that make it valuable in a flood-hit district and inconvenient during a riot, which is precisely why the case is hard.

PARAMETER	SECTION 69A, IT ACT, 2000	SECTION 79(3)(B), IT ACT, 2000
Nature of provision	An express statutory power to block	A condition attached to safe harbour
Consequence of invocation	Access to the information is disabled by direction	The intermediary loses immunity if it fails to act
Procedure prescribed	Blocking Rules, 2009: committee scrutiny, opportunity of hearing, reasons in writing, review	None prescribed by statute or rule
Trigger	Government direction on enumerated grounds	Court order, or notification by the appropriate government or its agency
Grounds	Sovereignty and integrity, defence, security of the State, friendly relations, public order, incitement to a cognizable offence	Material being used to commit an unlawful act
Judicial treatment	Upheld in <i>Shreya Singhal</i> (2015) because of its safeguards	Read down in <i>Shreya Singhal</i> (2015) to require a court order or government notification

THE CORE ARGUMENT / ISSUE

What the order actually says

Notice No. 11072601011432, issued at **11.16 p.m. on 23 July 2026** under **Section 79(3)(b)** read with **Rule 3(1)(d)** of the 2021 Intermediary Guidelines, requires GitHub to disable access to **three repositories**, including the Android application and its release files, **within three hours** and “without vitiating evidence in any manner”, warning that failure to comply could invite criminal prosecution.

The recorded reasoning is architectural, not content-based. The order states that the application enables anonymous communication without mandatory user registration, phone number verification or centralised logging; that its technical architecture significantly impedes lawful interception, attribution and investigation; and that because communications occur directly between nearby devices through a decentralised mesh, the platform can be misused to evade lawful surveillance, facilitate anonymous coordination and circumvent lawful restrictions during public order situations, riots, terrorism, organised crime or internet shutdowns. Such platforms, it says, “are capable of being exploited for coordinating unlawful assemblies, violent protests, dissemination of misinformation, radicalisation, criminal conspiracies, and other activities prejudicial to the sovereignty and integrity of India, defence of India, security of the State, public order, and for facilitating the commission of cognizable offences.”

Note the verb tense running through that passage. It is the language of capability, not of commission. Nothing in the order identifies a particular unlawful communication that passed over BitChat, which is what makes the legal question sharp rather than academic.

The State's case, at its strongest

The government's position deserves to be stated at full strength before it is tested. Lawful interception is not an incidental power; it is the operational spine of criminal investigation, and Parliament has built it into successive statutes precisely because a democratic State polices by warrant rather than by force. A mesh network that routes around the internet also routes around every one of those powers at once. Where communication is engineered so that no intermediary exists on which to serve a warrant, investigative capacity does not degrade gradually; it collapses to zero, and it does so for terrorism and organised crime exactly as it does for peaceful assembly.

There is a second, subtler point in the State's favour. Constitutional adjudication has traditionally distinguished between speech and the instrumentalities of speech, and has accepted that instrumentalities can be regulated (licensing of broadcasting spectrum, registration of printing presses) without that regulation being censorship. On this view, requiring that a mass communication channel remain warrant-accessible is a neutral condition of operation, not a restriction on any message. If that reasoning holds, the State is not censoring at all; it is declining to let a distribution point for warrant-proof capability sit unregulated on a platform within its jurisdiction.

The legal difficulty, which is the heart of the matter

The difficulty is not with the aim but with the instrument. **Section 79 does not itself confer a blocking power.** Section 79(3)(b) provides only that an intermediary may **lose** its safe harbour if, upon receiving actual knowledge or on being notified by the appropriate government or its agency that material residing on its computer resource is being used to commit an unlawful act, it fails to expeditiously remove or disable access to that material without vitiating evidence. It is a liability provision addressed to the intermediary's immunity, not a command power addressed to content.

Blocking directions are ordinarily issued under **Section 69A** and the **Blocking Rules, 2009**, which require a committee to examine the request, an opportunity of hearing to the originator or intermediary, reasons recorded in writing and periodic review. A safe harbour provision is thus being used to secure a blocking outcome while bypassing the procedure that Parliament and the rule-maker attached to blocking. The safeguards are not incidental to Section 69A; they are the reason it survived constitutional challenge.

Shreya Singhal v. Union of India (24 March 2015) is directly on point. The Supreme Court read down Section 79(3)(b) so that "actual knowledge" arises only upon a court order or upon notification by the appropriate government or its agency, precisely to prevent intermediaries becoming private censors on unstructured executive request. In the same judgment it upheld Section 69A because that provision comes wrapped in procedure. Section 69A is the door with safeguards; Section 79(3)(b) is the door without them. The constitutional objection is that the State has chosen the second door for a task the first was built for.

There is also a structural mismatch worth noticing. **Rule 4(2)** of the 2021 Rules requires a significant social media intermediary providing messaging services to enable identification of the first originator of information. BitChat has no intermediary, no account and no originator record to surrender. A rule designed for platforms

has no purchase on a protocol, which is a sign that the regulatory framework has run past the end of its own architecture.

The civil liberties case, at its strongest

The **Internet Freedom Foundation (IFF)** argues that the order relies on the application's potential for misuse rather than identifying any unlawful content in the repositories. Its formulation is the sharpest in the debate: "Anticipated misuse of a communications tool is not a lawful basis to prohibit the tool." Accept that principle and almost every general-purpose technology is safe from prohibition; reject it and almost none is, because encryption, cameras, vehicles and cash are all capable of misuse.

The IFF further contends that a notice issued close to midnight with a three-hour compliance window fails the proportionality standard laid down in **Anuradha Bhasin v. Union of India (10 January 2020)**, where the Supreme Court held that "the degree of restriction and the scope of the same, both territorially and temporally, must stand in relation to what is actually necessary to combat an emergent situation", and that tailoring must account for the territorial extent, the stage of the emergency, the nature of the urgency, the duration and the nature of the restriction. Read alongside the four-limb test in **K.S. Puttaswamy v. Union of India (2017)**, that is, legitimate aim, rational **nexus**, least restrictive means and balancing, the third limb is where the order is most exposed: targeted investigation of identified offenders, device-level forensics and prosecution of actual unlawful assembly all remain available.

Two further objections follow. The first is futility. BitChat is open source and mirrored across repositories worldwide; deleting three of them subtracts convenience, not capability, and a measure that restricts rights without achieving its aim cannot satisfy the least restrictive means test by definition. The second is precedent. If publication of source code can be disabled on an assessment of what the code makes possible, the same reasoning reaches compilers, cryptographic libraries and open-weight artificial intelligence models, none of which the executive has said it intends to touch, and all of which would be within reach of the principle.

The shutdown backdrop

The reason BitChat exists in Indian protest settings at all is that internet suspensions happen. **Anuradha Bhasin** held that expression and trade over the internet are constitutionally protected, that suspension orders must be published and reasoned, that indefinite suspension is impermissible and that orders must be periodically reviewed. The **Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017**, framed under the Indian Telegraph Act, 1885, and the successor rules made under the Telecommunications Act, 2023, supply the procedural discipline. Where that discipline is observed, the demand for shutdown-proof messaging falls. Prohibiting the response while leaving the practice untouched treats the symptom as the disease.

HOW TO THINK ABOUT THIS (ANALYTICAL FRAME)

Use the **Four Layer Test** for any technology restriction, and apply the layers in order rather than jumping to the merits.

Layer 1, Source of power. Is the provision invoked actually a power, or merely a condition of immunity? A liability rule cannot be converted into a command power by usage.

Layer 2, Object of the restriction. Is the State targeting identified unlawful content, an identified person, or an architecture? Content and conduct are regulable on established principles; architecture regulation is presumptively over-broad because it reaches every future lawful use along with the unlawful ones.

Layer 3, Procedure. Was a safeguarded statutory route available and bypassed? If it was, the burden shifts heavily onto the State to explain the choice, since procedure is what made the safeguarded route constitutional in the first place.

Layer 4, Efficacy. Will the measure achieve the aim, given that code replicates freely across jurisdictions? A restriction that is simultaneously rights-restricting and ineffective cannot clear the least restrictive means limb of Puttaswamy, because a measure that does not work cannot be the least restrictive means of achieving anything.

The frame transfers directly to virtual private networks, end-to-end encryption mandates, cryptocurrency protocols and open-weight artificial intelligence models. In each case, ask which layer the government's case actually rests on, and you will usually find it resting on Layer 4 assertions that Layer 1 does not support.

THE DIAGRAM IN WORDS

Picture two pipelines carrying the same message between the same two citizens. The upper pipeline runs through a telecom licensee and then a platform, each with an Indian presence, a compliance officer, a grievance officer and a licence to lose, so the State can lawfully tap it at either joint, and both joints are drawn as valves the law already knows how to turn. The lower pipeline is not a pipeline at all but a scatter of handsets hopping Bluetooth signals hand to hand across a crowd, each phone relaying for the next, with no valve, no office and no joint anywhere on which a warrant can bite. Because the State cannot reach the lower pipeline directly, the takedown order reaches across from the upper one, where it does have **leverage** over GitHub as an intermediary, and erases the drawing from which anyone could build the lower pipeline again. Around both sits the constitutional envelope: Article 19(1)(a) and Article 21 pressing outward on one side, Article 19(2) reasonable restrictions pressing inward on the other, with the Puttaswamy proportionality ladder drawn as the only lawful bridge between them, and the Section 69A procedure drawn as the only staircase up that bridge.

WAY FORWARD

- ❶ **Route architecture-level action through Section 69A.** If the State genuinely believes an application must be restricted, the direction should travel through the provision that carries committee scrutiny, an opportunity of hearing and reasons in writing, not through the safe harbour clause the Supreme Court has already read down.

- ② **Set a statutory standard for code takedowns.** Amend the IT Rules to require a judicial order before source code repositories are disabled, with notice to the developer and an opportunity to be heard, so that publishing software is not silently equated with committing an offence.
- ③ **Publish orders and aggregate transparency data.** Extend the Anuradha Bhasin publication principle to Section 79(3)(b) notices, with periodic reporting by I4C on the volume of notices, the grounds invoked, compliance rates and outcomes, so that the practice can be studied rather than inferred from leaked notices.
- ④ **Discipline shutdowns to reduce demand for shutdown-proof tools.** Strict compliance with the suspension rules, including publication, reasoned orders, duration limits and review committee scrutiny, removes the very conditions that make mesh messaging attractive to ordinary protesters.
- ⑤ **Invest in lawful capability rather than prohibition.** Strengthen metadata analysis, device-level forensics, digital evidence handling and trained cyber investigation capacity within I4C and State police, all of which survive encryption, instead of pursuing bans that do not.
- ⑥ **Create independent oversight for digital orders.** A statutory appellate authority outside the issuing executive, with the power to review blocking and takedown directions, would close the accountability gap that this episode and the litigation around intermediary obligations have both exposed.

PYQ LINKAGE AND PRACTICE

UPSC has repeatedly asked on the right to privacy as a fundamental right and its implications for governance, on the challenges that social media and encrypted messaging pose to internal security, and on the role of digital platforms in mobilisation and public order. It has also asked on the tension between security imperatives and civil liberties, which is the spine of this editorial. The distinctive value here is that the answer can turn on a precise statutory distinction between two sections of the same Act, which is the sort of specificity that separates a good answer from a general one.

Practice question: “The regulation of communication architecture, as distinct from communication content, tests the limits of proportionality in Indian constitutional law.” Examine with reference to the Information Technology Act, 2000 and contemporary takedown practice. (250 words, 15 marks)

Interview angle: If an application is designed so that lawful interception is technically impossible, is publishing that code protected expression or an act of frustrating the law?

Sources: The Hindu, PIB, Internet Freedom Foundation

Source: Code as Contraband: When the State Takes Down an Architecture, Not a Post — [Ujjayi.com](https://ujjayi.com) | Free UPSC & State PCS Editorial Analysis

RELATED DAILY ARTICLES

27 Jul **Current Affairs Today, July 27, 2026**

27 Jul **Public Examinations Amendment Bill, 2026: Ten Years in...**

27 Jul **NTA Overhaul and a Minister's Exit: The Nilekani Task...**

27 Jul **Supreme Court (Number of Judges) Amendment Bill, 2026:...**



CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

[in linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)[Read Full Article on Ujiyari →](#)<https://ujiyari.com/editorials/2026/07/th-bitchat-takedown-it-act-encryption-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](#)

📌 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