

Disabling BitChat in India? | Explained

The notice was issued close to midnight on July 23

Updated - July 24, 2026 06:56 pm IST

RIZMI LIA M.

A large, bold, white sans-serif font spelling out the letters 'B', 'I', and 'T' in sequence, centered against a solid black rectangular background.

The government order states that since communications on BitChat occur directly between nearby devices through a decentralised mesh network, the platform can be misused to evade lawful surveillance, facilitate anonymous coordination and circumvent lawful restrictions imposed by competent authorities during situations involving public order, riots, terrorism, organised crime or internet shutdowns. Photo: <https://upload.wikimedia.org/>

The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, directed GitHub on July 23, 2026, to remove repositories hosting BitChat, the Bluetooth mesh messaging application developed by X (formerly Twitter) co-founder Jack Dorsey, stating that the app could be exploited to coordinate unlawful assemblies and circumvent

lawful restrictions imposed by competent authorities during situations involving public order.

The order comes at a time when repeated internet shutdowns near protest sites have led protesters to increasingly rely on Bluetooth-enabled messaging platforms such as BitChat for communication.

What is BitChat?

BitChat is a decentralised peer-to-peer messaging application that operates over Bluetooth mesh networks. It requires no internet connection, no servers and no phone numbers.

Traditional messaging apps depend on centralised infrastructure that can be monitored, censored or disabled. BitChat creates ad hoc communication networks using only devices in physical proximity, with each device acting as both a client and a server, automatically discovering peers and relaying messages across multiple hops to extend the network's reach.

According to the platform, this approach provides censorship resistance, surveillance resistance and infrastructure independence. The network remains functional during internet outages, natural disasters, protests or in regions with limited connectivity.

What does the order say?

The order directs GitHub to disable access to three repositories, including the Android application and its release files, within three hours. It also warns that failure to comply could invite criminal prosecution.

According to the order, the application enables anonymous communication without mandatory user registration, phone number verification or centralised logging of communications. It states that the application's technical architecture significantly impedes lawful interception, attribution and investigation by law enforcement agencies.

It further states that since communications occur directly between nearby devices through a decentralised mesh network, the platform can be misused to evade lawful surveillance, facilitate anonymous coordination and circumvent lawful restrictions

imposed by competent authorities during situations involving public order, riots, terrorism, organised crime or internet shutdowns.

The order also states that “such decentralised communication platforms 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.”

What does the law say?

The order, Notice No. 11072601011432, was issued at 11.16 p.m. on July 23, 2026, under Section 79(3)(b) of the Information Technology Act, 2000, read with Rule 3(1)(d) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Section 79(3)(b) provides that an intermediary may lose its safe harbour protection if, upon receiving actual knowledge or being notified by the appropriate government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit an unlawful act, it fails to expeditiously remove or disable access to that material without vitiating the evidence in any manner.

However, Section 79 itself does not confer a blocking power. Blocking directions are ordinarily issued under Section 69A of the IT Act and the Blocking Rules, 2009, which require a hearing and reasons recorded in writing, subject to review. It empowers the Central Government to direct the blocking of public access to information on grounds such as national security, public order and the prevention of incitement to the commission of cognisable offences. Such orders are required to follow the procedure prescribed under the law.

The Supreme Court’s judgment in *Shreya Singhal v. Union of India* (2015) is a landmark ruling on digital free speech in India. The Court read down Section 79(3)(b), clarifying that intermediaries are obligated to remove content only when directed by a court or a government authority acting under due process. This interpretation protected platforms from being compelled to comply with informal or arbitrary takedown notices.

The Court also held that speech on the internet enjoys the same constitutional protection as offline speech. It emphasised that vague laws have a chilling effect on free speech and violate Article 19(1)(a) of the Constitution unless they satisfy the test of reasonable restrictions under Article 19(2).

The Internet Freedom Foundation (IFF) criticised the order, arguing that it relies on the application's potential for misuse rather than identifying any unlawful content hosted in the repositories. "Anticipated misuse of a communications tool is not a lawful basis to prohibit the tool," the organisation said.

The order directs GitHub to "remove and disable access to the concerned URLs within three hours of the issue of this communication without vitiating evidence in any manner." According to IFF, the notice, issued close to midnight, fails the proportionality standard laid down by the Supreme Court in *Anuradha Bhasin v. Union of India* (2020).

In *Anuradha Bhasin*, 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." The Court observed that the principle of proportionality requires restrictions to be tailored to the territorial extent of the restriction, the stage of the emergency, the nature of the urgency, the duration of the restrictive measure and the nature of the restriction.

Published - July 24, 2026 06:16 pm IST