THE CENTRE FOR internet & society

A Guide to Navigating Your Digital Rights:

A primer

By Anamika Kundu, Radhika, Shruti Trikanad, Torsha Sarkar, in alphabetical order

Edited by Cheshta Arora and Pallavi Bedi

DESIGN
Aparna Chivukula

This work was supported by a research grant from the East-West Management Institute (EWMI). All errors remain the authors' own.

A GUIDE TO NAVIGATING YOUR DIGITAL RIGHTS:

A primer

By Anamika Kundu, Radhika, Shruti Trikanad, Torsha Sarkar, in alphabetical order

Edited by Cheshta Arora and Pallavi Bedi

THE CENTRE FOR internet & society

Contents

CONTENT TAKEDOWN **4**

Content takedown under Indian law 4

Information Technology Act, 2000 4

Criminal legislations 8

For content creators: The Right to Information Act and content takedown 9

Barriers to access 10

Potential routes for informational access 12

Resources for further research 12

SURVEILLANCE **16**

Surveillance laws 16

Information Technology Act and Telegraph Act 16

Surveillance framework and Review Committee 16

Unlawful Activities Prevention Act, 1967 ('UAPA') 17

The Right to Privacy 18

Preventive measures 18

Remedies 19

Appropriate Forums 19

In case your RTI application is rejected 20

DEVICE SEIZURES **21**

Code of Criminal Procedure 21

Procedural safeguards to remember 22

Right to privacy and the Data Protection Bill, 2021 24

Right against self-incrimination 25

Person accused of any offence 25

Compelled to be a witness against himself 25

In practice: Virendra Khanna v State of Karnataka 27

INTERNET SHUTDOWNS **30**

Section 144, Code of Criminal Procedure 30

Telegraph Act and Telecom Services Rules 31

How internet shutdowns work 32

Tools to circumvent internet shutdowns 33

Things to remember 34

Legal Tools 35

Right to Information Requests 35

Strategic litigation 37

Content Takedown

Content takedown laws empower the government to request online intermediaries to censor content that violates the local law of the country. This basically means that any website, blog post, or application that is illegal can be blocked by sending a notice to the Telecom Service Provider (Like Airtel and Jio). An example of such a ban is the popular application Tik Tok which was banned under national security concerns. The nature of this content can vary from Tweets, Facebook posts to even user accounts on social media platforms and applications developed by third-party developers.

> **In this context, online Intermediaries means any person who, on behalf of another person, receives, stores or transmits electronic messages, or provides any other service.**
>
> **In practice, this means entities like social media platforms such as X, Facebook, search engines like Google, DuckDuckGo, app stores like app store, internet service providers (ISPs) like Airtel and Jio, online payment sites such as Razorpay, and many others.**
>
> **The legal definition for an intermediary can be found in section 2(w) of the Information Technology (IT) Act, 2000.**

In India, there are a variety of laws that give the government the power to order intermediaries to censor, or 'take down' content. In this guide, we would be discussing these laws, their features, and what civil society, human rights advocates and content creators can do to push for more accountability around government's orders.

Content takedown under Indian law

The issue of content takedown concerns the censorship of speech online, and technically that means, any legal provision that allows the government to prosecute speech, could be used to request intermediaries to remove content. Broadly, therefore, there are two legislative formats that the government can resort to: a) The specialised legislations that empower the government to censor speech online, especially the Information Technology (IT) Act, and b) More general criminal legislations, like the Indian Penal Code (IPC) and the Code of Criminal Procedure (CrPC).

Information Technology Act

The Information Technology (IT) Act, 2000 was enacted to bring India in compliance with the Model Law on Electronic Commerce, which was adopted by the United Nations in 1997. The IT Act is the governing law for a majority of digital transactions, communications and other relevant matters in India.

Section 69A and the Blocking Rules 2009

Section 69A(1) of the IT Act empowers the Central Government to order an intermediary or a government agency to block public access to information that is a threat to:

> *"the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence"*

These reasons are borrowed from Article 19(2) of the Indian Constitution, which prescribes reasonable restrictions to the fundamental right to freedom of speech and expression.

Section 69A(2) states that the procedure and safeguards concerning such blocking processes may be prescribed, following which Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 [aka, "the Blocking Rules"] were issued. Generally, Blocking can be ordered through a general block as well as emergency blocks under Rule 9 of the Blocking rules.

What is the procedure for removing content u/s 69A and the Blocking Rules?

1) Nodal Officer: Ministries and departments of the central government, state governments, union territories and any other government agency as designated by official gazette ["organisations"], are responsible for appointing a Nodal Officer (NO). These organisations **must** publish information about their nodal officers on their websites.

A NO would be eligible to receive a complaint from 'any person' regarding the blocking of access to public information.

2) Designated Officer: An officer of the Central Government, not below the rank of a Joint Secretary, shall be appointed as the Designated Officer (DO).

The DO may receive a request from the NO or a competent court to block access to content. The request from the NO must be in writing, and signed by the NO. The DO **must not** entertain any requests from any person directly.

3) Committee for examination of request: The request and the printed sample of the offending content must be examined by a committee comprising of: a) The DO as the chairperson, b) Representatives from Ministries of Law and Justice, Home Affairs, Information and Broadcasting and Indian Computer Emergency Response Team (none under the rank of Joint Secretary).

4) Examination: The DO **must** make all reasonable efforts to identify the originator of the content or the intermediary who has hosted the content. Once identified, the DO must give a notice to either the person or the intermediary. This notice would invite them to submit their replies/clarifications against the blocking request, within a timeframe of **not less than 48 hours**.

The committee must examine the request + printed copy of the offending information, determine whether it falls within the ambit of section 69A(1) of the IT Act, and give specific recommendations **in writing**.

5) Submission of recommendation: The DO **must** submit the recommendations from the committee to the Secretary of the Department of Technology (DoT).

On approval of the same, the DO can direct either the relevant government agency or the intermediary to block the offending information.

6) Emergency: In emergencies, "*for which no delay is acceptable*", the DO will examine the request and the printed copy of the information themselves, and submit it to the DoT with their specific recommendations **in writing**. The DoT will have the discretion to pass an interim blocking order, after recording their reasons **in writing** and without giving the originator/intermediary an opportunity of hearing.

Within 48 hours of such an interim order, the DO **must** bring the request to be examined by the aforementioned committee. Post the receipt of the committee's recommendations, the DoT will pass its final order.

Important: In case the DoT does not approve of the blocking request, then the interim order **must** be revoked and the person/intermediary in charge of the information **must** be ordered to unblock the information.

7) Competent court: The DO is also eligible to receive blocking orders from a competent court. For such orders, the DO must immediately submit them to the DoT, and proceed according to the court's direction.

8) Review committee: The Review Committee, configured under Rule 419A of the Indian Telegraph (Amendment) Rules, 2007, **must** meet at least once in two months, and review whether the orders passed are in accordance with section 69A(1).

If it is of the opinion that such orders are not in accordance with section 69A(1), then it may set aside the orders, and direct for unblocking of previously blocked information.

9) Confidentiality: Strict confidentiality **must** be maintained regarding all the requests/complaints received, and the action taken on them.

Section 79 and the IT Rules 2021

Section 79(1) of the IT Act provides that notwithstanding anything contained in any laws in force, an intermediary **shall not be liable** for any third-party information made available or hosted by them. An illustration for this can be, if a user uploaded a defamatory statement on Facebook, Facebook will not be liable for the statement uploaded if it complies with provisions of the law.

Section 79(2)(c) provides that the benefits of this immunity would apply only if the intermediary observes due diligence and observes "*such other guidelines as the Central Government may prescribe*". Accordingly, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [aka, "IT Rules 2021"] were issued, which lays down another legal framework for the government to order intermediaries to remove content.

What is the procedure for removing content u/s 79?

1) Scope of illegality: The government may only request an intermediary to remove content that is against:

"the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force"

2) Relevant authorities: A valid takedown request under section 79 and the IT Rules 2021, can only come from either a court order, or an appropriate government or its agency.

3) Actual knowledge: An intermediary would be only liable to remove content when it has actual knowledge of illegal content on its platforms.

An intermediary would be presumed to have actual knowledge of such content, **only** when it has received a valid takedown order that adheres to the scope of illegality and originates from the relevant authorities.

4) Timeframe: Once an intermediary has actual knowledge of illegal content on its platforms, it would be bound to remove such content **no later than thirty-six hours**.

The Copyright Act, 1957 provides creators with remedies for infringement of their work. In the event of an infringement, the copyright owner has a number of options for legal action. Under Section 52(1)(c) of the Act transient or incidental storage of a part of work does not constitute as infringement of copyright. The exception for this is if the intermediary or the party storing this is aware that such copy is infringing material. The section also states that upon receiving written complaint of infringing material, the access must be stopped for a period of 21 days within which the complainant has to obtain a court order otherwise the said content can be unblocked. There are various remedies available under the Act in terms of injunctions, damages etc. TSP's are bound to block access to infringing content post a court order.

Under the recently enacted The Digital Personal Data Protection Act, 2023 under Section 37 of the Act, the Central Government can direct blocking of content through the Data Protection Board.

Criminal legislations

During the General Elections of 2019, a group of social media platforms, along with the industry body Internet and Mobile Association of India (IAMAI) presented a 'Voluntary Code of Ethics', that was to govern information flow during the election period. A channel of communication was to be established with the Election Commission of India (ECI), where the ECI would have the power to send notifications to the platforms, informing them about potential violations of provisions of the Representation of Peoples Act (ROPA), as well as "*other applicable electoral laws*". All notifications were expected to be acted upon within three hours.

It was not imminently clear which legal provisions would empower the ECI to send these takedown notices since, as discussed in the previous section, the power to send such notices, at least under the IT Act, is vested with very specific authorities. We searched through the Lumen Database, maintained by the Berkman Klein Centre for Internet and Society, which archives takedown notices received by online intermediaries.

On our search, we found three notices that were sent by ECI, and that correspond to the timeline of the Code of Ethics. Two of these were sent under section 171G of the IPC, while one was sent under section 505 of the IPC. Both of these notices asked Twitter to censor tweets containing allegations about the manipulation of electronic voting machines (EVM). A sample screenshot of these notices is provided in the later sections.

Section 171G, IPC

What it says: *Whoever with intent to affect the result of an election makes or publishes any statement purporting to be a statement of fact which is false and which he either knows or believes to be false or does not believe to be true, in relation to the personal character or conduct of any candidate shall be punished with fine.*

What it was used for: For censoring ostensible 'misinformation' about EVM manipulations. It is clear that the scope of section 171G is restricted to statements related to the character or conduct of a candidate, and not at large about the electoral process. Additionally, the sanctions attached to section 171G refer to fine, and not content takedown orders.

In such light, it is difficult to rationalise the invocation of section 171G, as done by the ECI.

Section 505, IPC

What it says: *Whoever makes any statement, rumour or report that:*

> *a) incites public officers to mutiny, or*
>
> *b) intends to cause fear or alarm to the public where the person is incited to commit an offence against the state, or*
>
> *c) intends to create or promote enmity on the grounds of religion, race, place of birth, residence, language, caste or community,*
>
> *shall be punished with imprisonment, or fine, or both.*

What it was used for: For censoring ostensible 'misinformation' about EVM manipulations. Arguably, the scope of the censored information would come under the prohibition against any statement, rumour or report that causes fear or alarm to the public.

However, section 505 is a penal provision, which means that the violation of the section would attract punishment (either imprisonment, or fine, or both). This also means that the punishments would be only applicable at the conclusion of a criminal investigation and the court determining the guilt of the accused. Therefore, this section, much like section 171G, is not meant to be used unilaterally, to request intermediaries to remove content.

For content creators: The Right to Information Act and content takedown

The Right to Information (RTI) Act was enacted in 2005, with the objective of ensuring transparency and accountability in a democracy. It empowers citizens to ask for disclosures from public authorities regarding public dealings.

As content creators, or as civil society advocates working towards the freedom of speech and expression, the RTI Act can be an invaluable tool to procure information about content takedown procedures, and to ensure that such takedowns are done in adherence to existing laws and safeguards. The RTI Act allows for individuals to:

a) Inspect of work, documents, records held by the government

b) Take notings, extracts or certified copies of documents or records

c) Take certified samples of materials

d) Obtain information in electronic modes, or through print-outs, for information stored in any computer devices.

Procedure for filing RTIs

As discussed in the previous section, there might be a variety of government agencies that might be involved in overseeing content takedown procedures under different laws. The basic procedure for filing an RTI request is:

a) Every government agency is to have a public information officer (PIO), who would be designated to receive and respond to RTI requests pertaining to that agency. In many cases, States also have their own information commissions, there are certain departments which are exempt from purview of RTI's as well. The first step, therefore, is to identify which government agency may be relevant for a particular instance of content takedown. For instance, in case content has been taken down on the order of the Election Commission of India, then it would be the PIO attached with the ECI, who would be eligible to receive an RTI request regarding this takedown.

b) In the request, write down the information you are seeking from the concerned

government agency. Best practices for an RTI request include being specific and clear about your questions, ensuring that the request is narrowed down to one particular search area, and avoiding vague questions.

c) Applications can be made either online (by visiting www.rtionline.gov.in) or by visiting the nearest PIO.

d) Provide personal details alongside your request, including your email ID, mobile number, and a mailing address for the reply. You must also pay a nominal fee of Rs. 10/- alongside your application.

e) For RTI applications submitted online, you can track the status of your request via the reference number provided at the time of submission.

f) One can also file an appeal against the information received through first appeal which is available on the RTI Portal. In case information is not received within the stipulated time of 30 days, an appeal can be filed.

g) A second appeal can also be filed if the response received through the first appeal is not satisfactory.

Barriers to access

Despite the affordances of the RTI Act, there are numerous barriers to information access that exist, both within the RTI Act, as well as within the content takedown laws discussed above.

Section 8, RTI Act

Section 8(1) of the RTI provides a long list of situations where the PIOs would be exempt from disclosing information. This includes information that could cause a breach of parliamentary privilege, information received in confidence from foreign governments, information available to a person in their fiduciary relationship, and so on.

However, section 8(2) states that notwithstanding these exemptions, a public authority may allow access to information in case the public interest in disclosure outweighs the harm to the protected interests.

This section has been used to refuse information concerning content removals. For instance, in 2018, the Centre for Internet and Society filed an RTI request with Bharat Sanchar Nigam Limited (BSNL), a public company which also operated as an ISP. The request asked for the following:

> *- What are the names and URLs of websites currently blocked by government notification in India?*
>
> *- Please provide copies of blocking orders issued by the Department of Telecommunications, Ministry of Communications and other competent authorities to block such websites.*

BSNL refused to provide this information, citing section 8 of the RTI Act. In particular, they cited two subsections of the provision, which exempt disclosure, in case the:

> *- 8(e): Information is available to a person in his fiduciary relationship, unless the competent authority is satisfied that the larger public interest warrants the disclosure of such information.*
>
> *- 8(g): The disclosure of information would endanger the life or physical safety of any person or identify the source of information or assistance given in confidence for law enforcement or security purposes.*

It is not immediately clear how the information asked for in the request fulfils the conditions of sections 8(e) and 8(g).

In particular, it is worth exploring the exemption claimed under section 8(e). In 2011, the Supreme Court of India, in the case of Central Board of Education v Aditya Bandopadhyay, described a fiduciary relationship [as under section 8(e)] as "*persons who act in a fiduciary capacity, with reference to a specific beneficiary or beneficiaries who are to be expected to be protected or benefited by the actions of the fiduciary*".

This means that a fiduciary relationship exists *only* when there is a beneficiary relationship between two entities: according to the court, the examples are "*a trustee with reference to the beneficiary of the trust, a guardian with reference to a minor, a parent with reference to a child, a lawyer or a chartered accountant with reference to a client*" and so on. In such light, it is difficult to understand what is the nature of the fiduciary relationship that exists between BSNL and (potentially) the users whose websites/URLs have been previously blocked.

Given the importance of the information that was asked for in the above RTI, it could even be argued that disclosure of this information outweighs the potential harms caused to the protected interests.

Either way, the use of section 8 to deny information, in this case, was probably not in adherence to what the law actually says.

Even in the past, section 8 has been misused in other contexts by PIOs to deny information in critical cases.

Rule 16, the Blocking Rules

As we have indicated earlier, Rule 16 of the Blocking Rules mandates that strict confidentiality **must** be maintained around the requests/complaints received and the action taken thereof. This means in case content is removed under section 69A and the Blocking Rules, the specifics of the proceedings leading up to such removal would not be disclosed by the relevant government authorities, owing to Rule 16.

In the past, therefore, government agencies have refused to answer RTI requests, citing Rule 16. For instance, in 2018, the Software Freedom Law Centre (SFLC) filed an RTI request, asking for:

- The number of websites that are currently blocked in India.

- Names and URLs of the websites that are blocked.

- Copies of blocking orders that have been issued by the Ministry of Electronics and Information Technology (MeitY) to block such websites.

MeiTY responded to this request, providing only the number of websites that are currently blocked in India, and denying information on the other two points, citing Rule 16.

For content removals under the IT Act, Rule 16 acts as a substantive hurdle against informational access. Given the opacity that this rule affords, governments seem to route a majority of content removal requests through section 69A, even though section 79 creates another legal framework. This was confirmed in the past during a conversation with a big intermediary in India, who stated that the majority of content removal requests they received, seemed to be routed via section 69A.

Potential routes for informational access

While barriers to access to information exist via the legal provisions in the RTI Act and the Blocking Rules, there are other routes within the legal framework discussed above that would allow for informational access.

Decency and morality: The scope of illegal content under section 69A and section 79 are nearly identical, with one exception — content that is against 'decency and morality' is covered only by section 79. Notably, section 79 does not have a confidentiality rule like section 69A does. This means that information about content that was removed in lieu of the 'decency and morality' clause can be accessed.

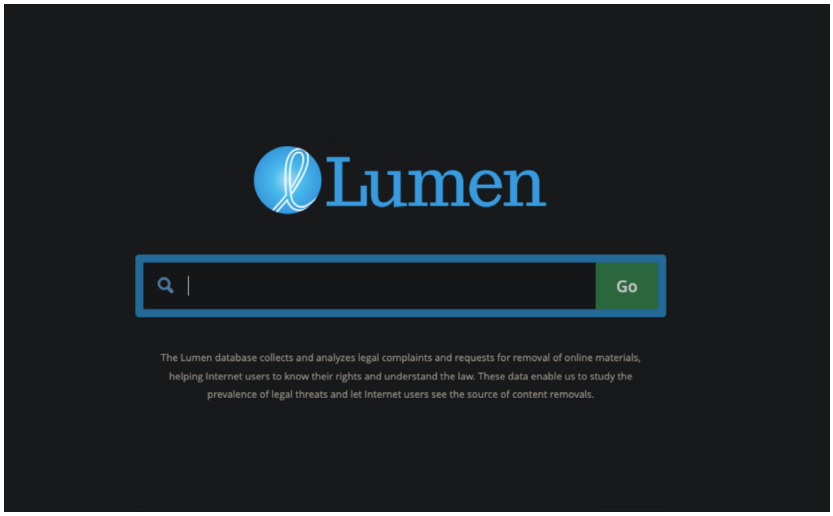
That also means that information on 'porn sites' can be potentially obtained by filing an RTI and asking for all the websites or URLs blocked under section 79. There is some evidence that such a request might succeed: in 2015, a leaked order showed that the government had asked ISPs to block porn sites on the ground that they violated the 'decency and morality' clause.

Criminal legislations: Additionally, not all content removals are routed via section 69A, or even the IT Act. The ECI for instance, have asked intermediaries to remove content under provisions of the IPC. Similarly, different Police Departments around the country have written to the intermediaries under section 91 or section 149 of the Code of Criminal Procedure (CrPC). None of these provisions come coupled with a confidentiality clause, and as such, information around content removed under these provisions should be accessible via RTI requests, including the removal orders, as well as any communications leading up to the removal.

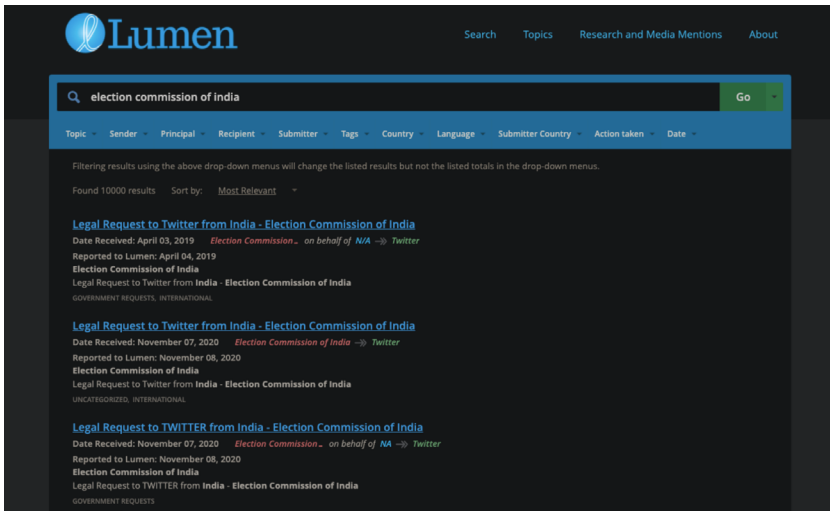
Resources for further research

For content removals, legal barriers to informational access continue to remain. However, civil society advocates and content creators can still resort to certain resources, to ascertain some forms of information around content removal processes in India.

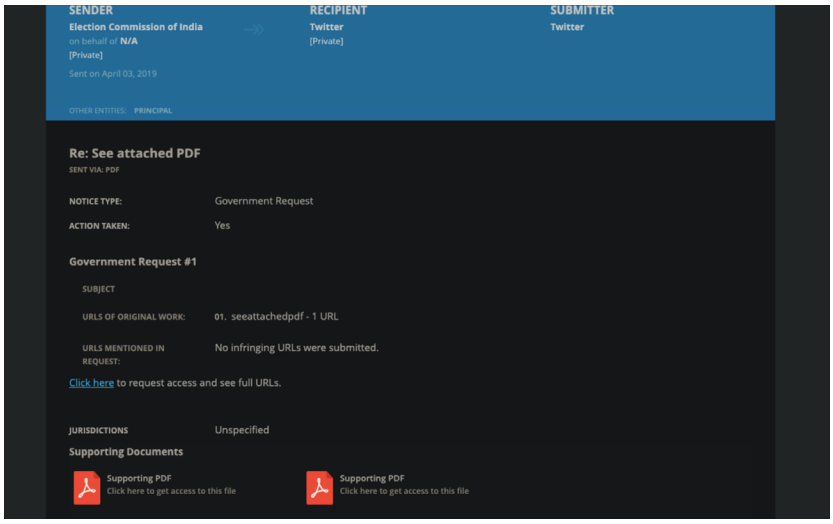
The Lumen database, maintained by the Berkman Klein Centre for Internet and Society, is one such key resource. The database contains takedown requests from governments around the world. These requests are submitted to the database voluntarily by different online intermediaries, provided there is no legal bar against doing so. Accordingly, the Lumen database contains empirical evidence of government removals in India. The home page of the Lumen looks like this:



Searching through this database, with the keyword 'Election Commission of India' for instance, would let you access takedown notices similar to the ones discussed previously.



Clicking on either of these links would direct you to the takedown notices sent by the ECI.



SENDER
Election Commission of India
on behalf of N/A
[Private]
Sent on April 03, 2019

RECIPIENT
Twitter
[Private]

SUBMITTER
Twitter

OTHER ENTITIES: PRINCIPAL

Re: See attached PDF
SENT VIA: PDF

NOTICE TYPE: Government Request
ACTION TAKEN: Yes

Government Request #1

SUBJECT
URLS OF ORIGINAL WORK: 01. seeattachedpdf - 1 URL
URLS MENTIONED IN REQUEST: No infringing URLs were submitted.
Click here to request access and see full URLs.

JURISDICTIONS Unspecified
Supporting Documents
Supporting PDF Click here to get access to this file
Supporting PDF Click here to get access to this file

Two sample screenshots of these takedown notices are shared here:

भारत निर्वाचन आयोग
Election Commission of India

File No. 491/Social Media/2019 Dated: 13 Apr, 2019

To
[redacted]
Grievance Redressal Officer
Twitter
[redacted]

Subject: Request to takedown a specific Tweet on Twitter reg.

Madam,

The Commission finds the Tweet mentioned in the Annexure on Fake news on EVM, highly objectionable and directs Twitter to take down the Tweet at the earliest. The said Tweet violates Section 171G of Indian Penal Code, which deals with false statement in connection with an election. Kindly take necessary action and intimate the Commission, on the status of the action taken, at the earliest.This issues with the approval of the competent authority.

Yours faithfully,

Arun Kumar P
Deputy Director
011-23052056
arunkumar.palani@gov.in

भारत निर्वाचन आयोग
Election Commission of India

File No. 504/Social Media/2019 Dated: 03 Apr, 2019

To
Ms. Payal Kamat
Grievance Redressal Officer
Twitter
(pkamat@twitter.com)

Subject: Take down request to Twitter reg.

Madam,

The Commission finds the Tweet mentioned in the Annexure on "Anything is possible with EVMs", highly objectionable and directs Twitter to take down the Tweet at the earliest. The said Tweet violates Section 505 of Indian Penal Code, which deals with statements conducing to public mischief. Kindly take necessary action and intimate the Commission, on the status of the action taken, at the earliest.This issues with the approval of the competent authority.

Yours faithfully,

Arun Kumar P
Deputy Director
011-23052056
arunkumar.palani@gov.in

These notices provide an invaluable, empirical aspect to research and advocacy around content takedown. This is because, apart from the letter of the law, a lot of practical information around content takedown processes comes from secondary sources, like news reports or anecdotes on social media platforms. As a result, it is not always clear if these documented instances of content removal are done in adherence to the legal framework. Having the original copy of the order in such cases allows for ascertaining the exact procedure via which these content removals are effectuated.

Surveillance

Indian law allows the state to go through a device to access certain information but there is no permission for the state to continuously go through an individual's device. A popular means of surveillance is through Facial Recognition Technology.

Surveillance laws

Information Technology Act and Telegraph Act

The government can carry out interception of messages as per Section 5(2) of the Indian Telegraph Act, 1885 ('Telegraph Act') and Section 69 of the Information Technology Act, 2000 ('IT Act').

Rule 419-A of the Telegraph Rules and the entirety of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ('IT Rules') list out procedures and processes for the parent Acts. As per the Telegraph Act, interception of messages is allowed only on the occurrence of any public emergency or in the interest of public health. The grounds of interception under both the Acts are as follows -

1. the interests of the sovereignty and integrity of India
2. the security of the State
3. friendly relations with foreign States
4. public order
5. preventing incitement to the commission of an offence

Although the grounds of interception are very much the same in both Acts, the IT Act does not have the requirement of public emergency or public safety. Section 69(1) of the IT Act empowers certain officers to pass orders compelling decryption. However, this can be done only after recording reasons for the same and any non-compliance invites possible prosecution. Another recent development that has taken place is the enactment of The Telecommunication Bill, 2023 which replaces the Telecom Act. The new act gives wide powers of surveillance to the Central government.

Surveillance framework and Review Committee

Rule 419-A of the Indian Telegraph Rules notified under the Section 5 of the Indian Telegraph Act, 1885 govern telephone tapping it mentions that -

1. Only a Home Secretary from the central or state government can authorise a wiretap; requests for interception must specify how the information will be used

2. Each order unless cancelled earlier will be valid for 60 days and can be extended to a maximum of 180 days

3. A review committee at the central/state level will validate the legality of the interception order

4. Before an interception order can be approved, all other possibilities of acquiring the information must be considered.

5. The review committee can revoke orders and destroy the data intercepted

6. Records pertaining to an interception order maintained by intelligence agencies will be destroyed every six months unless required for functional purpose

7. Records of an interception maintained by the service provider will be destroyed every two months.

Rule 419A also mentions that a lawful order can be issued only once all other reasonable means for obtaining information have been ruled out. Any such order issued will remain in force for 60 days from the date of issues unless revoked earlier. Although the order can be renewed later if needed, no order can stay in force for more than a total of 180 days.

All lawful orders need to have -

1. Reasons for the order

2. Name and designation of the authority to whom the intercepted information will be disclosed

3. A statement that the use of such information will be subject to Section 5(2) of the Telegraph Act.

A similar provision exists in the IT Rules: Rule 24(1) prohibits any person from intentionally intercepting communications without authorisation. The remedy against unauthorised interception is hindered in India's present surveillance framework as under Rule 25 of IT Rules- service providers are prohibited from disclosing information about governmental requests and orders.

Unlawful Activities Prevention Act, 1967 ('UAPA')

The UAPA allows for information to be collected through an interception as evidence of an offence under the Act. However, such evidence is not admissible unless the accused is given a copy of the order allowing such interception. Section 46 of UAPA talks about admissibility of evidence collected through interception of communications. This section allows for evidence to be gathered through interception of any electronic device or oral communication, this can be used in court. Although it can be admitted only where an accused is provided with a copy of the said interception and the order 10 days prior to the hearing. It can be waived at the discretion of the judge. Thus, unless the interception order was produced through fraud, this clause gives limited safeguard against the use of illegally obtained interceptions as evidence.

The Right to Privacy

The Supreme Court in *Justice K.S. Puttaswamy (Retd.) and Anr. vs Union of India and Others* upheld the right to privacy as a fundamental right under Article 21 of the Constitution. Compelling an individual to give access to their devices, therefore, is a breach of this protection.

For any government action in this regard to be legal, it must be proportionate, have a legitimate aim and have a clear legal basis. Searches have been held to be illegal where they do not fulfil the tests of proportionality and legitimate aim. Any restriction on the right to privacy must satisfy the aforementioned requirements -

1. **Legality**: the existence of clear law and provision

2. **Necessity and purpose**: must have a legitimate aim or purpose and must be necessity i.e. issues of national security, public safety, prevention of crime, and protection of health

3. **Proportionality**: there must exist a rational nexus with the legitimate aim that is to be achieved

4. **Safeguards**: procedural safeguards which are just, fair and reasonable.

The Justice AP Shah Committee report recommended a number of privacy principles for India to follow. These principles should be applied in situations of interception of communications, access to data and audio and video recording. The report emphasised the principles of notice, consent, choice, access and correction to be applied in surveillance technologies.

The enumerated principles are in line with Articles 12 and 17 of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the United Nations General Assembly Resolution on the Right to Privacy in the Digital Age. These international documents are non-enforceable by law. However, due to their customary nature i.e. widely practiced and long standing existence, they can be incorporated into the municipal law framework unless there are clear contradictions between the two systems.

Preventive measures

In case you suspect that your device is under surveillance, the following are a few preventive measures that you can take:

1. **Regular forensic examination**: Anti-spy/anti-virus software from reliable sources can give protection against spyware to some extent in android phones.

2. **Changing devices**: On changing a device, the software downloaded and activated on the device cannot automatically be transferred to another phone even if the sim card remains the same. However, this is not full proof as those undertaking surveillance can quickly figure out that the device has been changed on not receiving data.

3. Suspicious messages: Ensure that you do not click on any suspicious messages as it can lead to downloading of spyware.

4. Keep mobile phones delinked from personal computers: Advanced spyware such as pegasus use zero-click or no-click software which can be activated on a device even without a click. Using Platforms such as Secure Drop for sharing information would provide additional security. Moreover, encrypted platforms ought to be used for any kind of communication as far as possible.

Remedies

Legal Provisions

If you suspect that you have been placed under surveillance illegally, judicial recourse is an effective remedy. Any kind of illegal monitoring method amounts to a violation of provisions of the IT Act assigning liability to those perpetrating the crime.

Section 43

This provision deals with penalties and compensation for damage to the computer/computer system etc. It assigns civil liability to those who cause damage to the computer/computer system and requires compensation for any damages.

Section 66

This provision deals with computer-related offences. If any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both. Section 66 ascribes criminal liability onto the perpetrator of a cybercrime.

Appropriate Forums

This section covers the forum that one can approach to seek a remedy.

Cyber Cells

Every State Police has a cyber cell where one can file a complaint of cybercrimes. First Information Reports ('FIR') can be filed under Section 154 of the CrPC in case one is a victim of cybercrimes such as malicious hacking. While filing an FIR, it is advised to disclose as much information as you are aware of the incident and contact a cyber expert if needed.

Magistrate Courts

In case you cannot file an FIR at a cyber cell, you can file a private complaint at the Magistrate Court as per section Section 156(3) and 190 of the CrPC. This complaint will seek a direction to the appropriate police station to look into the case.

High Courts

If there is an illegal order violating Section 5(2) of the IT Act and Rule 419A of the Telegraph Rules or Section 69 of the IT Act, one can approach the appropriate High Court under Article 226 of the Indian Constitution. This will be to invoke the writ jurisdiction to do away with the illegal surveillance and award damages. The relevant order and its processes should be gathered through RTI applications.

In case your RTI application is rejected

An RTI application can be rejected by citing exemptions as per Section 8 of the Right to Information Act, 2005. Under normal circumstances, the information sought under the RTI Act has to be given within 30 days from the date of the application and 48 hours in case the information sought covers aspects of one's life and liberty. In case your RTI application has not been responded to within the stipulated timeline or the answer is not sufficient, you can raise an appeal to the first appellate authority within 30 days. If the appeal is also unsatisfactory, you can approach either the State or Central Information Commission by filing another appeal called the second appeal. A second appeal can be filed within 90 days of the decision of the first appellate authority in case a reply is not satisfactory. It can also be filed within 45 days in case there is no response that has been received.

Device Seizures

What is the legality of law enforcement agencies demanding you to hand over your personal, electronic devices? What about when the police ask you to unlock your mobile phone, or provide the password to your email account? In this section, we go over the legal rights that you might have under the existing legal position, as well as the procedure and safeguards that law enforcement agencies must adhere to, while dealing with device seizures.

Device seizures happen under multiple laws and legislations in India. There is no clear jurisprudence on the law and its sections getting evoked. As per the latest developments in the legal landscape, the Supreme Court has directed the Center to follow the CBI Manual of 2020 for device seizures. These guidelines have come under the directions issued under Ram Ramaswamy and others V. Union of India.[1] The power to seize devices can come from the following instruments of law:

- The Code of Criminal Procedure, 1973
- The Income Tax Act, 1961
- Unlawful Activities (Prevention) Act, 1967, and
- Prevention of Money Laundering Act, 2002
- CBI Manual of 2020

Different authorities under these instruments of law can be authorised for seizure of devices. In this guide, we will be discussing two main instruments - The Code of Criminal Procedure as well as the CBI Manual of 2020.

Code of Criminal Procedure

The Criminal Procedure Code, 1973 sets out how searches and seizures for criminal investigations can be conducted. The police have powers to search/seize residents' property, including mobile phone and computer devices, both with or without a warrant (although in the latter case, they are required to record reasons in writing for such search).

The following sections have been used by police to apply to the seizure and unlocking of electronic devices:

Section 91, Cr.P.C: Allows the police and magistrates the power to compel any person to produce "*any document or other thing*" that is "*necessary or desirable*" for the purposes of

1 https://thewire.in/government/union-govt-tells-sc-it-will-follow-cbi-manual-on-device-seizure-heres-what-the-manual-says

"*any investigation, inquiry, trial or other proceeding under this Code*." This can extend to a person's mobile phone, if the police think it is "*necessary or desirable*" for the investigation of an offence.

Section 93, Cr.P.C.: Governs the issue of search warrants. Here, the court can issue a search-warrant if (a) it considers that a person will not produce a document / thing as directed under Section 91, Cr.P.C., or; (b) where that document / thing is not known to be in the possession of any person, or; (c) where "the purposes of any inquiry, trial or other proceeding under this Code will be served by a general search or inspection".

Section 94: Confers powers on a magistrate to issue a warrant to authorise the police to search any place suspected to contain stolen property, forged documents, etc.

In a case before the High Court of Karnataka in 2021, the court clarified that that word "place" in Sections 93 and 94 extend to a digital device (in that case, a mobile phone).

Section 100: In the event the place to be searched is closed, the person residing in or in charge of the place is required to allow the officer executing the warrant to enter and search, *on production of such warrant*.

Section 102: Confers powers upon police officers to seize property "alleged or suspected to have been stolen" or "found under circumstances which create suspicion of the commission of any offence", and details the procedure consequent to any such seizures, including mandated reporting to the relevant magistrate. Importantly, this does not require a prior warrant.

Section 165: This section allows the police greater power to conduct searches in the absence of search warrants, when there is a perceived *urgency* in the matter. It confers power upon a police officer, to conduct a warrantless search of a place if he has reasonable grounds for believing that "anything necessary for the purpose of an investigation into any offence" may be found in such a place, which "cannot be otherwise obtained without undue delay". In the exercise of this power, the police officer is required to record in writing the grounds for such belief, and as far as possible, identify the item for which search is to be made.

Procedural safeguards to remember:

Warrants/notice:

1. Under section 91, if the police are requesting the surrender of an item, such as a mobile phone, they are required to serve a formal notice before taking any action. One can refuse to hand over the device unless served with a copy of this notice.

2. The CrPC confers a right on persons to see the search warrant issued under section 93 and 94 before they comply with the police. This is guaranteed by section 100, that governs how a police officer may inspect a "closed" place when in possession of a warrant. If a person in charge of the closed place, or in this case the owner of the device that is sought to be seized, does not comply with the warrant they may be

faced with criminal charges for non-compliance,[2] and the police officer is permitted to break into the space.[3] In case of compliance however, the search must be done in the presence of the person/owner, along with witnesses from the local community, and a list of things found in the place/device signed by the witnesses has to be given to the owner. They cannot be denied presence during the search.

3. Section 165 allows warrantless searches in case there is urgency in conducting the investigation, such that a warrant cannot be obtained in time. The absence of any conditions on the exercise of this power was recognised by the Supreme Court as potentially arbitrary;[4] To address this, it was made necessary for the police to record reasons for needing such an urgent search, in the absence of which the search could be challenged for illegality. Persons who are subject to such a search should demand to see a record of reasons, and could challenge its legality if the police officer in question fails to show them.

Interrogation:

1. While the application of the CrPC to the seizing or forfeiting of devices has become clear, its application to the unlocking of phones is less clear. Commonly, the police demand passcodes during interrogation. A person being interrogated can be one of the following:

a) **An accused/arrested person**: Section 54A governs the identification of arrested persons. This section requires the person to be subject to identification, in any manner the court seems fit. Section 311A allows the court to order accused persons to give specimen signatures or handwriting.[5] The police have relied on these sections to demand the disclosure of passwords for unlocking devices.[6]

b) **A witness**: Section 161 requires that all witnesses examined by police to answer "truly" any questions put by the police, except those "*which would have a tendency*" to expose the person to "*a criminal charge or to a penalty or forfeiture*".[7] This is the protection against self-incrimination guaranteed by

2 Under section 187 of the Indian Penal Code, 1860

3 In accordance with section 47(2) of the Criminal Procedure Code, which deals with search of place entered by an accused person.

4 *State of Rajasthan v. Rehman* [1960 (1) SCR 1991]

5 In *Ritesh Sinha v. State of Uttar Pradesh (2019)* 8 SCC 1, the Supreme Court of India held that the Magistrate could order the collection of voice sample under Section 311-A. It was claimed that since the disclosure of password is akin to giving specimen signature, disclosure can be ordered under this provision.

6 See *Virendra Khanna v State of Karnataka, 2021.* The defense claimed the police relied on these sections while demanding that the petitioner disclose the password to unlock his phone.]

7 Section 161(2), Criminal Procedure Code

the Indian constitution (please see more on this below). It is important to note that the police can question a witness only after sending a notice to them (or an "order by writing")[8] and they cannot issue inducements or threats to force the compliance of the witness.[9] Thus, a person has a legal basis to refuse to answer questions about the phone if this requirement is met.

The following ingredients should be a part of the seizure protocol which should be requested as part of seizure protocol:

- Date and time of seizure
- Location of seizure
- Description of seized devices (make, model, serial number)
- Names of witnesses present during the seizure
- Reason for seizure

These can be the safeguards that can be used for inquiries:

1. Inventory request - Detailed list of all seized items including chargers, sim cards.
2. Reasons for seizure - Laws and provisions under which devices were seized.
3. Access to legal representation
4. Basics of the order such as validity check of the warrant, seizure duration etc.

Right to privacy and the Digital Data Protection Act, 2023

Meta-data exists with third parties either through the apps we use or service providers. This data can be useful for the State but also for unwanted advertising etc. Personal data that remains with service providers can be easily accessed by law enforcement authorities. In order to protect an individual's right to privacy, there is a need to control unauthorised surveillance. The current legislative framework consists of two rules and rules which do not provide for adequate protection.

The Aadhaar judgement held that "under the garb of prevention of money laundering or black money, there cannot be such a sweeping provision which targets every resident of the country as a suspicious person". Although this statement was made in the context of linking Aadhaar with bank accounts, it can be extended to random checking of mobile phones.

The Digital Data Protection Act, 2023 does not have proper safeguards against device seizures

8 Section 160(1), Criminal Procedure Code

9 Section 163, Criminal Procedure Code

per se. Section 17 of the new act gives wide exemptions to the government in respect to personal data of the citizens. Obligations of data retention, and right to erasure are not applicable to the Central Government. Moreover, the Central Government can exempt any data fiduciaries for 5 years.

The act also amends the Right to Information Act, 2005 through section 8 where personal data of any citizen cannot be provided.

Right against self-incrimination

The right against self-incrimination is a constitutional guarantee, codified in Article 20(3) of the Indian Constitution. The right reads as:

> *"No person accused of any offence shall be compelled to be a witness against himself."*

In essence this means that in a criminal proceeding, you may not be compelled to be a witness against yourself, or say/do/provide things that might incriminate you.

There are several elements within protection of Article 20(3) that are worth unpacking. Given the sparse wording of the clause, the scope of its protection has not always been clear. Nevertheless, Article 20(3) is an important consideration during criminal proceedings, and would be accordingly relevant in an instance of device seizures, and especially in situations involving compelled production of passwords.

Person accused of any offence

This is the first element that must be fulfilled for the protection of Article 20(3) to trigger. The Supreme Court, in the case of MP Sharma v Satish Chandra, have interpreted this phrase to mean that the protection of Article 20(3) would be only extended to a person against whom a "formal accusation relating to the commission of an offence has been levelled which in the normal course may result in prosecution." This means that only in situations where a formal law enforcement document (like a FIR) names the person as an accused, would Article 20(3) come into play.

Compelled to be a witness against himself

This is a complex phrase that has gone through several constitutional interpretations over nearly sixty years of constitutional jurisprudence. What does it mean to be a witness? What sort of information can an individual provide that would make them a witness, and accordingly, what sort of information would the witness be not entitled to provide in lieu of the protection of Article 20(3)?

State of Bombay v Kathi Kalu Oghad

In 1961, an eleven-judge bench of the Supreme Court of India delivered its judgement in State of Bombay v Kathi Kalu Oghad. This judgement concerns the most definitive interpretation

of the phrase "*to be a witness against himself*". In *Kathi Kalu*, the majority held that to be a witness meant to communicate **personal knowledge** of a relevant fact. An individual would be only called to be a witness against themselves in the context of information, or a fact that can be changed, or altered. This meant that if the individual is compelled to provide information that cannot be changed, like their fingerprints, handwriting samples, or blood samples, then that would not make them a witness against themselves, and therefore such information would not be violative of Article 20(3)'s protection.

A concurrent and partially dissenting opinion in *Kathi Kalu* differed slightly from the majority opinion, in that it did not agree that to be a witness is to impart *personal knowledge* of a relevant fact. Rather, to be a witness is to provide evidence, and that even fingerprints or blood samples would be providing evidence. *However*, even assuming that an individual made to provide their fingerprints, or blood samples was made to be a witness, it did not mean that they were being made to be a witness '*against themselves*'. This is because the fingerprint, or the blood sample was not in itself incriminating the individual. Rather, it becomes incriminating only when such information is successfully matched with another piece of evidence. Therefore, providing such information in itself, was not self-incriminatory.

The crux of this judgement, in the context of criminal proceedings, is this: the police can compel you to give information that: a) relates to your immutable characteristics, and, b) needs comparison with other pieces of evidence to be of value. This means, fingerprints, blood samples, handwritings etc., are well within the rights of the law enforcement agencies to demand out of you, and Article 20(3) would not protect these.

Selvi v State of Karnataka

In 2010, in Selvi v State of Karnataka, the Supreme Court was called to re-examine the meaning of Article 20(3), and decide on the constitutional validity of interrogation tools like narco-analysis test and polygraph.

While *Kathi Kalu Oghad* continued to be the controlling precedent, *Selvi* iterated and expanded on the logic of the previous judgement in the following way: a) it distinguished personal testimony (personal knowledge of a relevant fact) from material evidence (physical, immutable evidence), b) it found that Article 20(3) can be invoked when an individual's testimony would lead to incrimination by themselves, or "*furnish a link in the chain of evidence*". This would mean that there is a difference between a situation where the response is used for comparison to facts already known **(allowed within the prohibition of Article 20(3))**, and a situation where the response is used to discover new facts **(not allowed within the prohibition of Article 20(3))**.

Is the production of passwords being a witness against oneself? There are two ways of thinking about this, since passwords can be largely divided into two types: a) numeric, or textual passwords, like a passcode and b) biometric passwords, which involve fingerprints, or facial recognition technologies.

Numeric/textual passwords

A numeric or textual password can be distinguished from fingerprints, blood samples or any other 'immutable' characteristics of an individual. By the majority's own logic in *Kathi Kalu*, a numeric or textual password actually relates to 'personal knowledge' of the individual, since unlike their fingerprint, a password is not immutable, and can be an alterable fact.

Further, provision of a password is also an incriminating act in itself, since it is not comparable to facts already known. The police might independently obtain fingerprints from a crime scene, and then ask an accused to provide their fingerprints, to match them to the already-obtained prints. However, the whole point of a password is that it is information that is within the personal knowledge of the individual; the police does not, in fact, already know the password. Provision of passwords in such a case would be, as *Selvi* pointed out, would be provision of a '*link in the chain of evidence*', and therefore, not allowed under Article 20(3).

Finally, on the same logic, a fingerprint is taken from an individual to match against another set of fingerprints. There is a specific purpose, or rather, a specific piece of evidence against which the information from the individual is meant to be compared with. However, a password would open up the entire device for investigation, allowing the police to have a look through all the records of the individual. This would be violative of Article 20(3). Alternatively, in situations where the police have a strong reason to believe that the device has incriminating evidence, the bar against self-incrimination would be nevertheless fulfilled, if the individual is made to give the passcode to their device.

Biometric passwords

For many of the reasons as for textual passwords, production of biometric passwords would be similarly self-incriminatory.

Even beyond that, there is a need to distinguish between fingerprints or facial biometrics provided to unlock a device, and fingerprints obtained to match against prints independently obtained. In the former case, the response is used to discover new facts, while in the latter case, the response is used to compare against already known facts. And as per *Selvi* only the latter would be permitted within the prohibition of Article 20(3).

Additionally, *Selvi* also found that personal testimony did not necessarily mean only oral or written statements, and would include personal knowledge conveyed through other means and communicative gestures. Therefore, even biometric passwords for personal devices could be brought within the ambit of personal testimony, and production of such information would be outlawed by Article 20(3).

In practice: *Virendra Khanna v State of Karnataka*

In 2021, the Karnataka High Court delivered its judgement in *Virendra Khanna v State of Karnataka*, which put the issues enumerated in the previous sections above in practice. The case called for the High Court to decide on the validity of a trial court order that had asked the petitioner to provide passwords to their smartphone and email account to the

investigative agency. There are intersections of the issues enumerated in the previous sections, including the right against self-incrimination and right to privacy.

Right against self-incrimination

The High Court held that compelling an individual to produce the password for their mobile phone and for their email account would *not* be self-incriminating, and therefore, would not be violative of the protection of Article 20(3). The court found that such passwords were not, in fact, a personal testimony, but 'physical evidence', akin to fingerprints, blood samples or handwriting samples. Accordingly, the mere production of a password would not be testimonial compulsion, and would be allowed.

However, as discussed in the previous sections, this does not seem to be the correct interpretation of the judgments that came before this decision. As has been argued by other notable commentators, a mobile password is simply not physical evidence, nor is it obtained only for the purpose of comparison with other existing evidence. Once a person gives up the password to their devices, the inferences that can be drawn against them can be numerous. First, it can be said that the person, in fact, is in control of the device. Second, should the police have suspicions that the device contains incriminating evidence, then that puts another clear link between the person and evidence. This is the kind of 'link in the chain of evidence' that Selvi had cautioned about. In such light, there is enough thrust to the argument that the judgement in *Virendra Khanna* was incorrectly decided, and deserves reconsideration.

Right to privacy

The High Court knew about the possible violation of the right to privacy due to the immense amounts of data available on digital devices. It noted that once a law enforcement agency has access to a device, the person's entire life is accessible. However after stating the same, the court changed its course by saying use of such information would not violate the right to privacy as it was covered by exemptions. In the same breath, it mentioned that unlawfully disclosing such data with third parties could invite penalties.

While a criminal investigation does require some degree of compromise on individual privacy, allowing all activities in the context of an investigation does away with the fundamental right. As per the case, the courts should allow for unrestrained access to the police. This did not lead to any proper safeguards to be formed and just takes away the right. The courts ought to guide the police to exercise reasonableness or establish a time limit for such snooping.

The case did not law down any remedies for such a violation of the right to privacy. Even though the HC noted that third party disclosures could lead to a breach, there is nothing more that they offered in the judgement.

Ram Ramaswamy and Ors. v. Union of India and Ors

In early 2021, five academics submitted a plea asking for the creation of guidelines to regulate the police and investigating agencies on seizure of mobile phones and computers of the

academia as "electronic evidence" by investigating agencies during raids, saying they have a right to protect their work and research embedded in these personal digital devices.[10] Claiming that devices of several people from the academic field have been seized by investigating agencies in the recent past, the petition stated that it causes loss of research work. The lack of any procedures for the police for appropriate mode of recovery of material in the electronic or digital format, which is unique only to digital devices, threatens the damage or loss of such work.

In 2022, the Foundation for Media Professionals ('FMP') approached the Supreme Court seeking regulation of the police's power to search or seize electronic devices.[11] In October, the Court issued notice to the government to respond.[12]

As per 14th December 2023, the Supreme Court has directed that CBI Manual, 2020 will be followed for device seizures. There will a separate committee that will in the longer run decide comprehensive guidelines around device seizures.

10 https://scroll.in/latest/990961/sc-issues-notice-to-centre-on-academics-plea-seeking-guidelines-on-seizure-of-electronic-devices

11 https://internetfreedom.in/sc-issues-notice-in-fmp-petition-regulation-of-polices-power-to-search-devices/

12 https://www.medianama.com/2022/10/223-stop-police-search-mobile-phones-plea-in-sc/

Internet Shutdowns

The Indian government has implemented internet shutdowns across the country through the operation of two legislative frameworks, by section 144 of the Code of Criminal Procedure and under section 5(2) of the Telegraph Act and the Suspension Rules. Different executive authorities are allowed the power and discretion to institute a shutdown under these laws, although the grounds triggering a shutdown are vague and open to interpretation.

Section 144, Code of Criminal Procedure

Prior to 2017, internet shutdowns were largely executed by District Magistrates or any government official empowered by the State under section 144 of the Code of Criminal Procedure, 1973 (CrPC).[13] Section 144 empowered the government to take "temporary measures to maintain public tranquillity", and accordingly allowed the states to take any immediate measures for remedy in case of apprehended danger.[14] This is not an explicit source of power for governments to order internet shutdowns, but has been interpreted to fit this scope. Its application to instituting shutdowns has been criticised by many, including the Supreme Court,[15] but is best explained in this way:

> **1. Authority**: The power to issue orders lies with the District Magistrate, a sub divisional magistrate or any other Executive magistrate specially empowered by the State Government on this behalf.
>
> **2. Grounds**: If the magistrate is convinced there is i) sufficient ground, ii) need for immediate prevention, iii) to prevent obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquillity, or a riot, of an affray. The need for shutting down the internet has been interpreted out of a requirement to quell communication and the "spreading of rumours" during a time of public disorder (or in anticipation thereof).
>
> **3. Action**: Once these grounds are fulfilled, the authorised official can direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management. Typically, this order is directed at Internet Service Providers ("ISP") in India, and they are directed to halt internet services in a specific area, for a given time period.

13 The grounds on which S. 144 can be invoked: sufficient ground/requirement for immediate prevention/speedy remedy - to prevent a likely obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, or an affray

14 See The Software Freedom Law Centre's explainer for more https://sflc.in/legality-internet-shutdowns-undersection-144-crpc

15 *Anuradha Bhasin v. Union of India*, Writ Petition (Civil) No. 1164 Of 2019.

As a result, shutdowns in different states have been justified as a measure to uphold law and order by the governing authorities, in situations of disorder or other windows of risk.

Telegraph Act and Telecom Services Rules

Section 5(2) of the Indian Telegraph Act of 1885 allows for the government to stop "telegraphic transmission" in times of public emergency or in the interest of public safety.[16] "Telegraphic transmission" has been defined broadly enough to include access to the internet,[17] and therefore creates a more explicit power to shut down internet services.

The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules ("Telecom Rules") was brought in in 2017, to provide the government with a procedure to exercise its powers under section 5(2) of the Act vis-a-vis internet services.[18]

1. Authority: The Telecom Rules give the power to suspend internet services (a) to the Secretary to the Home Ministry in the case of the Central Government, and (b) to the Secretary to the Home Department, in the case of the State Government. This power is explicitly not permitted to be exercised by anyone else.[19] In "unavoidable" situations where these authorities are not available, the suspension order can be issued by a duly authorised officer provided that it is confirmed by the authorities within 24 hours.[20]

2. Grounds: The government is permitted to stop telegraphic transmission in times of "public emergency" or interest of public safety, and if such a measure is necessary or expedient in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence.[21]

3. Action: The government is given the power to direct that the transmission of messages be stalled, intercepted, or detained.[22] Similar to section 144, this direction is aimed at Internet Service Providers, and they are directed to stop or limit their services. The Telecom rules also specify how and in what form communication of this direction could be given.[23]

16 Section 5, Indian Telegraph Act, 1885.

17 Section 3(1AA), Indian Telegraph Act, 1885 - 'telegraph' means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electromagnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means.

18 The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017

19 Rule 2, Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017

20 Rule 2(1), Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017

21 Section 5(2), Telegraph Act 1885.

22 Section 5(2), Telegraph Act 1885

23 Rule 2(3), The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017.

4. Safeguards: The Rules create a Review Committee[24] that is tasked with examining (with a record of their findings) whether the internet shutdown is in line with Section 5(2) of the Telegraph Act. Recently, in 2020, an Amendment ensured that a suspension order cannot be in operation for over 15 days.[25]

Anuradha Bhasin v Union of India

In 2019, the Supreme Court of India heard a case that challenged the prolonged internet shutdown in Jammu and Kashmir.[26] Among other things, it clarified the applicability of some procedural safeguards within the legal framework:

1. All orders passed under the Telecom Rules have to be published, to ensure that they are amenable to judicial review.

2. Orders passed under the Telecom Rules must be 'reasoned'.

3. Internet shutdowns need to be 'temporary' and not indefinite..

4. The Review Committee must meet within 7 days of the preceding review, and ensure compliance with the conditions of section 5(2) of the Telegraph Act.

How internet shutdowns work

Internet shutdowns typically exist on a spectrum, and can include everything from complete communication blackouts or disruptions of mobile service, to obstructing or slowing down connections, to selectively blocking/censoring certain platforms. Additionally, this blocking can be done directly by a government body, when there is a national gateway or firewall where all traffic enters or exits a country, or at the carrier and ISP level.

In India, mobile internet is the predominant mode of accessing the internet.[27] As a result, it is also the major target of internet shutdowns in India in recent times,[28] sometimes leaving broadband and fixed cable services available for use. In other instances however, all internet

24 Review committee comprises other executive members, including the Cabinet Secretary, Secretary to the Government of India In-charge, Legal Affairs, and Secretary to the Government, Department of Telecommunications. See Rule 2(5), The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017.

25 Rule 2A, Temporary Suspension of Telecom Services (Amendment) Rules, 2020.

26 *Anuradha Bhasin v Union of India*, Writ Petition (Civil) No. 1164 Of 2019.

27 Estimates suggest upto 73% of India's total web traffic come from mobile phones. See https://ecoti.in/PCS1mb55

28 See page 26 https://www.accessnow.org/cms/assets/uploads/2022/04/2021-KeepItOn-Report-1.pdf

and telecom services, including calls and SMS services, have been stopped.[29] In practice, this is implemented merely by officials writing a letter and sending (or emailing) it to all Internet Service Providers with regional offices in a specific geographic area. The ISPs then block all incoming and outgoing data moving through cell-phone towers and fibre-optic networks in that particular area.[30] However, it is now obligatory for the government to also publish this order for public access. In India, common triggers for internet shutdowns have been anti-government protests, communal tensions, law and order situations — or the risk of any of these — and public examinations.

Tools to circumvent internet shutdowns

Since internet shutdowns in India are instituted by suspending internet services, as opposed to selectively blocking or slowing down platforms, several circumventing tools used (such as using a VPN) are not available for use. Simultaneously, it is important to remember that internet shutdown orders are aimed at ISPs, and seek to enforce their compliance. Citizens will not be (legally) punished in any way for attempting to circumvent this, provided of course they use legal means and tools. However, there is certainly always some amount of risk involved here, as it is difficult to predict how attempts to circumvent a government order might be taken by the executive in charge.[31]

Another factor to consider is that while there may be other available options for communicating during a lockdown, it is also likely that such options are being surveilled, particularly if the shutdown is instituted to thwart anti-government protests (as was the case in Hong Kong).

> **1. Peer to Peer apps, or MESH networks**: Mesh networks are useful alternative platforms of communication during complete internet shutdown when all outside connectivity is blocked and users are unable to use VPNs. Mesh networks allow users to maintain communications without relying on the internet or SMS services; instead, they use Bluetooth or Wi-Fi technology to create a chain of devices that can send messages to one another when they are in the same vicinity.[32] The power of the model typically depends on the scale of users, with popular platforms like Bridgefy

29 From 5th August to at least 17th August (although many records suggest a much longer shutdown) a complete communication shutdown was instituted in Jammu and Kashmir, including all landlines, voice calls, SMS services, broadband internet and mobile internet. See https://internetfreedom.in/recap-part-i-kashmir-communication-shutdown-and-movement-restrictions-cases/

30 See https://spectrum.ieee.org/how-the-worlds-largest-democracy-shuts-down-the-internet

31 In 2020, several FIRs were registered against persons in Kashmir who used VPNs to circumvent a social media ban in the State, despite the use of VPNs being legal. See https://tcrn.ch/37Fwx5p

32 Kelsey Houston-Edwards, "The Mathematics of How Connections Become Global," Scientific American, April 1, 2021, https://www.scientificamerican.com/article/the-mathematics-of-how-connections-become-global

or Briar having a range of about 100 metres between devices.[33] The addition of more devices to the network increases its effective range.[34] As a result, in situations where there is a sufficient density of users, such as in a protest, this network can create a cluster of connected nodes that allow seamless communication in a geographic area. Essentially, instead of sending a signal from your phone to a cell tower to connect to the mobile network and then onward to the next device, as is typical in telecom services, mesh networks cut out the intermediary. This is done by allowing phones to communicate directly via their internal Bluetooth or WiFi antenna.[35]

During the anti-government protests in Hong Kong, and the protests in New Delhi against the Citizenship Amendment Act, protestors organised amidst internet suspension using Bridgefy.

2. SMS services: SMSWithoutBorders is a platform that was created during Cameroon's 240-day-long shutdown in 2017–2018, during which internet connectivity was severed but remained functional.[36] SMSWithoutBorders allows smartphone users to communicate with online third-party platforms using SMS messages. In cases where internet services are unable but SMS and voice services remain, this could be a useful way for mass communication/organisation. For instance, citizens could register their Twitter and Gmail credentials with the service, and then use their SMS functions during an internet shutdown to post on Twitter or to send/receive emails. There has not been reported use of this platform in India, as of yet.

Things to remember

1. Preparing in advance: Citizens, and particularly civil society actors, should take steps in advance to prepare for impending internet shutdowns.[37] In India, shutdowns are typically instituted during periods of civil unrest, religious or community strifes, protests, public examinations, etc. Citizens should proactively acquire digital tools and possibly create awareness about their use (safely, in a manner that wouldn't preempt the eventual use of these tools) ahead of these windows of risk, while the internet is still accessible.

33 See Michael Caster, "How to Bypass 'Digital Dictatorship' During the Myanmar Coup," Vice, February 8, 2021, https://www.vice.com/en/article/dy8ekx/how-to-bypass-digital-dictatorship-during-the-myanmar-coup

34 See Michael Caster, "How to Bypass 'Digital Dictatorship' During the Myanmar Coup," Vice, February 8, 2021, https://www.vice.com/en/article/dy8ekx/how-to-bypass-digital-dictatorship-during-the-myanmar-coup

35 See Michael Caster, "How to Bypass 'Digital Dictatorship' During the Myanmar Coup," Vice, February 8, 2021, https://www.vice.com/en/article/dy8ekx/how-to-bypass-digital-dictatorship-during-the-myanmar-coup

36 Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," New York Times, September 2, 2019, https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html.

37 Read https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687 for more

Civil society organisations that are better equipped to anticipate the triggers that may lead to a shutdown could coordinate awareness efforts by recommending actions to citizens on how to safely use communication tools. A risk that they must be prepared for in this situation is that if such information reaches the government, it could be considered a security concern and the tools in question may be prohibited or otherwise removed.

2. Focusing on accessibility: Internet shutdowns are intended to target communication between citizens; in India, this comprises a majority of people that are not digitally literate. To enable them to use digital tools during a period of internet shutdown, they need to learn how to use them quickly and effectively, with limited technical knowledge. Civil society actors should focus on advocates from local communities, potentially in local languages, to ensure they are also responding to local community needs. It is also important to inspire trust in these tools, as people could be (rightly) weary of taking action that directly opposes government orders. While the use of these tools are not illegal in India at this moment, it is difficult to predict how it may be used against users by an unscrupulous actor.[38]

3. Digital Documentation: In periods when the internet (and other communication) is completely shut down, it is especially important to digitally document important footage for later use, even if it cannot be transmitted immediately. This footage helps monitor, report, and address violations, and can be later used by activists, human rights investigators etc. Since internet shutdowns also block news and media platforms from becoming aware of or reporting on incidents/events in that region (both to that region and the rest of the country), documenting violations for later use becomes especially important. To that end, citizens can download specialised documentation apps, such as ProofMode, Tella, or Eyewitness to Atrocities, that supplement footage with metadata or technical information pulled from a user's phone for verification purposes.[39]

Legal Tools

Right to Information Requests

The law that allows internet shutdowns, as it stands, is broad and vague, allowing much discretion to the executive to make such decisions. However, there are some legal safeguards that were put in place to ensure that such power is not misused, and that the impact of a

38 In 2020, several FIRs were registered against persons in Kashmir who used VPNs to circumvent a social media ban in the State, despite the use of VPNs being legal. See https://tcrn.ch/37Fwx5p

39 Read https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687 for more

shutdown is not more dire than any benefit it serves. These safeguards are not always followed or protected, importantly including the obligation of the executive to publish internet suspension orders. Owing to the general opaqueness in these situations, there is also little information and transparency involved in the measures. Civil society actors could also consider using Right to Information requests and strategic litigation to hold governments accountable for their shutdown measures.

Some grounds that could be used:

1. The presence of a review committee: A Review Committee is supposed to convene within five days of each internet shutdown order that is passed, and 'record its findings' on whether the order is in accordance with Section 5(2) of the Indian Telegraph Act, 1885. Among other things, this is intended to ensure that internet shutdowns are carefully considered, and are lawful, necessary, and proportionate to the situation they are attempting to address. Using an RTI request, citizens could gather information on the extent to which this was followed. Recently, the Internet Freedom Foundation filed an RTI with the Rajasthan Government in response to an internet shutdown order, asking for findings of the Review Committee on the necessity of such an order. In response, the government stated that the Review Committee did not record findings while evaluating the legality of internet shutdown orders and instead merely confirmed internet shutdown orders by circulation. This is a violation of the law, and could potentially be used as a ground to challenge the order in a court of law.

2. The use of S. 144: In *Anuradha Bhasin*, the court clarified that after the 2017 Telecom rules, internet shutdowns could not be instituted by the District Magistrate using s.144 of the CrPC. However, in practice, this continued unabated in several States, notably recently in Madhya Pradesh, Uttar Pradesh and West Bengal.[40] Civil society actors can consider filing RTIs to ascertain what provision of law the executive is using, in an attempt to increase accountability. Alternatively, RTI requests can be used to find out what is being done to increase awareness amongst government executives about the invalidity of the use of s.144 for imposing internet shutdowns, as the Internet Freedom Foundation has done here.

3. Failure of the executive to publish internet suspension orders: This obligation was reiterated by the Supreme Court in Anuradha Bhasin, but continues to be ignored by governments. The lack of published suspension orders impacts citizens' awareness and preparedness for internet shutdowns, but more importantly obscures the scope and validity of the shutdown. As certain criteria must be fulfilled to require a shutdown, and the order must be lawful, necessary, and proportionate, published orders would also help hold the executive government accountable. An example of an RTI filed by the Internet Freedom Foundation can be found here and here.

40 See https://internetfreedom.in/rti-responses-from-andhra-pradesh-and-gujarat-show-compliance-failure-with-the-anuradha-bhasin-internet-shutdown-decision/

Strategic litigation

Previously, strategic litigation has been used to challenge specific instances of internet shutdowns in different parts of the country. However, there have been only two known instances where courts in India stepped in to stop an ongoing shutdown. The first, 2019, was when the Gauhati High Court admitted a petition challenging the suspension of mobile internet that had been earlier imposed in parts of Assam, and ordered the authorities to restore such services. A constitutional challenge to the TSTS Rules is currently pending in front of the same court. The second was in 2022, when the Kolkata High Court stayed an internet shutdown order that was meant to shut down services in several districts of West Bengal, to prevent cheating during school secondary exams. Another petition has been pending in the Supreme Court of India in which shutdowns imposed to prevent cheating in examinations have been challenged. A recent judgement by the Jharkhand High Court directs state authorities to publish all orders concerning Internet Shutdowns in the state of Jharkhand within 48 hours.[41]

41 https://www.livelaw.in/high-court/jharkhand-high-court/upload-previous-internet-suspension-orders-within-48-hours-on-official-website-of-the-state-government-jharkhand-238210


THE
CENTRE
FOR
internet
& society