# Revising the Information Technology Act, 2000

VRINDA BHANDARI

*Advocate, Delhi High Court*

RISHAB BAILEY

*Visiting Fellow, XKDR Forum*

KARTHIK SURESH

*Research Associate, XKDR Forum*

RENUKA SANE

*Visiting Fellow, XKDR Forum*

March 30, 2023

## Acknowledgement

We thank the Broadband India Forum for supporting this research. We are grateful to Rakesh Roshan for research assistance, and to Ajay Shah, Saikat Datta, and Nandkumar Saravade for valuable discussions and comments. The views expressed are personal and all errors are our own.

# Contents

**Acronyms** **5**

**1 Introduction** **6**

**2 Censorship** **9**
2.1 Background . . . 9
2.2 Statutory framework . . . 10
2.3 Analysing the censorship framework . . . 12
2.3.1 Lack of accountability: Committee of Examiners . . . 12
2.3.2 Lack of accountability: Review Committee . . . 13
2.3.3 Denial of information: Mis(use) of Rule 16 . . . 14
2.3.4 Lack of clarity around unblocking . . . 15
2.4 Recommendations . . . 15
2.4.1 Institutional Reform . . . 16
2.4.2 Revisions in the IT Act: . . . 16

**3 Intermediary liability** **19**
3.1 Background . . . 19
3.2 Statutory framework . . . 19
3.2.1 Section 79 of the IT Act . . . 20
3.2.2 IT Rules, 2021 and 2022 . . . 20
3.3 Analysing the intermediary liability framework . . . 22
3.3.1 Lack of differentiation amongst intermediaries . . . 22
3.3.2 Privatising and broadening censorship through the safe harbour framework . . . 24
3.3.3 Encouraging surveillance . . . 25
3.3.4 Violation of principles of natural justice . . . 26
3.3.5 Government interference via the Grievance Appellate Committee 27
3.4 Recommendations . . . 27
3.4.1 Statutory reform: Section 2(1)(w), IT Act . . . 27
3.4.2 Statutory reform: IT Rules, 2021 . . . 28
3.4.3 Institutional reform . . . 29

**4 Surveillance** **30**
4.1 Background . . . 30
4.2 Statutory framework . . . 31
4.2.1 Section 69 . . . 31
4.2.2 Section 69B . . . 32
4.2.3 Section 67C . . . 33
4.2.4 Obligations imposed through Rules . . . 33
4.3 Analysing the Surveillance Framework under the IT Act . . . 34
4.3.1 Interception and Monitoring . . . 34
4.3.2 Data Retention . . . 37
4.3.3 Surveillance using end-user devices . . . 39
4.3.4 Mandating traceability . . . 40

4.3.5 Mass surveillance programs . . . . . 42
4.4 Recommendations . . . . . 43
4.4.1 Implement a comprehensive surveillance framework . . . . . 43
4.4.2 Revisions in the IT Act . . . . . 45
4.4.3 Other legislative changes . . . . . 47

**5 Cybersecurity** **48**
5.1 Background . . . . . 48
5.2 Statutory framework . . . . . 49
5.2.1 CERT-in . . . . . 50
5.2.2 NCIIPC . . . . . 52
5.2.3 Understanding the broader cybersecurity ecosystem: . . . . . 52
5.3 Analysing the cybersecurity framework . . . . . 55
5.3.1 Shortcomings in substantive provisions . . . . . 55
5.3.2 Lack of inter agency coordination . . . . . 56
5.3.3 Excessive delegated powers . . . . . 57
5.3.4 Flaws in institutional design . . . . . 58
5.4 Recommendations . . . . . 61

**A Appendices** **63**
A.1 Appendix A: Comparison of surveillance safeguards . . . . . 63
A.2 Appendix B: Comparing cybersecurity laws across jurisdictions . . . . . 65

# Acronyms

| | |
|---|---|
| AIIMS | All India Institute of Medical Sciences |
| CEA | Central Electricity Authority |
| CERT-in | Indian Computer Emergency Response Team |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CISO | Chief Information Security Officer |
| CMS | Central Monitoring System |
| DARPA | Defense Advanced Research Projects Agency |
| DOT | Department of Telecommunications |
| DSCI | Data Security Council of India |
| EU | European Union |
| GDPR | General Data Protection Regulations |
| IOT | Internet of things |
| ISAC | Information Sharing and Analysis Centre |
| ISSC | Information Security Steering Committee |
| KYC | Know your customer |
| LEA | Law Enforcement Agency |
| LIMP | Lawful Intercept and Monitoring Project |
| MEITY | Ministry of Electronics and Information Technology |
| NATGRID | National Intelligence Grid |
| NCIIPC | National Critical Information Infrastructure Protection Centre |
| NETRA | Network Traffic Analysis |
| NTRO | National Technical Research Organisation |
| RBI | Reserve Bank of India |
| RDSP | Relevant digital service provider |
| SEBI | Securities and Exchanges Board of India |
| UIDAI | Unique Identification Authority of India |
| UK | United Kingdom |
| USA | United States of America |

# 1 Introduction

The Information Technology Act, 2000 ("IT Act") is a comprehensive law enacted to build trust in the digital ecosystem by regulating e-commerce, facilitating electronic filing of documents, and creating criminal offences applicable to the digital ecosystem. Despite amendments in 2009, the IT Act is commonly seen as being outdated.[1] The proliferation of the internet and the development of a range of new digital technologies over the last decade has raised a number of questions concerning the safety and security of the digital ecosystem, and in particular about the role to be played by both the government and private sector players therein. Reports indicate that the Government of India is now planning to replace the IT Act with new legislation as part of a broader package of laws concerning the digital ecosystem.[2]

This report attempts to contribute to the process of revision of the IT Act, by examining four critical issues pertaining to the online ecosystem. These are:

- *Censorship*: The power and processes used to censor digital content in India have been a bone of contention for a number of years. While the digital ecosystem is typically seen as a haven for free speech, the Indian constitutional framework dictates that there must be a method to regulate harmful online content. However, the current framework under the IT Act provides extremely broad powers to the government, with minimal safeguards to fetter abuse.

- *Intermediary liability*: There is significant debate globally and in India on the role played by intermediaries in ensuring user safety. At present, the IT Act affords intermediaries protection from prosecution for third party content on their platforms, based on the role played by the intermediary in enabling access to the content, as well as their adherence to due diligence obligations. However, this framework has been criticized for failing to adequately account for the variety of online harms, the role and ability of different intermediaries to address such harms and the imposition of broad obligations through the route of due diligence related rules.[3]

- *Surveillance*: The surveillance related provisions in the IT Act were drafted prior to the recognition of privacy as a fundamental right in the *Puttaswamy* case.[4] It has

[1] Rishab Bailey, Faiza Rahman, and Varun Sen Bahl, "Internet Intermediaries and Online Harms: Regulatory Responses" [2020] ; Aniruddh Nigam and others, "Primer for an Information Technology Framework Law" (September 2020) <https://vidhilegalpolicy.in/research/primer-for-an-information-technology-framework-law/>; NS Napinnai, "Cyber security and challenges: Why India need to change IT Act" (February 2017) <https://www.cyberpeace.org/CyberPeace/Repository/20180412-IT-Act-Need-for-Laws-%20to-Spruce-Up-02.02.2018-1.pdf>.

[2] Viraj Gaur, "India Is Moving To Replace Two-Decade-Old IT Act With New 'Digital India Act'" (April 2022) <https://www.thequint.com/tech-and-auto/tech-news/india-is-moving-to-replace-decades-old-it-act-with-new-digital-india-act-and-data-governance-framework-rajeev-chandrasekar>; Gulveen Aulakh, "India to replace IT Act with Digital India Act, part of comprehensive legislative framework expected in 3-4 months" (September 2022) <https://www.techcircle.in/2022/09/07/india-to-replace-it-act-with-digital-india-act-part-of-comprehensive-legislative-framework-expected-in-3-4-months>.

[3] Bailey, Rahman, and Bahl (n 1); Rishab Bailey, Smriti Parsheera, and Faiza Rahman, "Comments on the (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018" (January 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328401>.

[4] Supreme Court of India, "Justice K.S. Puttaswamy v. Union of India" (August 2017) <https://

been argued that the surveillance powers provided to the government are broad, and contain limited safeguards to prevent misuse.[5] At the same time, the growth of digital communication channels and the ubiquity of privacy enhancing technologies such as end-to-end (E2E) encryption has led to a variety of new challenges faced by Law Enforcement Agency (LEA)s in accessing data required for the prosecution of offences.[6]

- *Cybersecurity*: Ensuring the robustness and resilience of the digital ecosystem is a precondition for growth of this sector. The IT Act establishes institutional frameworks to deal with issues of cybersecurity, though these are said to be ineffective and in need of reform.[7]

Each of these issues is connected by a common thread — how can one promote trust in the digital ecosystem? Finding answers requires a careful consideration of multiple concerns such as national security and public order, the growing instances of online harm, the need to protect fundamental rights, and the need to promote innovation in and development of the digital ecosystem. For instance, in the context of surveillance and censorship, competing constitutional principles such as that of privacy, expression, state security and public order must be accounted for. Intermediary regulation is a thorny issue involving difficult questions about the ability of private platforms and the government to make the digital ecosystem safer, while promoting innovation. Similarly, the issue of cybersecurity raises questions about the role of the state and private players in ensuring networks and systems are made more secure, resilient and robust.

In this context, this report examines literature, case law, and media reports in order to understand the current structure of the IT Act and its shortcomings. Based on best practices including experience from foreign jurisdictions, various recommendations are made to revise relevant provisions of the IT Act.

In the first section of the report we address issues of censorship. We find that the IT Act framework is largely based on Article 19(2) of the Constitution. Thus, the priority should be to ensure institutional reform to ensure independent decisions on content blocking as well as effective review and accountability. The processes prescribed by the IT Act framework could be improved by providing a hearing to affected content creators, laying down processes for unblocking content and enhancing transparency in blocking processes.

In the second section of the report we address the issue of intermediary liability. Noting

indiankanoon.org/doc/91938676/>.

[5] Rishab Bailey and others, *Use of personal data by intelligence and law enforcement agencies* (techspace rep, National Institute of Public Finance and Policy 2018); Vrinda Bhandari, "The Pegasus Case must be used to press for change in surveillance laws" (August 2021) <https://www.theindiaforum.in/article/pegasus-case-must-be-used-press-change-%20surveillance-laws>.

[6] Rishab Bailey, Vrinda Bhandari, and Faiza Rahman, *Backdoors to Encryption: Analysing an intermediary's duty to provide "technical assistance"* (techspace rep, National Institute of Public Finance and Policy 2021).

[7] Udbhav Tiwari, "Cyber security and the CERT-in: A Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian Cyber Security Ecosystem" (November 2016) <https://cis-india.org/internet-governance/files/cert-ins-proactive-mandate.pdf>; Napinnai (n 1).

the trend of broad obligations being imposed on intermediaries through the route of rules issued under Section 79 of the IT Act, we point to how the present intermediary liability framework incentivises censorship of content. We suggest revision of the Section 79 framework to better delineate obligations of different types of intermediaries, ensure processes for take-down of content follow principles of natural justice, and narrow tailoring of due diligence related provisions. We also recommend adopting a co-regulatory framework for content moderation, so as to avoid the problems arising from private censorship as well as excessive government interference in the digital ecosystem.

In this third section of the report we deal with surveillance related provisions in the IT Act. Noting that the framework prescribed by Sections 69 and Section 69B provide excessively broad powers to the government with inadequate checks and balances, we suggest that the entire surveillance framework be revisited in a new law. In the alternative, provisions in the IT Act (or indeed any other law such as the proposed Telecommunications Bill, 2022) could be revised to narrow the scope of state powers and improve accountability.

In the final part of the report, we examine cybersecurity related provisions in the IT Act. We find that the substantive provisions in the law, i.e. those defining and delineating cybersecurity related offences, are relatively robust. However the statute could be amended to introduce various general defences. We also find that the institutional mechanisms established under the IT Act need significant overhaul. We suggest clarifying the role and powers of the two cyber security agencies - Indian Computer Emergency Response Team (CERT-in) and National Critical Information Infrastructure Protection Centre (NCIIPC) by merging their functions into one agency. We also suggest limiting mandatory incident reporting to specific entities, and establishing better coordination mechanisms between the various cybersecurity regulators, sectoral regulators and other authorities.

# 2 Censorship

**Summary of recommendations**

The provisions in the IT Act pertaining to censorship and blocking were framed in an era when the digital ecosystem was not as pervasive as today and before the use of social media platforms exploded. The IT Act provides broad powers to the executive, with inadequate procedural safeguards to check government action. It also suffers from a lack of consistent enforcement and proper accountability. We therefore recommend:

- Revising Section 69A of the IT Act to remove the government's power to block access to online content because it is "expedient" to do so in the interest of national security or public order.
- The creation of an independent and neutral body (such as an ombudsman) to adjudicate on blocking requests. In the alternative, blocking decisions made by the executive apparatus must be subject to judicial oversight as a matter of course.
- Clarifying that mass blocking orders should not be permitted.
- Ensuring greater transparency in blocking processes by providing content creators with a copy of the blocking order. Content creators must also be provided a hearing before a decision to block content is taken, as far as practicable.

## 2.1 Background

The Indian Constitution guarantees the freedom of speech and expression to all citizens. However, this right is subject to reasonable restrictions listed under Article 19(2) of the Constitution, viz. in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. Broad or arbitrary censorship can be a threat to free expression on the internet, the right to free dissemination of information, and the right to receive information - all of which are protected under Article 19(1)(a). Excessive censorship can result in an erosion of democratic rights, both online and offline, including by targeting activists, journalists, and dissenters.

The union government has relied on its power under Article 19(2) to enact various provisions under the IT Act that enable it to censor online content. Notably Section 69A of the IT Act allows the government to direct blocking or take-down of online content. Reports indicate that the powers under this provision are being used with increasing frequency. For instance, while the Indian government required Twitter to delete/take down 248 tweets in 2017, just three years later in 2020, this number increased to nearly 10,000 tweets.[8] The Freedom House Report of 2022 noted that over 200 mobile apps were blocked on the directions of the government since 2020, with 54 apps being blocked

[8] Paroma Soni, "Online censorship is growing in Modi's India" (December 2021) <https://www.cjr.org/investigation/modi-censorship-india-twitter.php>.

in February 2022 alone.[9]

In addition to censorship powers under Section 69A of the IT Act, the government can also 'shut down' access to the internet under the Telegraph Act, 1885. Internet shutdowns are a commonly used method of broad-based censorship whereby the government disrupts, limits or denies access to the internet or telecommunication services in a particular geography. Internet shutdowns are a form of mass censorship, in which India is unfortunately, a world leader.[10] Shutdowns are regulated under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 ("TSP Rules"), which have been notified under the Telegraph Act, 1885.

Under the draft Indian Telecommunication Bill, 2022, the Department of Telecommunications (DOT) has proposed a clear statutory internet suspension power, although various concerns regarding the lack of judicial oversight and other procedural safeguards have been raised by civil society.[11] However, unlike the IT Act, which authorises censorship at the *content* level, the Telegraph Act and internet shutdowns function at the *network* level. Hence, this report does not delve deeper into the issue of internet shutdowns or suggest recommendations for amendments to the Telegraph Act, the TSP Rules, or the proposed Telecommunication Rules, 2022. Instead, in this section, we focus on the blocking powers of the state under the IT Act, and propose amendments to the IT Act in view of various shortcomings.

## 2.2 Statutory framework

The Central Government's power to issue directions for blocking online content stems from Section 69A of the IT Act.[12] This provision authorises the Central Government or an authorised officer, to issue a reasoned order directing that any government agency or intermediary block online content in 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 relating to above. Notably, morality or decency, despite being recognised grounds for censorship under Article 19(2) are *not* grounds for blocking under the IT Act.[13] Under Section 69A(3) of the IT Act, intermediaries are bound to comply with blocking directions, or face criminal sanction.

Processes and safeguards for the blocking of content are prescribed under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (the "*Blocking Rules*").

[9] Freedom House, *Freedom on the Net, 2022* (techspace rep, Freedom House 2020).

[10] American Bar Association, *The Impact of Internet Shutdowns on Human Rights Defenders in India* (techspace rep, ABA 2022).

[11] IFF, "The draft Indian Telecommunication Bill, 2022 retains its colonial roots" (September 2022) <https://internetfreedom.in/the-draft-indian-telecommunication-bill/>.

[12] This provision was introduced to the IT Act via an amendment in 2009. Prior to 2009, the DOT issued blocking orders based on the instructions of authorised government agencies such as the CERT-in. Press Information Bureau, "Blocking of website" (22 September 2003) <https://archive.pib.gov.in/archive/releases98/lyr2003/rsep2003/22092003/r22092003314.html>.

[13] However, as we discuss in subsequent sections, the intermediary liability framework under Section 79 is often used to overcome this 'limitation'.

Rule 3 of the Blocking Rules empowers the Central Government to nominate a Joint Secretary as the "Designated Officer" to exercise the power of blocking online content. Under Rules 4 and 6, government agencies, central and state governments, and ministries may appoint "Nodal Officers" who are tasked with receiving a complaint from the public, assessing the need to take action under Section 69A, and further notifying the Designated Officer. Thereafter, each blocking request must be evaluated by a Committee of Examiners established under Rules 7 and 8 (the "Committee").[14]

On receiving a blocking request, the Designated Officer is required to make "all reasonable efforts" to identify the person or the intermediary who has hosted the impugned information online, issue a notice to them to appear before the Committee and present their case opposing the proposed blocking. Thus, under Rule 8(1), prior notice to the originator of content or the intermediary is a necessity. The Committee must then examine the blocking request to determine whether it falls within the parameters of Section 69A(1) of the IT Act. The Designated Officer then sends the Committee's recommendations to the Secretary of the Department of Information Technology, who takes the final decision regarding blocking. Upon approval, the Designated Officer directs the concerned government agency or intermediary to block the offending content.

Rule 9 deals with blocking content in cases of an emergency, in which case no prior notice is required to be given to the originator of content. However, such an action must be confirmed within 48 hours. These emergency powers seem to have been invoked by the government in June 2020, when they banned 59 Chinese mobile apps, including TikTok, although many believe that the powers were wrongly invoked.[15]

Subsequent to blocking, Rule 14 provides that a three member "Review Committee" (comprising of the three top bureaucrats) must meet once every two months to assess the compliance of the Committee's directions with Section 69A of the IT Act. Finally, one of the most problematic/litigated provisions of the Blocking Rules is Rule 16, which requires strict confidentiality to be maintained regarding "*all the requests and complaints received and action taken thereof*."

The constitutionality of Section 69A of the IT Act along with the Blocking Rules was upheld by the Supreme Court in *Shreya Singhal v Union of India* in 2015, primarily on the strength of how the Blocking Rules provided detailed procedural safeguards to prevent misuse.[16] This is in contrast to Section 66A of the IT Act, which prohibited sending

[14]This comprises the Designated Officer and other high-level bureaucrats such as Joint Secretary in the Ministries of Law and Justice, Home Affairs, Information and Broadcasting, and CERT-in.

[15]The apps were blocked for being prejudicial to sovereignty and integrity of India, defence of India, security of state and public order. Interestingly, the press release issued by the government seems to suggest that they had certain privacy concerns that prompted the ban. However, privacy is not an authorised ground for blocking content under Section 69A, and could not have been used as a justification Press Information Bureau, "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order" (June 2020) <https://pib.gov.in/PressReleasePage.aspx?PRID=1635206>. Even the timing of the TikTok ban was suspect, given that it came in the backdrop of rising geopolitical tensions between India and China. Thus, questions have been raised regarding the use of emergency powers to ban TikTok. Anupriya Dhonchak and Nikhil Purohit, "Is India's ban on Tiktok and 58 other Chinese apps consistent with the provisions of IT Act?" (July 2020) <https://scroll.in/article/966131/is-indias-ban-on-tiktok-and-58-other-chinese-apps-consistent-with-the-provisions-of-it-act>.

[16]Shreya Singhal v Union of India, "Supreme Court of India" (2015).

“offensive messages" or causing "annoyance" online and was used as a tool for arbitrary censorship. The Supreme Court held that unlike Section 66A, the Blocking Rules, 2009 provided sufficient procedural safeguards that, *inter alia* enabled users to challenge the legality of blocking orders).

## 2.3 Analysing the censorship framework

There are various infirmities with the current censorship regime under the IT Act which arise out of four primary issues: the lack of accountability of the Committee of Examiners, the lack of accountability of the Review Committee, the inability of aggrieved individuals to access blocking orders, and the lack of clarity around the unblocking procedure. We discuss each of these issues in this section.

### 2.3.1 Lack of accountability: Committee of Examiners

Over the years, there has been a substantial increase in blocking of online content as is made clear from the following table:[17]

| Year | Number |
|---|---|
| 2010 | 9 |
| 2011 | 21 |
| 2012 | 362 |
| 2013 | 62 |
| 2014 | 471 |
| 2015 | 500 |
| 2016 | 633 |
| 2017 | 1385 |
| 2018 | 2799 |
| 2019 | 3603 |
| 2020 | 9849 |
| 2021 | 6096 |
| 2022 (Jan-Mar) | 1482 |

The last two years have also witnessed a sudden surge in the number of YouTube videos and Chinese apps being blocked. Parliamentary questions reveal that 78 YouTube news channels and 560 YouTube URLs were blocked in 2021 and 2022.[18] Additionally, 2021 mobile apps were blocked in 2022.[19]

[17] Press Trust of India, “Over 6,000 URLs, accounts or websites blocked in 2021: Chandrasekhar” (February 2022) <https://www.business-standard.com/article/current-affairs/over-6-000-urls-accounts-or-websites-blocked-in-2021-chandrasekhar-122020201347_1.html>; Mehab Qureshi, “1482 websites were blocked by IT Ministry in 2022, RTI reveals” (July 2022) <https://indianexpress.com/article/technology/tech-news-technology/1482-websites-were-blocked-by-it-ministry-in-2022-rti-reveals-8059435/>.

[18] NL Team, “India has blocked 78 YouTube news channels, 560 URLs since 2021: I&B minister” (July 2022) <https://www.newslaundry.com/2022/07/19/india-has-blocked-78-youtube-news-channels-560-urls-since-2021-ib-minister>.

[19] IFF, “Revealed: MeitY blocked 6096 URLs and 347 applications in 2021 but held less than 40 hearings” (April 2022) <https://internetfreedom.in/revealed-meity-blocked-6096-urls-and-347-applications-in-2021-but-held-less-than-40-hearings/>.

Given the sharp rise in the number of blocking orders, it is possible that the procedural safeguards have proven to be ineffective. On the other hand, this could merely illustrate the growing (mis)use of the Internet prompted by an expanding user base in the country. In any event, the explosion of content on the internet requires improved state capacity to make correct, time-sensitive decisions regarding blocking online content. Currently however, the legal framework lacks any clear accountability standards that allow us to assess whether the procedural safeguards have proved effective. RTI replies reveal that in deciding to block 6096 accounts and 347 mobile apps in 2021, the Committee of Examiners only met 39 times.[20] Thus, at every meeting, the Committee, on average, *confirmed* the blocking of 166 URLs/apps. These numbers indicate the impossibility of application of mind to each individual case. It is also unclear how many content creators were heard before blocking was carried out. Twitter has raised this issue in a legal challenge to various blocking orders issued by the government.[21] Thus, there appears to be a lack of due process in the censorship processes under the IT Act.

The government has also failed to provide data to clarify this issue. In response to a right to information ("RTI") request seeking clarification on whether hearings were provided to affected content creators, the government has stated that "*Data is not maintained in the form as desired by the applicant. 48 hours advance notice were issued to respective intermediary in respect of all URLs as per Rules. Respective Intermediary representative generally attended almost all the meetings.*" It thus appears that the government generally provides an opportunity of hearing only to intermediaries concerned, notwithstanding that the interests of intermediaries (towards compliance) may not match that of the content creators (who are affected by a blocking order).

### 2.3.2 Lack of accountability: Review Committee

The lack of accountability is further exacerbated by the absence of information on the processes followed by the Review Committee. There is no public record on when the Review Committee has met nor of its deliberations[22] All we know is that in a response to an RTI, the Ministry of Electronics and Information Technology has stated that "*MeitY is not part of Review Committee. So far, MeitY did not receive any such communication wherein blocking order is revoked based on a disapproval from the Review Committee*".[23] This seems to indicate that at least as far as the Ministry is concerned, there is no instance of the Review Committee overturning a blocking order, thereby indicating that the Review Committee may function largely as a "rubber stamping" exercise.

[20] IFF, "Revealed: MeitY blocked 6096 URLs and 347 applications in 2021 but held less than 40 hearings" (n 19).

[21] Mustafa Plumber, "Twitter Inc Approaches Karnataka High Court Challenging Centre's Take Down Orders" (July 2022) <https://www.livelaw.in/top-stories/twitter-karnataka-high-court-ministry-of-electronic-it-section-69a-it-act-203017?infinitescroll=1>.

[22] In response to an RTI request regarding the number of meetings held by the Review Committee, the Ministry of Electronics and IT simply clarified that it did not maintain such data as it was not a member of the Review Committee. It further cited Rule 16's confidentiality requirements as a justification for failing to provide a specific response (IFF, "Revealed: MeitY blocked 6096 URLs and 347 applications in 2021 but held less than 40 hearings" [n 19]).

[23] Saurav Das, "RTI Reply" (April 2022) <https://drive.google.com/file/d/1-KUS0VXwrWtdDMNrUb5L8YMaRA5XJeCV/view>.

Taking the statutory mandate of meeting six times a year, it can be estimated that at *each* meeting of the Review Committee in 2021, it had to take a decision regarding 1016 orders. This is in addition to evaluating compliance with interception/surveillance requests under the Telegraph Act and IT Act as well as internet shutdown orders under the TSP Rules. One is thus, left to wonder, whether the Review Committee is able to serve as an effective safeguard to check instances of misuse of blocking powers.

### 2.3.3 Denial of information: Mis(use) of Rule 16

When access to content is blocked, there is no legal requirement for the government to notify the concerned content creator or owner. Instead, once blocking is completed by the intermediary, content creators/owners will either find that the website does not load, or will see a text message stating that their "*requested URL has been blocked as per the directions received from Department of Telecommunications, Government of India. Please contact administrator for more information*"

The immediate action any content creator/website owner can take is to file an RTI request with the government to seek a copy of the relevant blocking order, so as to assess the reasons for the same. However, as various RTI replies have revealed, the government consistently cites Rule 16 of the Blocking Rules and confidentiality concerns to deny supplying a copy of the blocking order to website creators and content owners.[24] This leaves account owners and creators with no choice but to engage with the prolonged and arduous legal system to *first* attempt to obtain a copy of the blocking order, and *then* challenge the same before a court of law.[25]

This issue has been litigated before various High Courts, such as with the blocking of the "Dowry Calculator" website (http://www.dowrycalculator.com/) in the Delhi High Court[26] and the blocking of the actor, Sushant Singh's Twitter account ("@sushant_says) before the Bombay High Court.[27] The Petition in *Tanul Thakur* sought a declaration that Rule 16 of the 2009 Rules is unconstitutional insofar as it extends to depriving owners/ creators of online content from having access to the record of proceedings resulting in blocking actions.

The government's interpretation of Rule 16 appears flawed insofar as it violates the letter and spirit of the Supreme Court's judgment in *Shreya Singhal*. While upholding the constitutionality of Section 69A and the Blocking Rules (including Rule 16), the Court held as follows, *"It will be noticed that Section 69-A unlike Section 66-A is a narrowly drawn provision with several safeguards. First and foremost, blocking can only be resorted to where the Central Government is satisfied that it is necessary so to do. Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a*

[24] IFF, "Delhi HC issues notice to the government for blocking satirical Dowry Calculator website" (December 2019) <https://internetfreedom.in/delhi-hc-issues-notice-to-the-government-for-blocking-satirical-dowry-calculator-website/>.

[25] Vrinda Bhandari, "Twitter case underlines web moderation issues" (July 2022) <https://www.hindustantimes.com/opinion/twitter-case-underlines-web-moderation-issues-101657209298117.html>.

[26] Tanul Thakur vUnion of India, "Delhi High Court" (2019).

[27] Sushant Singh vUnion of India, "Bombay High Court" (2021).

*writ petition under Article 226 of the Constitution.*" (emphasis supplied)

Thus, instead of publishing its blocking orders, the government has relied on Rule 16 to deny any information to website owners/content creators about the reason for which their account has been blocked. This limits the opportunity for aggrieved persons to the challenge the legality of blocking through proceedings under Article 226 of the Constitution or otherwise. This therefore violates the principles of natural justice and undermines the transparency and accountability processes that were viewed by the Court in *Shreya Singhal* as protecting the constitutionality of the Blocking Rules. This secrecy in process also violates India's commitments under international law. Notably, in its 2011 report, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression observed that wide blocking powers amassed by governments violates the International Covenant on Civil and Political Rights ("ICCPR") since, *inter alia*, blocking lists are kept secret, which makes it difficult to evaluate the legitimacy of the blocking decision.[28]

### 2.3.4 Lack of clarity around unblocking

The Blocking Rules are primarily concerned with blocking public access to online content. However, content can also be 'unblocked' - either because of (a) a court order, (b) the directions of the Review Committee under Rule 14, (c) the direction of the Secretary, Department of Information and Technology given under Rule 9 reversing the emergency blocking decision, or (d) the decision of the Committee of Examiners given in a *post facto* hearing. The legal framework however does not clarify the process for unblocking content by intermediaries across the internet supply chain.

There is no clarity, for instance, on whether the Department of Telecommunications issues an unblocking order marking all the concerned telecom and internet service providers (collectively "access service providers"), and whether the website owner is marked on this communication. Further, as unblocking orders are implemented by access service providers at a regional/local level, anecdotal evidence indicates it is common for content to be unblocked in some regions but not others. Thus, website owners can be faced with selective enforcement of unblocking orders, with no clear remedy in sight. This problem is exacerbated as the Blocking Rules do not provide for any redress mechanism which can be used by individuals who want to ensure the unblocking order is complied with nationally. Thus, it is left to the aggrieved individual to write to all access service providers to ensure their website/app is unblocked.

## 2.4 Recommendations

Censorship of online content through blocking orders issued to intermediaries directly implicates the fundamental right of the content creator, to freely express their opinion, and the fundamental right of the public, to freely receive information. Apart from this, the efficacy of blocking can also be questioned. Blocking directions can be over-broad, thereby covering lawful or legitimate content within their scope (particularly if an entire

[28] UN Special Rapporteur, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (techspace rep, UN General Assembly 2011).

website or app is blocked). In any event, blocks can by bypassed fairly easily through the use of tools such as VPNs.[29] In this context, we suggest certain revisions to the IT Act framework below.

### 2.4.1 Institutional Reform

The section above has listed various problems with the current legislative framework for blocking. The first step towards reform should involve revising the institutional framework for censorship. The process of hearing by a Committee of Examiners (consisting of government officials) ought to be replaced by a more neutral and independent committee, such as an ombudsman. This body should be free from political and other undue influences, as recommended by the UN.[30] Other countries, such as Australia, which also introduced the post of an eSafety Commissioner as part of the Online Safety Act of 2021 (brought in force in 2022), who was empowered to block access to websites, remove online content) have faced similar criticism about excessive centralisation of power in the hands of a single person/entity.[31]

An alternative to the creation of an independent body, is to introduce judicial oversight over the blocking process, carried out by the executive. For instance, under the UK Online Safety Bill, the Secretary has to apply to a court if they want to exercise the "nuclear" option of an "access restriction order".[32] Bringing in courts within the blocking framework introduces an element of friction in the blocking process, to prevent blocking orders from being issued as a convenient option. The Online Safety Bill reinforces this intention, since an access restriction order can only be passed under certain specified and narrowly tailored situations, only if there is a "genuine and severe risk of substantial harm".[33]

However, assuming such broader institutional change is not brought about, it is clear that amendments to the IT Act and the Blocking Rules are needed to reduce the scope for disproportionate and arbitrary censorship.

### 2.4.2 Revisions in the IT Act:

The grounds that justify blocking under Section 69A are relatable to Article 19(2), and go a step further by omitting "decency or morality" as grounds. While the omission of "decency or morality" is commendable, it may be worthwhile to examine the *type* of content that justifies the use of extraordinary blocking powers. For instance, in many countries in Europe, content regarding child sexual exploitation abuse material (CSAM),

[29] Koan Advisories, *Reimagining India's Information Technology Act* (techspace rep, Koan 2021).

[30] UN Special Rapporteur (n 28).

[31] Cam Wilson, "A New Internet Law Has People Worried And The Australian Government Isn't Listening [Updated]" (March 2021) <https://www.gizmodo.com.au/2021/03/a-new-internet-law-has-people-worried-and-the-australian-government-isnt-listening/>; Digital Rights Watch, "Explainer: The Online Safety Bill" (February 2021) <https://digitalrightswatch.org.au/2021/02/11/explainer-the-online-safety-bill/>.

[32] Heather Burns, *Access Denied: Service Blocking in the Online Safety Bill* (techspace rep, Open Rights Group 2021).

[33] Ibid.

terrorism, and raising national security concerns can be blocked.[34] In India, however, Section 69 is more broadly worded, including justifications such as friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence.

As we have seen, the primary problem lies with the implementation of the provision and the lack of procedural safeguards. However, it must also be kept in mind that these grounds can be invoked by the competent authority if considered "necessary or expedient" to achieve national security or public order aims. The use of the term "expedience" denotes convenience and allows for a broad and arbitrary application of the blocking powers. This facilitates an overuse of the blocking powers.

The use of the term "expedient" is also contrary to the dictum of the Supreme Court in *S. Rangarajan v. P. Jagjivan Ram* that the nexus between the speech (sought to be restrained) and the apprehension of the breach of public order should be narrowly tailored, akin to a "spark in a powder keg".[35] Thus, the phrase should be revised to only permit blocking where "necessary".

Additionally, the following statutory amendments can be carried out:

1. **Hearing process**: It appears from RTI responses that the Committee of Examiners routinely authorises blocking orders without proper application of mind. In most cases, the aggrieved individual (whether the content creator or the owner of the website) is not heard, and instead, only the intermediary's submissions are taken into account. Affected individuals should be provided the right to contest a blocking request. As noted in *Shreya Singhal*, intermediaries are not in a position to judge the legality of content, and as such, their focus is on compliance with the Committee's decision (and not necessarily to contest it). Thus, *assuming* that the Committee is retained in the amended IT Act, it is imperative to ensure the presence of owners/content creators at the hearings (as far as practicable or reasonable) so that they can make representations against the proposed action. At a minimum, through the Blocking Rules, the government should be mandated to check the WHOIS details of the website to ensure compliance with their "reasonable effort" obligation.

2. **Judicial oversight**: Given the opacity concerning the functioning of the institutions tasked with blocking content as well as the lack of expertise of these bodies in what is essentially a judicial function, it is essential to have independent judicial oversight of the orders of the Committee of Examiners. Interestingly, Twitter in its recent petition before the Karnataka High Court has also sought judicial review over 39 blocking orders imposed by the government.

3. **Amending Rule 16**: As discussed previously, Rule 16 is often used as a pretext to deny individuals information about blocking of their content. This limits the ability for individuals to challenge any illegal orders. Based on the portion of the *Shreya Singhal* judgment extracted above, it appears that the said rule was never

[34] Swiss Institute of Comparative Law, *Comparative study on blocking, filtering and take-down of illegal internet content* (techspace rep, Council of Europe 2017).

[35] (1989) 2 SCC 574

intended to protect the confidentiality of the final blocking order, but was limited to protecting the confidentiality of the original complaints made and if at all, to limit the circulation of the final decision.[36] Currently, the government is citing Rule 16 to reject RTI requests from individuals seeking a copy of the blocking order passed in respect of their website/app. Hence, either Rule 16 should be amended applying the transparency logic provided by the Supreme Court in *Anuradha Bhasin*,[37] such that all blocking orders are published online. In the alternative, the interpretation of Rule 16 should be clarified to ensure website owners are, *post facto*, provided a copy of their blocking order to enable them to challenge the same.

4. **Improved accountability**: Blocking access to online content is a significant restriction on the right to free speech, guaranteed under Article 19 of the Constitution. It should require the Committee of Examiners and the government to specifically consider the proportionality of the restriction, and apply its mind to each website or app proposed to be blocked. However, the government often issues a mass blocking order covering multiple websites/apps.[38] This precludes a detailed analysis on every single app. For instance, a perusal of the 58 apps blocked by the government together with TikTok reveal their varied nature, ranging from social media apps, to e-commerce apps, browsers, news aggregators and utility apps.[39] Such mass blocking orders should be avoided and the government must be made to justify *each* instance of blocking.[40] Such a change can be made either legislative through the text of the law (Section 16) or by an executive notification amending the Rules. In both cases, however, it must be clarified that the blocking order must contain reasons for each individual case of blocking, and cannot contain multiple unrelated websites in the same order.

5. **Unblocking**: The Blocking Rules should be amended to specifically provide for unblocking, and to lay down the procedure to be followed in all cases of unblocking. To begin with, all orders for unblocking access to a website or online resource must be published online and must be directly communicated to the concerned website owner. Further, such unblocking orders should be issued to all access service providers, with directions to apply in a time-bound manner, of which the government should ensure strict compliance.

---

[36] Rule 16 states as follows, "*Strict confidentiality shall be maintained regarding all requests and complaints received and action taken thereof.*"

[37] The Telecom Suspension Rules do not provide for internet shutdown orders to be published online. However, keeping in mind the importance of the freedom of speech and expression and the right to do business online under Articles 19(1)(a) and 19(1)(g), the Supreme Court in Anuradha Bhasin directed that all shutdown orders must be made public.

[38] Press Information Bureau, "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order" (n 15).

[39] Koan Advisories (n 29).

[40] Dhonchak and Purohit (n 15).

# 3 Intermediary liability

**Summary of recommendations**

The IT Act framework pertaining to intermediary liability requires urgent revision, especially considering that new rules introduced in 2021 and 2022 have significantly increased the obligations on intermediaries. Importantly, the current statutory framework does not sufficiently distinguish between different types of intermediaries based on size. We therefore recommend:

- Imposing additional obligations on intermediaries based on their effects on the ecosystem. Classification in terms of size may be a simple and proportionate method to impose additional obligations on large, ecosystem players. Such obligations could range from the need to implement grievance redress mechanisms or ensure greater transparency of platforms towards users.
- Substantive obligations should not be imposed through the intermediary liability framework. Any interventions targeted at broader harms in the ecosystem (ranging from safety to competition related), should be based on an identified need and preferably through less intrusive options such as through co-regulatory methods.
- Amendment of Rule 3(1)(b) of the IT Rules, 2021, to narrowly tailor the conditions under which content can be taken down and to remove proactive content removal obligations.
- Amendment of Rule 3(1)(j) and Rule 4(2) of the IT Rules, 2021, to clarify that end-to-end encryption should not be broken.
- Amendment of Rule 3(2)(a) of the IT Rules, 2021, to provide a statutory right of hearing and a right to appeal to content creators before any decision regarding their content is taken by an intermediary.

## 3.1 Background

Content regulation under the IT Act primarily takes place through three avenues: *first*, the prohibition and criminalising of the publication of obscene and sexual content under Sections 67, 67A, and 67B of the IT Act; *second*, blocking content under Section 69A, IT Act; and *finally*, by incentivising private censorship through the use of intermediary liability frameworks. This section is concerned with censorship (taking down content) via the due diligence obligations imposed on intermediaries, an issue which requires considering the free speech rights of the content creator, the free speech rights of the users, the rights of the intermediaries to conduct their business, as well as the right of the state to protect national security and public order. Each of these rights is affected in a different manner from the implementation of the intermediary liability frameworks.

## 3.2 Statutory framework

In this section, we discuss the intermediary liability framework prescribed by Section 79 of the IT Act and the rules issued thereunder, i.e. the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "2021 IT Rules") and

the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 ("*2022 Amendment*").

### 3.2.1 Section 79 of the IT Act

Under Section 79 of the IT Act, intermediaries are provided safe harbour from prosecution for carrying illegal content posted or transmitted by third parties, subject to following a number of conditions. Intermediaries must act as a passive agents (or distributors) insofar as the illegal content is concerned, must observe "due diligence" conditions, and also disable access to unlawful content upon receiving "actual knowledge" thereof. The due diligence standards are elaborated under the Intermediary Rules, 2021, as amended in 2022. it is through these standards - and the proscription of obscenity, insults or harassment on the basis of gender, racially or ethnically objectionable - that elements of decency and morality (which are not part of the Section 69A framework) are brought in to censor content online.

Initially, the actual knowledge standard was interpreted as a simple notice and take down framework. Empirical research demonstrated that this was severely misused, and intermediaries would over-comply with requests and take down content, regardless of the relevance of the request.[41] Section 79(3)(b) was interpreted by the Supreme Court in Shreya Singhal v Union of India[42] to mean that intermediaries had to remove or disable access to information only after receiving a court order or based on notice from the government. Notice and take-down requests by users were not permitted since "*otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.*"

### 3.2.2 IT Rules, 2021 and 2022

At the outset, it is worth noting that the 2021 IT Rules and the 2022 amendments thereto, impose a range of broad obligations on intermediaries under the garb of "due diligence" guidelines.[43] These obligations go well beyond the scope of Section 79 of the IT Act and point to a disturbing trend of obligations being imposed through executive fiat rather than through statutory amendment following parliamentary debate.[44] The constitutionality of the 2021 IT Rules is currently pending adjudication before various High Courts in India. Apart from the challenge on merits, the petitions also raise questions about substantive changes being brought about through executive notification (without the benefit of legislative deliberation).

Rule 3(1)(b) of the 2021 Rules require intermediaries to insert provisions in their terms of use that informs users that they must not publish or host any content that breaches a list of proscribed content.[45] This provision has been subtly changed in the 2022 amend-

[41] Rishab Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet* (techspace rep, Centre for Internet and Society 2011).

[42] n 16.

[43] Bailey, Parsheera, and Rahman (n 3).

[44] Ibid.

[45] For example, content that: (i) is defamatory, obscene, pornographic, invasive of privacy, or racially and

ment, whereby intermediaries must now "make reasonable efforts" to prevent their users from publishing such content. Essentially, a provision requiring information be provided to users has been changed to a provision requiring intermediaries to take "reasonable" measures to filter proscribed content.

Following *Shreya Singhal*, Rule 3(1)(d) requires intermediaries to "expeditiously" take down proscribed content within 36 hours.

Rule 3(1)(j) requires intermediaries to provide "information or assistance" to any government agency within 72 hours. The phrase"information or assistance" is wide enough to include requests for interception, monitoring or decryption of communication, which are strictly governed by Section 69 of the IT Act 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (*"Surveillance Rules"*) notified thereunder. Thus, Rule 3(1)(j) expands the scope of electronic surveillance and gives a go-bye to the statutory framework envisaged by parliament.

Rule 3(2)(a) allows users to file a complaint against the violation of any of the provisions of the 2021 IT Rules, and requires intermediaries to acknowledge any complaint within 24 hours and dispose off the same within 15 days. This provision has also been amended by the 2022 Rules. Post the 2022 amendment, for certain specified types of content, the request for removal of information must be resolved within 72 hours.[46]

As per the newly introduced Rule 3A, the Central Government is to constitute (one or more) "Grievance Appellate Committee(s)" (GAC) to decide user appeals against the decision of social media intermediaries. The GAC shall be staffed by members of the executive – "*a chairperson and two whole time members appointed by the Central Government, of which one shall be a member ex-officio and two shall be independent members.*"

Rule 4(2) requires a "significant social media intermediary", which provides messaging services (such as WhatsApp) to identify the 'first originator' of messages based on a judicial order or order of a competent authority under Section 69 of the IT Act (concerning surveillance).

Under Rule 4(4) of the 2021 Rules, significant social media intermediary "shall endeavour" to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts explicit or implicit acts of rape, child sexual abuse or conduct. Intermediaries must implement mechanisms for appropriate human oversight of measures, including a periodic review of any automated tools. They must also evaluate these automated tools having regard to their accuracy and fairness, the propensity of bias and discrimination, and the impact on privacy and security of

ethnically objectionable; (ii) is misleading in nature; (iii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation.

[46]Under Rule 3(2)(a), the intermediary shall "*acknowledge the complaint within twenty-four hours and resolve such complaint within a period of fifteen days from the date of its receipt: Provided that the complaint in the nature of request for removal of information or communication link relating to clause (b) of sub-rule (1) of rule 3, except sub-clauses (i), (iv) and (ix), shall be acted upon as expeditiously as possible and shall be resolved within seventy-two hours of such reporting;*"

such tools.

## 3.3 Analysing the intermediary liability framework

There are various problems with the current intermediary framework that have cumulatively resulted in proactive censorship by intermediaries and excessive regulation by the government.[47] In this section, we analyse five such issues – the lack of any statutory distinction amongst different classes of intermediaries; the over-broad operation of the safe harbour framework; encouraging surveillance through the 2021 IT Rules; non-compliance with principles of natural justice before intermediaries take down user content; and, the creation of a government-linked Grievance Appellate Committee. These concerns exist in addition to the previously mentioned problem that the 2021 IT Rules were passed through executive notification despite bringing in substantive and broad changes to the intermediary liability framework.[48] Hence, any amendment to the IT Act must statutorily incorporate the substantive due diligence obligations imposed on intermediaries.

### 3.3.1 Lack of differentiation amongst intermediaries

The definition of an intermediary under Section 2(1)(w) of the IT Act is extremely wide. It brings within its ambit all service providers in the internet supply chain, including user-facing platforms such as social media websites and back-end services such as cloud service providers ("CSPs"). It also includes within its ambit, cyber cafes, payment apps, traditional e-commerce platforms, and search engines.

While all intermediaries are similar, in that they all provide users the ability to publish or consume content, they play different roles in the digital ecosystem and serve different markets. The impact of different intermediaries (and the types of harms) thus differ.

Section 79 imposes obligations in a broad manner, on all intermediaries without drawing any distinction based on the type of intermediary at hand. This can create practical problems. For instance, internet service providers and CSPs must comply with the same legal obligations cast on social media platforms under Section 79 of the IT Act and the 2021 IT Rules when it is extremely difficult for such intermediaries to undertake acts such as removing or blocking content, especially since CSPs may have to comply with bilateral confidentiality obligations.[49] Indeed, casting such obligations has cost, security and privacy implications in terms of forcing these intermediaries to scan all content on their platforms.

Similarly, the definition of a "social media intermediary" under Rule 2(1)(w) of the 2021 IT Rules is also very wide and brings within its ambit gaming and e-commerce platforms, as well as app stores.[50]

[47] Vrinda Bhandari and Anja Kovacs, *What's Sex Got to do with it? Mapping the Impact of Questions of Gender and Sexuality on the Evolution of the Digital Rights Landscape in India* (techspace rep, Internet Democracy Project 2021).

[48] LiveLaw vUnion of India, "Kerala High Court" (2021).

[49] Koan Advisories (n 29).

[50] Social media intermediaries are defined as intermediaries that "*primarily or solely enables online*

As explained above, such a broad framing is disproportionate since it casts similar and broad obligation on all service providers, regardless of the size and the effects on the ecosystem. Such broad framing ends up treating an online gaming intermediary in the same way as an e-commerce platform, without recognising the different markets in which they operate and the range of harms that need to be mitigated. It thus, may not pass the constitutional tests of necessity and narrow tailoring, in addition to creating practical problems.

Additionally, such a framing diverges from international best practice. For instance, under the UK Online Safety Bill, exclusions are carved out for specific user-generated content such as email services, SMS and MMS services. Additionally, the Bill exempts user-to-user services from the obligations under the law if the only way of communicating on the service is through comments or reviews posted or through expressing one's views through "likes or dislikes" button.[51] Paragraph 7 of the Bill also exempts "internal business services" from its purview and application, encompassing productivity and collaboration tools and business intranet.[52] Even under the proposed European Digital Services Act, there is a distinction drawn between intermediaries based on their size, role and impact on the online ecosystem.[53] The size of the intermediary at hand (based on say, user numbers) could be one significant factor in imposing additional obligations. As will be detailed in the subsequent section, distinction by size (which links to the increased relevance in the ecosystem and greater possibility of harm) is also relevant for a number of other obligations and duties under the IT Act, including for the purpose of cyber security incident reporting.

Hence, there may be a need for specialised interventions that apply to intermediaries, based on identified effects on the ecosystem, keeping in mind that classification should be simple and proportionate. However, there is a need to consider whether the safe harbour framework under Section 79 of the IT Act is the appropriate route to ameliorate the various problems seen in the digital ecosystem and implement additional duties that go beyond the purview of a content take down system. We suggest that additional obligations pertaining to safety, etc., of the online ecosystem should occur outside the ambit of the safe-harbour provision in the IT Act, and should be based on dealing with specifically identified harms. Notably, obligations such as that of implementing grievance redress mechanisms, increased transparency and reporting, or even competition-related interventions, etc., could be made applicable to bigger platforms, breach of which could lead to appropriate punitive action (outside the framework of intermediary liability issues). The safe harbour framework however must continue to apply to all intermediaries (who do not actively participate in commission of an offence, etc).

---

*interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services*".

[51] Clause 4(2) of Part 2 of the UK's Online Safety Bill. See Online Safety Bill, *Online Safety Bill: Explamatory Notes* (techspace rep, UK Parliament 2022)

[52] Ibid.

[53] DrNils Rauer and Wouter Seinen, "A guide for online intermediaries on the scope of the EU Digital Services Act" (2022) <https://www.pinsentmasons.com/out-law/guides/guide-digital-services-act-for-online-intermediaries>.

### 3.3.2 Privatising and broadening censorship through the safe harbour framework

Section 79 and the 2021 and 2022 IT Rules privatise censorship functions by passing the buck to intermediaries to serve as watchdogs over the content on their platform. This is particularly an issue in cases where intermediaries are made to police content that is not per se illegal, but is nevertheless proscribed. This includes ten broadly worded subjective categories such as content that is - in the opinion of the user or an intermediary - “ethnically objectionable”, “misleading in nature", “insulting other nation", “patently false and untrue” or “defamatory”.

This problem is exacerbated under the 2022 Amendment, which make two changes that further increase the censorship role of intermediaries. First, apart from prominently publishing their policies and user agreements on their websites, under the amended Rule 3(1)(a), intermediaries must also “ensure compliance of the same." There is no clarity on how such compliance is to be achieved, and whether it requires proactive removal of content.

Second, the obligation of the intermediaries under Rule 3(1)(b) has changed to making “reasonable efforts" to “cause" the users not to upload content that is covered under the ten categories. This changes the obligation from monitoring compliance based on government requests, court orders, and user complaints to proactively removing content (through automated content moderation and algorithmic tools). The combined impact of these amendments is to further incentivise intermediaries to censor content (failing which they will be held denied the protection of safe harbour under Section 79).

The manner in which the safe harbour framework is crafted implies that intermediaries are under a constant fear of being hit by criminal sanction to ensure user compliance with terms of service. This makes them gatekeepers of the “correct” type of content online.[54]

Encouraging intermediaries to proactively police their platforms and remove content that is considered unacceptable results in facilitating over-censorship and restricting free speech.[55] This is especially because intermediaries function under the ever-present threat of criminal liability, which threat is more pronounced for significant social media intermediaries whose Chief Compliance Officers can be held personally criminally liable. Under such constraints, intermediaries are forced to judge – and now take down – impugned content which is defamatory, obscene, privacy-invading, or patently false. This is different from policing compliance with their own terms of service, which has other issues concerning transparency, accountability, and consistent decision making.

It is worth considering whether criminal liability should be imposed on intermediaries in the first place, instead of focusing on heavy civil penalties and fines. There have been arguments to remove criminal liability for intermediaries, including because it impacts the ease of doing business.[56] This is an important issue that requires consideration.

[54] Apar Gupta and others, “IFF’s Submission to the Proposed Draft Amendment to the IT Rules, 2021” (2022) <https://drive.google.com/file/d/1wamOJoj_jGNOwMzlR62nKj4t0tKp1BM1/view>.

[55] Bhandari and Kovacs (n 47).

[56] Neelanjana Sharma, “Impact of Criminalising Provisions on Ease of Doing Digital Business in India” (2022).

One may argue that the wholesale imposition of criminal liability – regardless of whether there is a minor infraction (such as failing to respond to law enforcement agencies in 72 hours) or a major infraction (such as allowing child sexual abuse material remaining online) - is problematic. Criminal liability, if any, must only be imposed after ascertaining the wilful and intentional nature of an intermediary's conduct (in contributing towards a specific offence). As a general rule, criminal liability for failing to adhere to procedural regulations should be avoided.

As mentioned above, the Supreme Court in *Shreya Singhal* read down Section 79(3)(b) to avoid a situation where private intermediaries were placed in a situation where they would need to adjudicate on permissible speech. However, Rules 3(2)(b) and 4(4) overrule the judgement by requiring the intermediaries to exercise their own judgment to take down certain kinds of information (which exposes the private area of an individual or shows them in full or partial nudity) on receiving a complaint from such individual, instead of receiving actual knowledge in the form of a court order or a blocking order.

The general trend of the government has been to make intermediaries more accountable for content moderation (e.g. through Rule 3(2)(b)). This follows the signals provided by the Supreme Court, which have directed intermediaries to proactively block content in specific cases relating to pornography (*Kamlesh Vaswani*), circulation of videos of gang rapes (*In re Prajwala*), and pre-natal advertising (*Sabu Mathew*).[57] It is also in line with global trends such as in Australia, where the criminal law was amended to introduce heavy penalties on content and hosting services for failure to notify the police about, and expeditiously remove 'abhorrent violent material'[58] and Singapore (where the government widened censorship powers through the regulation of fake news).[59]

When an obligation is placed on intermediaries to make online systems safer, it can result in relying on algorithms, at the cost of human moderation. This can have unintended consequences. OFCOM has identified challenges in online AI moderation including a lack of transparency of decision making, the possibility of unchecked bias creeping in, and most importantly, the algorithm's inability to review content based on context.[60] These problems were illustrated recently when Google flagged the account of a man who took a photo of his son's swollen penis for uploading on his healthcare provider's portal as circulating child sexual abuse content.[61]

### 3.3.3 Encouraging surveillance

As explained above, under Rule 3(1)(j), intermediaries can be asked to provide "information or assistance" which is in the form of interception. This sidesteps the procedural

[57] For more details, see Bhandari and Kovacs (n 47)

[58] Govt of Australia, "Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act" (2019) <https://www.legislation.gov.au/Details/C2019A00038>.

[59] Mary Hui, "Singapore's fake news law is facing its first real challenge in court" (2020) <https://qz.com/1784632/%20singapore-faces-legal-challenge-over-fake-news-law/>.

[60] Ofcom, *Use of AI in Online Content Moderation* (techspace rep, 2019).

[61] Kashmir Hill, "A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal" (2022) <https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html>.

safeguards that have been built into the surveillance framework under Section 69 of the IT Act.

Further, under Section 69(3) of the IT Act and the notified Surveillance Rules, the obligation of intermediaries is limited to providing "technical assistance." As we discuss in subsequent sections pertaining to surveillance, such an interpretation should not extend to creating backdoors to encrypted products and services.[62] However, Rule 4(2)'s requirement to identify the 'first originator", in so far as it requires modifications to the technical design of encrypted platforms, enables traceability. This is beyond the scope of either Section 69 or 79 of the IT Act 2000, apart from raising serious free speech and privacy concerns.

In any event, the power to prescribe encryption standards and methods originates from Section 84A and not Section 79, which is a safe harbour provision. Thus, it should not be included as part of the intermediary rules issued under Section 79.

### 3.3.4 Violation of principles of natural justice

Currently, the 2021 IT Rules fail to comply with principles of natural justice and due process. This is particularly so in the case of Rule 3(2)(a), which violates the *Shreya Singhal* judgment by re-introducing a user complaint/notice and take down framework. Rule 3(2)(a) allows users and third parties to complain about content posted on an intermediary's platform and the intermediary must decide such complaint within 15 days.

Post the 2022 amendment, Rule 3(2)(a) requires that for most content, the user complaint must be resolved by the intermediary expeditiously within 72 hours. Such short timelines will only increase concerns of arbitrary decision making, while also posing a significant cost for intermediaries.[63] To be kept in mind that compliance costs are generally easier to internalise for larger intermediaries, implying that such requirements could actually increase barriers to entry in the digital ecosystem.

In addition, there is no requirement for the intermediary to hear the the original content creator, whose content has been impugned in the complaint while making a decision on a user complaint. As the recent debate surrounding the sudden automated take down and silent restoration of the Instagram post by @cringeactivist showing a man worshipping a statute of the U.P. Chief Minister Adityanath demonstrates, individuals often have no knowledge about the reason for take down.[64] Through the 2022 Amendment, the government has now provided a right to appeal, but as we explain below, it is extremely problematic.

If intermediaries are being made to serve as "proxy censors" and adjudicate the desirability of user-generated content, then their interests towards protecting themselves from legal consequences are in conflict with a user's interest in retaining the post on her account.[65] Hence, strict natural justice principles have to be built to provide users with a

[62] Bailey, Bhandari, and Rahman (n 6).

[63] Gupta and others (n 54).

[64] Scroll Staff, "Meta vs The Wire: Instagram restores satirical post on Adityanath" (October 2022) <https://scroll.in/latest/1035326/meta-vs-the-wire-instagram-restores-satirical-post-on-adityanath>.

[65] Seth Kreimer, "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem

hearing prior to, or after, their post is taken down.

### 3.3.5 Government interference via the Grievance Appellate Committee

There are various problems with the constitution of the GAC under Rule 3A of the 2022 Rules. First, it results in government control of content online and increases censorship powers. The GAC body does not have any institutional independence and there are no provisions to ensure its independence (in terms of establishing independent financing and appointment processes, etc.).[66]

Second, details concerning the appointment process, qualifications of members of GAC, their powers (to summon documents and persons), their obligation to publish their decisions online, are absent from the law. There is no clarity whether intermediaries and content creators will have a *right* to be heard and to lead evidence. The law is completely silent about how the GACs will manage the transaction and volume-intensive discretionary exercise, that requires proper state capacity.[67]

Third, there are concerns around excessive delegation since the government has used its executive powers to establish an entire appellate grievance redress mechanism, thereby bypassing Parliament.[68]

Fourth, related to the above, the constitution of the GAC represents an attempt to bypass the statutory remedy of blocking that is available under Section 69A of the IT Act, which allows aggrieved users to seek take down of content online.

## 3.4 Recommendations

Section 79 of the IT Act proactively encourages private censorship by intermediaries through its broad due diligence obligations and the explicit threat of revoking safe harbour for intermediaries. Based on the discussion above, we suggest various revisions to the Section 79 framework.

### 3.4.1 Statutory reform: Section 2(1)(w), IT Act

Any classification system for intermediaries should be simple and easy to apply. Arbitrary, narrowly defined classification of services in a rapidly changing digital space risks being outdated quickly, as well as fragmenting the industry/sector. There is a need for principles-based, systems-based, and outcomes-based regulation that providing sufficient flexibility for tech companies to innovate and respond in a way that is in the best interest of their user communities; respects user rights, including free speech and safety; and ensures a positive user experience.

---

of the Weakest Link" [2006] (11) Univ. of Penn. L. Rev. 11.

[66] Rishab Bailey and Smriti Parsheera, *Comments on the Proposed Draft Amendments to the IT Rules, 2021* (techspace rep, xKDR Forum 2022).

[67] Lant Pritchett and Michael Woolcock, *Solutions when the Solution is the Problem: Arraying the Disarray in Development* (techspace rep, Center for Global Development Working Paper No 10 2020).

[68] Vrinda Bhandari, "Regulating Information Technology Intermediaries: Tragedy of Government Control of Grievance Redressal" (December 2022) <https://tinyurl.com/2ztt3yya>.

A clear method of classification of intermediaries would be based on size. This would implement additional obligations on larger platforms, with a greater reach, and hence, greater impact. For instance, the European Digital Services Act imposes additional duties on platforms that have a wide reach, which has been stipulated to be a platform with over 45 million users. In Germany, the NetzDG law places additional obligations on social network platforms with over 2 million users, requiring such platforms to take down content deemed to be "manifestly unlawful" within 24 hours.[69] The 2021 IT Rules have already imposed a threshold criteria to classify only those platforms with over 50 lakh registered users in India as 'significant social media intermediaries'.[70]

Further, additional obligations on platforms pertaining to issues such as implementing grievance redress mechanisms, ensuring greater transparency, etc., should be implemented outside the ambit of Section 79. Rather than linking safe-harbour to the commission/omission of several unconnected duties, separate, co-regulatory models should be created to deal with specifically identified problems.

### 3.4.2 Statutory reform: IT Rules, 2021

Based on the concerns highlighted above, the following amendments are proposed to the 2021 IT Rules

1. **Rule 3(1)(b)**: Intermediaries have the discretion to formulate their own terms of service that determines how they want to police their platform. They must be permitted to adopt their own terms of service and a differential standard, as long as they comply with applicable law in force.

   However, any legal obligations that are imposed on intermediaries to censor and take down content through Rule 3(1)(b) read with Rule 3(2) and Rule 7 should be narrowly tailored. Thus, the list of proscribed categories in Rule 3(1)(b) should be narrowly tailored to only include those categories that are illegal/unlawful. Thus, ambiguous and vague terms such as "ethnically objectionable", "misleading in nature", "insulting other nation", and "patently false and untrue" (which were not present in the original 2011 version of the IT Rules, upheld by the Court in *Shreya Singhal*) should be removed. It should be kept in mind that the list of proscribed information under this provision includes various categories of information that are not illegal under any substantive law in force.

   *Requiring* intermediaries to decide whether any content is violative of the "law in force" contravenes the dictum in *Shreya Singhal* that intermediaries must not be put in a position to decide what is lawful and unlawful. Such a role should be left to government agencies or the courts.

2. **Rule 3(1)(j)**: It should be clarified that if the "information or assistance" sought from the intermediaries under Rule 3(1)(j) of the 2021 IT Rules extends to assisting in interception, monitoring, or decryption, then the law enforcement agency must comply with the surveillance framework under Section 69 of the IT Act and the

[69] Koan Advisories (n 29).
[70] MeitY, "Notification No. SO 942(E)" (February 2021) <https://tinyurl.com/2v4pw6sa>.

Surveillance Rules. The government should not be allowed to bypass the procedural safeguards embedded in the surveillance framework (however measly they may be) by relying on the 2021 IT Rules.

3. **Rule 3(2)(a)**: The 2021 IT Rules need to be amended to provide a statutory right of hearing to content creators before their post is taken down by an intermediary, based on a user complaint. Further, the user should be allowed to file an appeal against this order and receive a decision within a time-bound framework. As content moderation is increasingly becoming automated, it is important for us to highlight the importance of human beings mediating such interactions to prevent context-neutral and algorithmic morality-based governance.

4. **Rule 4(2)**: It should be clarified that enabling the identification of the first originator on popular messaging services under Rule 4(2) should not be interpreted as requiring companies to create a backdoor or break their end-to-end encryption or "fingerprint" each message. Rule 4(2) should be subject to the technical limitations of the particular social media platform/app, and should not weaken encryption (or reduce the privacy and data security of users) in any manner.

### 3.4.3 Institutional reform

The current focus of Section 79 of the IT Act is to link compliance with the provisions of the 2021 IT Rules with safe harbour. This creates an incentive for intermediaries to over-censor content. This will eventually result in a loss of speech in the ecosystem, both through proactive enforcement and self-imposed censorship (caused by a chilling effect).

Currently, intermediary regulation can take the form of two extremes. The laissez faire approach, exemplified by the text of Section 230 of the U.S. Communications Decency Act, may not work in today's reality, where social media platforms exert enormous concentrated power.[71] The Indian experience is the converse, with the government playing a heavy hand in regulation, set to get worse with the 2022 amendments to the 2021 IT Rules.

Hence, the government should examine whether a co-regulatory model of regulation of online content is feasible and desirable, particularly since it would reduce the risk associated with intrusive and far-reaching state regulation, while clamping down on intermediary inaction. It would also allow for, and facilitate, industry dialogue and collaboration to help define workable solutions. Co-regulatory models would also possibly enable greater 'buy-in' from businesses. The difficulty lies in drawing the correct balance between self-regulation and governmental intervention.

A co-regulatory model could include codes of practice where intermediaries would have more flexibility to adapt and change, as risks change on different platforms/services.

Essentially, the government's level of regulation is restricted to *ensuring* the presence

[71] Ellen P Goodman and Ryan Whittington, *Section 230 of the Communications Decency Act and the Future of Online Speech* (techspace rep, Rutgers Law School Research Paper 2019); Michael D Smith and Marshall Van Alstyne, "It's Time to Update Section 230" (August 2015) <https://hbr.org/2021/08/its-time-to-update-section-230>.

of transparency and content removal policies of intermediaries. Under such a regime, intermediaries will be tasked with establishing effective and efficient grievance redress mechanisms. Government can ensure the enforcement of such models through the provision of civil penalties (but not the loss of safe harbour). Thus, unlike the 2022 Rules, the government will not be in any position to influence the content posted on social media or re-evaluate the intermediary's decision. However, it can ensure that various intermediaries set up different grievance redress mechanism. Such level of governmental oversight is actually welcome.[72] The biggest advantage of this model is that it removes the involvement of the government from any decision regarding the content posted online, and further reduces the risk of excessive state intervention in a "risk based, proportionate manner".[73]

# 4 Surveillance

**Summary of recommendations**

The IT Act framework pertaining to surveillance requires significant revision, having been framed prior to the recognition of privacy as a fundamental right, and in an era when the digital ecosystem was not as pervasive as today. The framework provides extremely broad powers to the executive, with insufficient checks against misuse. It is also inadequate to deal with new developments in the digital ecosystem such as the use of end-to-end encryption. We therefore recommend:

- A comprehensive surveillance framework be implemented in the form of a new legislation. This could streamline and harmonise surveillance practices, while creating appropriate institutional frameworks for oversight.
- In the alternative, the provisions in the IT Act (or indeed the proposed Telecommunications Bill, 2022) must be revised.
- The scope of executive authority under Sections 69, 69B, 67C, must be narrowed, in accordance with norms of necessity and proportionality
- Statutory safeguards over surveillance practices must be provided for in the form of prior judicial authorisation for surveillance, greater transparency and accountability of law enforcement entities including through appropriate oversight, implementation of accessible grievance redress mechanisms, bar on illegally collected evidence, etc.
- The legislation should bar practices such as mass surveillance or the creation of systemic weaknesses in platforms for the purpose of surveillance.

## 4.1 Background

The growth of the digital ecosystem has introduced new avenues for the State to carry out invasive surveillance over citizens.[74] The State can now access a vast quantity of data

[72] Bailey and Parsheera (n 66).

[73] Rishab Bailey and Vrinda Bhandari, *Towards holistic regulation of online hate speech* (techspace rep, IT For Change 2021).

[74] The term 'surveillance' is used broadly to indicate the ability of the State to access information about individuals, whether by intercepting communications or accessing stored data.

on citizens - either directly or through intermediaries. While States require the ability to carry out surveillance over individuals in order to meet various public interest goals such as preventing crime, they must also protect and promote fundamental rights.[75] Ensuring a proper balance between the competing interests is therefore essential.

It is commonly accepted that the current surveillance framework under the IT Act is unfit for purpose, having been put in place in 2000 when the digital ecosystem in India was still at a nascent phase. The recognition of privacy as a fundamental right in *Supreme Court of India*[76] ("*Puttaswamy*") also makes it necessary to re-calibrate the existing framework. Accordingly, this section examines provisions in the IT Act pertaining to the State's surveillance powers, and makes recommendations for revision.

We point to four main weaknesses in the current regime under the IT Act: (a) over-broad surveillance powers (which are only increasing in scope pursuant to new obligations being introduced through the mechanism of rules), (b) excessive executive authority with no statutory checks and balances on state powers, (c) no transparency and accountability in surveillance processes, and (d) no incentive for LEAs to follow due process. We therefore recommend revision of the surveillance framework, ideally in the form of a specific surveillance related law. In the alternative, we suggest revisions to the IT Act, including for instance, implementing various checks and balances such as ensuring judicial oversight of surveillance.

## 4.2 Statutory framework

The IT Act empowers the government to carry out surveillance under two main provisions - Section 69 and Section 69B.[77] We examine these provisions and the rules issued under each, below.

### 4.2.1 Section 69

Section 69 empowers the Central or State Government to, through a written order, direct "any government agency" to intercept, monitor or decrypt information transmitted through or stored in a computer resource, where it is "necessary or expedient" to do so on certain specified grounds.[78] Intermediaries are required to provide all technical assistance and facilities to enable such interception or monitoring, failing which they can face

[75] Unchecked surveillance can chill the exercise of fundamental rights, force behavioural change, enable discrimination, or selective enforcement of laws, thereby eroding democratic norms (Neil Richards, "The Dangers of Surveillance" [2013] Harvard Law Review 1934).

[76] n 4.

[77] Sections 28 and 29 of the IT Act also provide powers of surveillance. These permit the Controller of Certifying Authorities or authorised officials to investigate breach of any provisions of the IT Act, and access computer systems to carry out investigations for breach of Chapter VI of the Act (pertaining to certifying authorities) respectively. These provisions have been used to call for information from intermediaries in the past (Ministry of Communications and Information Technology, "India's surveillance state: Other provisions of law that enable collection of user information" (December 2015) <https://bit.ly/2yWZXzZ>). However, they are excluded from the scope of this study.

[78] These are in the interest of the sovereignty or 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 relating to above or for investigation of any offence.

criminal liability.

The procedural framework for using the powers under Section 69 is laid out in the Surveillance Rules issued in 2009.[79] These rules are based largely on Section 419A of the Indian Telegraph Rules, 1951, which implements procedural guidelines laid down in *PUCL vUnion of India*[80]. The rules envisage a system of executive authorisation and oversight over surveillance processes. Authorisation for surveillance can only be granted by a Competent Authority, which must also record its reasons for doing so.[81] The Competent Authority can also notify any agency of the government to carry out surveillance.[82] All directions for surveillance are to be scrutinised by a Review Committee comprising three high-ranking government officials.[83]

The Surveillance Rules also prescribe additional safeguards against misuse, including:

- A requirement for alternative measures to be considered.
- Limiting the period of surveillance to 60 days, extendable to a total of 180 days.
- A requirement for intermediaries to verify interception orders, and maintain secrecy of intercepted communications.
- Intermediaries can only be required to decrypt an encrypted message where it has control of the decryption key or where it has encrypted the information itself.

### 4.2.2 Section 69B

Section 69B empowers the Central Government to authorise any government agency to monitor and collect information from computer resources to "enhance cyber security", or

[79]The Ministry of Home Affairs has also issued Standard Operating Procedures (SOPs), which lay down certain additional processes to be followed by LEAs and intermediaries. These SOPs relate to issues such as the manner in which directions will be issued to service providers, the nature of information that can be called for and methods of validation of interception requests (Shalini Singh, "Centre issues new guidelines for phone interception" (January 2014) <https://www.thehindu.com/news/national/centre-issues-new-guidelines-for-phone-interception/article5559460.ece>; Internet Freedom Foundation, "Centre issues new guidelines for phone interception" (March 2019) <https://internetfreedom.in/revealed-secret-operating-procedure-followed-by-the-govt-for-digital-snooping/>).

[80]PUCL vUnion of India, "Supreme Court of India" (December 2016) <https://indiankanoon.org/doc/31276692/>.

[81]The 'Competent Authority' is a Secretary in the Ministry of Home Affairs (in the case of the central government) or the Secretary in charge of the Home Department (in case of a State Government or Union territory). In "unavoidable circumstances" an order may be passed by an officer not below the rank of Joint Secretary to the Government of India, who has been duly authorised by the Union Home Secretary (or equivalent officer at state level). In emergency situations, surveillance can be carried out with the prior approval of the head or the second most senior officer of the relevant LEA. The competent authority must be informed of the issuance of such an order within three working days, and confirmed within seven working days.

[82]Ten central agencies have been empowered to carry out surveillance under this provision (Ministry of Home Affairs, "Order of the Cyber and Information Security Division" (December 2018) <https://egazette.nic.in/WriteReadData/2018/194066.pdf>)

[83]The Review Committee, established under Rule 419A of the Telegraph Rules, 1951, is required to meet at least once in two months to scrutinise the legality of surveillance orders. In case of any infirmities, surveillance must be discontinued and intercepted communications must be destroyed.

identify, analyse or prevent intrusions or spread of computer contaminants. This power can be used to intercept "traffic data", defined to include metadata, thereby enabling access to personal information of individuals.

The processes for collecting information under Section 69B are prescribed in the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (*"2009 Traffic Rules"*), which lay down authorisation processes and safeguards similar to that under the Surveillance Rules. To date, only CERT-in has been empowered under this provision.[84]

### 4.2.3 Section 67C

Section 67C empowers the government to prescribe data retention standards to be followed by intermediaries, breach of which can attract criminal liability.

Data retention norms enable surveillance as they mandate storage of user data. They can also impose costs on intermediaries, while subjecting users to the possibility of privacy harms arising from the misuse of stored data.

The government has issued rules pertaining to retention of information by digi-locker providers under this section, and has considered issuing regulations applicable to other intermediaries, though none have yet been notified.[85]

### 4.2.4 Obligations imposed through Rules

Various rules issued under the IT Act enable LEAs to carry out surveillance. Notably:

- Rule 6(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (*"Security Rules"*) authorises the disclosure of personal data by a body corporate to government agencies for the purpose of identity verification, crime prevention or the prosecution of offences. A request for any information under this provision, must be in writing.
- Rule 7 of the Information Technology (Guidelines for Cyber Cafe) Rules, 2011, (*"Cyber Cafe Rules"*) requires cyber cafes to provide "any necessary information" to authorised officers conducting an inspection. This can include information such as the browsing histories of individuals, which cyber cafes are required to retain.
- The 2021 IT Rules grant safe harbour to intermediaries *inter alia* if they follow appropriate "due diligence" as prescribed. Obligations in this respect include the need to retain information connected to any blocked content, as may be required for the purposes of an investigation,[86] and a requirement to retain identification of users for a period of 180 days following the end of the relationship between the

[84] Ministry of Communications and Information Technology, "Notification of the Department of Electronics and Information Technology" (April 2016) <https://bit.ly/3SzPNca>.

[85] Asheeta Regidi, "The Indian Government Proposes New Data Retention Rules: Will Privacy be Compromised?" (October 2016) <https://www.firstpost.com/tech/news-analysis/the-indian-government-proposes-new-data-retention-rules-will-privacy-be-compromised-3690439.html>.

[86] This information must be retained for 180 days or such other period as notified by a judicial authority or LEA

parties, if such information is collected. As discussed in previous sections, intermediaries must also provide appropriate information and assistance to government agencies in a time bound manner. Further, they require "significant social media intermediaries" providing messaging services to enable traceability of users on their platform, subject to a court order or direction under Section 69.[87]

## 4.3 Analysing the Surveillance Framework under the IT Act

In *Puttaswamy*, the Supreme Court prescribed a four-part test to examine the constitutionality of any interference with the fundamental right to privacy.[88]. Any interference with privacy rights must:

- Be permitted by law
- Meet a legitimate State aim
- Be proportionate, i.e. there must be a rational nexus between the goals and ends adopted, the extent of interference must be proportionate and necessary to meet the stated aim or be the least intrusive means to meet the end.
- Be fettered by safeguards to prevent against abuse

We discuss whether the surveillance framework under the IT Act meets these tests below.

### 4.3.1 Interception and Monitoring

Surveillance when carried out under Section 69 or Section 69B is prescribed by law, thus satisfying the test of legality. Insofar as Section 69 authorises use of powers to meet the goals of maintaining "the sovereignty or integrity of India", "security of the State", "friendly relations with foreign States", "public order", and "for preventing incitement to the commission of any cognizable offence relating to above" it is clear that these are all legitimate State aims, notably being related to Article 19(2) of the Constitution. Similarly, Section 69B also targets legitimate state goals viz. ensuring safety and security of cyber resources from viruses and other computer contaminants.

However, Section 69 does not meet the proportionality test laid down in *Puttaswamy* as:

- it does not require the tests of "public safety" or "public emergency" to be met. This lowers the standard for invocation of powers by the government.[89] Given that the use of surveillance powers is an significant intrusion into individual rights,

[87] Such an order can be passed on the grounds specified in Article 19(2) or in relation to offences of rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years. This provision also contains certain safeguards - alternative, less intrusive methods must be considered prior to invocation of this power, contents of communications or information related to other uses must not be disclosed

[88] Vrinda Bhandari and others, "An analysis of Puttaswamy: the Supreme Court's privacy verdict" (September 2017) <https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html>.

[89] Bharat Vasani, Ramgovind Kuruppath, and Samiksha Pednekar, "Surveillance in the Post-Puttaswamy Era" (November 2019) <https://corporate.cyrilamarchandblogs.com/2019/11/surveillance-post-puttaswamy-era-right-to-privacy/>; Bailey and others, *Use of personal data by intelligence and law enforcement agencies* (n 5).

any provision conferring such powers should be narrowly tailored. Notably, these phrases are used in the Telegraph Act, and have also been retained in the draft Telecommunications Bill, 2018.

- it uses the phrase "defence of India", which is not found in Article 19(2) of the Constitution, and is undefined and vague.[90] Given that Section 69 already allows the invocation of powers to protect the "sovereignty and integrity of India" or to ensure "security of the state" - phrases pertaining to which jurisprudence has developed - it is unclear why this third phrase is required.

- it uses the broad phrase "investigation of any offence".[91] This enables surveillance even for small offences. While there is a compelling state interest in crime prevention, preventing misdemeanours or civil wrongs may not require the use of a similarly intrusive power.[92]

- it uses the test of necessity and expedience as preconditions for invocation of surveillance powers. As discussed in Section 2.4.2, the expedience test is vague and sets an extremely low bar which can provide an easy justification for invocation of this provision.[93]

Section 69B suffers from similar shortcomings. It enables personal data to be collected under the low bar of *enhancing* cybersecurity. This is vague, capable of arbitrary use and therefore in violation of the principle of narrow tailoring.[94]

While the Surveillance Rules and Traffic Rules accord with the guidelines laid down in PUCL vUnion of India,[95] they are insufficient in the context of modern day surveillance.[96] The procedural framework fails the proportionality and safeguards tests in *Puttaswamy* as:

- The safeguards are subject to executive discretion, limiting the ability of other organs of the State to check abuse. There is also no requirement for independent (ex-ante) authorisation or (ex-post) oversight of surveillance practices, thereby limiting accountability.[98] The executive is essentially given "unlimited discretion" in matters of surveillance, which violates the proportionality principle.[100] It is notable that the Supreme Court itself has recognised the importance of judicial oversight in

[90] This phrase is also absent in the Telegraph Act.

[91] This phrase is absent in the Telegraph Act.

[92] Rishab Bailey and others, "Comments on the draft Personal Data Protection Bill, 2019" (April 2020) <https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data.html>.

[93] Ibid; S Rangarajan vPJagjivan Ram, "Supreme Court of India" (March 1989) <https://indiankanoon.org/doc/341773/>.

[94] The fact that "any" government agency (as opposed only to agencies tasked with maintaining network security) can be authorised to act under this provision is also a power that could be misused.

[95] n 80.

[96] The Supreme Court had envisaged the guidelines in PUCL vUnion of India[97] to be a "temporary solution".

[98] The Bombay High Court noted in Bombay High Court[99] that effective review of surveillance practices would have prevented harm being caused to the petitioner.

[100] Vrinda Bhandari and Karan Lahiri, "The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World" (2020) 15 Oxford Human Rights Hub Journal 15.

cases where surveillance may be possible.[101] Judicial authorisation is also recommended by the Committee of Experts chaired by Justice B.N. Srikrishna ("Srikrishna Commmittee").[103]

- There is little information provided to any independent authority, Parliament or the public, on the nature and number of surveillance requests, the mechanisms used to carry out surveillance, etc. Not only do LEAs function under a veil of secrecy, intermediaries are also prohibited from disclosing any information pertaining to surveillance requests. This, combined with the lack of oversight increases the possibility of abuse.[104]

- Oversight by the Review Committee does not account for the number of orders being issued and the capacity of the committee to conduct effective scrutiny.[105] Scrutiny of surveillance practices is a highly resource intensive exercise, requiring application of mind in each individual case.[106]The existing system of oversight is therefore virtually pointless, with the Srikrishna Committee terming their functions as "unrealistic".[107]

- There is no requirement for notice to be provided to the individual concerned, even after surveillance activities have been stopped. This enables surveillance to be conducted entirely in secret and denies individuals the chance to access remedies against State excesses. The absence of a specific grievance redress mechanisms also limits the avenues of recourse. As illustrated in A.1, various foreign jurisdictions notably Australia and Canada, require such notice to be provided to the individual concerned.

- While no country can be said to have a perfect system of safeguards or oversight in place, India lags considerably when compared to international precedent.[108] As illustrated in A.1, a number of countries implement a system of independent, judicial authorisation for surveillance requests. Each country also adopts multiple mechanisms for review and oversight of surveillance activities, including in the form of scrutiny by the legislature or independent authorities. Previous efforts to regulate surveillance activities in India also suggest similar mechanisms.

- Evidence that is procured illegally, that is, without following the processes laid

[101]The Supreme Court struck down Section 33(2) of the Aadhaar Act in Justice KSPuttaswamy vUnion of India[102] on the grounds that disclosure of biometric or demographic information on grounds of national security, at the discretion of a Joint Secretary was unconstitutional. Prevention of misuse of this power required an application of "judicial mind".

[103]Committee of Experts under the Chairmanship of Justice BNSrikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (techspace rep, MEITY 2018).

[104]In this context, the Srikrishna Committee notes that "Periodic review alone can ensure that the personal data sought was indeed used for a legitimate national security purpose and not otherwise" (ibid).

[105]As per a Right to Information Request, an average of 7500 - 9000 telephone-interception orders are issued by the central government each month (Ministry of Communications and Information Technology, "India's surveillance state: Other provisions of law that enable collection of user information" [n 77]). This number would only have increased with time - though no updated information is available in this respect.

[106]Bailey and others, *Use of personal data by intelligence and law enforcement agencies* (n 5).

[107]Committee of Experts under the Chairmanship of Justice BNSrikrishna (n 103).

[108]Ibid.

down in the Surveillance Rules, can be admitted in court. This does not create incentives for LEAs to follow due process.[109] While Indian courts typically admit evidence based only on relevance, this has recently been called into question in the context of surveillance by the Bombay High Court. In *Vinit Kumar v. Central Bureau of Investigation* the Court held that messages intercepted by the Central Bureau of Investigation could not be admitted in evidence as the interception was outside the scope of the legal regime under the Telegraph Act.[110] It may also be noted that various foreign jurisdictions, such as the US also adopt a "fruit of the poisoned tree" doctrine where illegally acquired evidence cannot be relied upon in court.[111] A similar provision can be found in the Personal Data and Information Privacy Code Bill, 2019, a private members bill introduced in the Indian parliament in 2019.[112]

- Criminal liability is imposed on intermediaries, including for failing to provide assistance within relatively short time frames. This reduces the chances that an intermediary can 'push-back' against any illegal surveillance orders, thereby removing a possible check on misuse of surveillance powers.[113]

To be noted that Section 69, amongst other provisions of the IT Act are currently under challenge in the Supreme Court in petitions that *inter alia* allege misuse of Pegasus software by the government and seek broad reform to the government's surveillance powers.[114]

### 4.3.2 Data Retention

Digital trails can reveal detailed information on users and are critical in investigating computer related offences. Accordingly, there may be a need to impose data retention mandates on intermediaries. However, the imposition of broad retention mandates could be considered problematic as they:[115]

[109] Bailey and others, *Use of personal data by intelligence and law enforcement agencies* (n 5); Kishita Gupta, "Understanding the doctrine of the fruit of the poisonous tree" (September 2021) <https://blog.ipleaders.in/understanding-doctrine-fruit-poisonous-tree/#Recommendations_of_the_94th_Law_Commission_Report>; Bhandari and Lahiri (n 100).

[110] The Court ordered the illegally intercepted communications to be destroyed.

[111] Gupta (n 109).

[112] Refer Section 29(5) of the Personal Data and Information Privacy Code Bill, 2019

[113] Telecom service providers have previously written to the Department of Telecommunications alleging that call data records were being called for in bulk, in contravention of established SOPs (TNM Staff, "Telcos say govt demanding call data records of all users, flags possible surveillance" (March 2020) <https://www.thenewsminute.com/article/telcos-say-govt-demanding-call-data-records-all-users-flags-possible-surveillance-120559>; Internet Freedom Foundation, "Mass Surveillance? You decide as per DoT's RTI responses" (June 2020) <https://internetfreedom.in/bulk-cdr-mass-surveillance/>).

[114] ML Sharma vUnion of India, "Supreme Court of India" (July 2021) <https://main.sci.gov.in/pdf/LU/27102021_082008.pdf>; Supreme Court Observer, "Pegasus Spyware Probe" (September 2022) <https://www.scobserver.in/cases/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-case-background/>.

[115] Cynthia Wong and Erica Newland, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development" (October 2011) <https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention_Long_Paper.pdf>.

- violate the presumption of innocence, as they require data of all individuals to be stored
- invade the right to privacy and chill right of expression
- create new privacy risks by exposing the stored data of users to malicious use
- impose costs on intermediaries to store unnecessary data, thereby limiting innovation and market entry
- hinder law enforcement by increasing the amount of low value data as compared to high value data

These problems are particularly noteworthy in the context of Section 67C, as the provision gives the government a free hand to specify any data be retained for any period of time, for any purpose. The provision therefore fails to meet the Puttaswamy tests of compelling state interest, proportionality and of implementing appropriate safeguards.

Retention norms under the 2021 IT Rules, the Cyber Cafe Rules and telecom licenses also cast broad obligations on intermediaries, with insufficient checks against misuse.[116] For example the 2021 IT Rules:

- cast a general data retention obligation following the curtailment of the user-intermediary relationship. There is no specific purpose to this requirement, other than the possibility that a user may have committed an offence at some point of time.
- permit LEAs to extend the retention period for information pertaining to investigation of an offence, indefinitely, and with no oversight or safeguards.

International experience on the issue of data retention norms is mixed.

In Europe, the European Court of Justice (CJEU) has struck down generic data retention mandates as being over-broad and disproportionate.[117] Retention is only permitted on a targeted basis for a necessary period of time.[118]

[116]The telecom licenses require service providers to retain IP details, log-in/log-out details and other such data for a period of two years (PTI, "Govt mandates telcos to keep call data, internet usage record for minimum 2 years" (December 2021) <https://economictimes.indiatimes.com/industry/telecom/telecom-news/govt-mandates-telcos-to-keep-call-data-internet-usage-record-for-minimum-2-years/articleshow/88469705.cms?from=mdr>). The retention mandates under licenses have no basis in law and as such, are susceptible to constitutional challenge on this ground alone.

[117]The CJEU struck down a general Data Retention Directive in 2014 (Court of Justice of the European Union, "The Court of Justice declares the Data Retention Directive to be invalid" (April 2014) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>). This position has been reiterated recently in a challenge to a German law requiring service providers to retain limited traffic and location data of users in order to prevent serious crimes. It was confirmed that generic and indiscriminate retention of data was not permissible, unless there was a specific, genuine and foreseeable circumstance (concerning national security or serious crime) that triggered such a requirement. Further, the retention mandate must be time-restricted in view the relevant situation and subject to independent review.

[118](Court of Justice of the European Union, "Judgment of the Court in Joined Cases C-793/19 and C-794/19: SpaceNet and Telekom Deutschland" (September 2022) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-09/cp220156en.pdf>). Similar positions have been adopted by courts in the Czech Republic and Argentina (Regidi [n 85]).

Certain other jurisdictions such as the US follow a process of "data preservation" rather than "data retention". This requires intermediaries to store specific data sets, pursuant to a request by an LEA. LEAs must then obtain a court order or subpoena for further access to the preserved information.[119] In the UK, the Investigatory Powers Act, 2016, empowers the Secretary of State to issue notices to ISPs, requiring them to retain various types of user data. However, this data can only be accessed by LEAs pursuant to authorisation from judicial officers.

Australia adopts a different position. The Telecommunications (Interception and Access) Amendment (Data Retention) Act, 2015, requires internet service providers (and not platforms such as WhatsApp, Facebook, etc.) to store various kinds of user data for a period of 2 years.[120] This data can be accessed by LEAs upon authorisation by the Attorney General.

### 4.3.3 Surveillance using end-user devices

The IT Act framework does not account for surveillance to be conducted using software implanted into a end-user's device.[121] To this end, Section 43A prohibits unauthorised access to a computer resource, whether by the State or a private entity. However, this is an issue that the IT Act will need to deal with given the revelations about the use of Pegasus software.[122] It is therefore useful to consider whether: (a) the government should have the power to introduce software onto end-user devices to meet compelling State interests, and (b) if so, when should such a power be exercised and what checks and balances should be implemented over its use.

While typically, governments have had the power to carry out extensive and intrusive surveillance on individuals, the range and nature of surveillance made possible in the digital ecosystem is of an entirely different order.[123] Digital devices are used by the majority of the population for virtually every daily activity. Permitting the State to introduce surveillance software onto devices can therefore pose a significant risk to privacy rights. Individuals will always live in fear of surveillance, which can chill rights. The ease of use and difficulty in detecting such software could open the floodgates to misuse and mass surveillance. Individuals will also have little chance of ever knowing if they are under scrutiny, which could carry on for prolonged periods. This method also removes the need for the government to proceed through intermediaries, who can act as a check on State excesses. The use of surveillance software can also cause ecosystem wide problems if it compromises other (non-targeted) systems. Surveillance software typically utilises

[119] Elonnai Hickok, "Data Retention in India" (January 2013) <https://cis-india.org/internet-governance/blog/data-retention-in-india>.

[120] Regidi (n 85).

[121] Software can be used to either access contents of the device or carry out surveillance of an individual's digital and other activities, for instance, by turning on the device's camera or microphone sflc in, "Sflc.in approaches the Supreme Court on the Pegasus issue" (September 2022) <https://sflc.in/sflcin-approaches-honble-supreme-court-pegasus-issue>.

[122] sflc in, "An Anatomy of the Pegasus Spyware" (July 2021) <https://sflc.in/anatomy-pegasus-spyware>; Supreme Court Observer (n 114); ML Sharma vUnion of India (n 114).

[123] Carpenter v United States, "Supreme Court of US" (June 2018) <https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf>.

weaknesses in commercially available software to function. It has been argued that rather than utilise such weaknesses, the government should report any bugs/weaknesses to the relevant software/hardware makers.[124] Finally, surveillance software can easily plant evidence on an end-user device, thereby falsely implicating individuals in offences (this has in fact been alleged in the recent past).[125]

Given the possible ecosystem wide effects, the significant intrusion into rights, and the difficulty in putting in place safeguards, permitting the State to implant software onto end-user devices would be a disproportionate intrusion into fundamental rights.

### 4.3.4 Mandating traceability

The 2021 IT Rules require significant social media intermediaries providing messaging services to enable identification of an originator of a message. In the context of platforms that utilise end-to-end (E2E) encrypted services (where encryption occurs on the end-user device), the rules effectively cast an obligation on intermediaries to modify their platforms to enable traceability of users.[126] Proponents of such a mandate point to the growing numbers of online offences and the need for law enforcement to be able to collect data, particularly in the context of heinous or serious offences.[127][128] It is commonly recognised that encryption allows users to "go dark", thereby making it difficult for law

[124] A failure to do so exposes citizens and businesses alike to threats from a range of malicious actors (Anamika Kundu and others, "Response to the Pegasus Questionnaire issued by the SC Technical Committee" (April 2022) <https://cis-india.org/internet-governance/response-to-the-pegasus-investigation>).

[125] Sukanya Shantha, "Surendra Gadling's Computer Was Attacked, Incriminating Documents Planted: Arsenal Consulting" (July 2021) <https://thewire.in/rights/elgar-parishad-surendra-gadling-cyber-attack-documents-planted>; Scroll Staff, "Pune Police allegedly planted fake evidence on devices of Bhima Koregaon accused, reports Wired" (June 2022) <https://scroll.in/latest/1026337/pune-police-planted-fake-evidence-on-devices-of-bhima-koregaon-accused-reports-wired>.

[126] Anand Venkatanarayanan, "Dr Kamakoti's Solution For WhatsApp Traceability Without Breaking Encryption Is Erroneous And Not Feasible" (August 2019) <https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceability-whatsapp-encryption-madras-anand-venkatanarayanan/>.

[127] The 2021 IT Rules implemented this mandate ostensibly to enable a check on fake news and pornography Press Information Bureau, "Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021" (February 2021) <https://pib.gov.in/PressReleasePage.aspx?PRID=1700766>; Press Information Bureau, "Permanent Mission of India responds to the concerns raised by Special Special Branch of Human Rights Council about India's IT Rules, 2021" (June 2021) <https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1728738>. This followed a Rajya Sabha ad-hoc committee recommending in 2020 that LEAs should be allowed to break E2E encryption to trace distributors of child pornography (Press Information Bureau, "Rajya Sabha Committee calls for mandatory apps on all devices and filters to regulate children's access to pornography content" (January 2020) <https://pib.gov.in/PressReleseDetail.aspx?PRID=1600505>). The issue of identifying users on messaging platforms has also been brought to the attention of various courts in India, though there has been as yet, no conclusive judicial pronouncement on the issue(Anthony Clement Rubin v Union of India, "High Court of Madras" (August 2018) <https://cyberblogindia.in/antony-clement-rubin-v-union-of-india/>; Supreme Court Observer, "Aadhaar-Social Media Linking: Facebook v Union of India" (December 2021) <https://www.scobserver.in/cases/facebook-inc-union-of-india-aadhar-social-media-linking-case-background/>; Reuters, "Government of India And WhatsApp Are Debating Encryption Laws: All You Need to Know" (October 2019) <https://www.news18.com/news/tech/government-of-india-and-whatsapp-are-debating-encryption-laws-all-you-need-to-know-2360453.html>).

[128] Note that the draft Telecom Bill, 2022, seeks to impose an identification mandate on a wide variety of intermediaries. The benefits or drawbacks of such a mandate are outside the scope of this study, which restricts itself to commenting on the traceability requirement imposed by the 2021 IT Rules.

enforcement to perform their functions.[129] Using brute force to crack encrypted communications can be time consuming and resource intensive, thereby making it an inefficient route for law enforcement to adopt.[130]

On the other hand, mandating the use of weakened encryption reduces the security of all data on the platform. This allows any malicious entity the opportunity to exploit weaknesses.[131] Creating backdoors to encryption can also enhance vulnerability of systems and impose unnecessary costs on intermediaries.[132]

A general mandate for intermediaries to enable traceability of users by removing or weakening E2E encryption would compromise the privacy and security of individuals at all times, regardless of whether there was any evidence of illegal activity on their part. This also ignores the alternative means available to LEAs to carry out investigations (such as accessing digital trails, IP addresses, etc). Thus, such a mandate would not be the least restrictive measure available, which would imply that the provision is unconstitutional.[133]

The constitutionality of the provision in the 2021 IT Rules has been challenged by various parties, including WhatsApp (before the Delhi High Court) for violating the right to privacy.[134] As explained by the WhatsApp spokesperson, "*Requiring messaging apps to "trace" chats is the equivalent of asking us to keep a fingerprint of every single message sent on WhatsApp, which would break end-to-end encryption and fundamentally undermines people's right to privacy."*[135] These petitions are currently pending consideration and a transfer petition has been filed to consolidate and bring all challenges to the Supreme Court.

It is worth keeping in mind that virtually no liberal democracy explicitly mandates weakening of encryption or the creation of backdoors in platforms. An exception is Australia, which has enacted the Telecommunications and Other Legislation Amendment (Assistance and Access) Act in 2018 ("TOLA"). This empowers LEAs to require "technical assistance" from "designated communications providers" in the form of Technical Assistance Requests (TARs), Technical Assistance Notices (TANs), and Technical Capability

[129] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (October 2014) <https://bit.ly/3ycSuZB>.

[130] Bailey, Bhandari, and Rahman (n 6).

[131] Ibid; Harold Abelson and others, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications* (techspace rep, MIT Computer Science and Artificial Intelligence Laboratory 2015); Internet Society, *Encryption: An Internet Society Public Policy Briefing* (techspace rep, Internet Society 2022).

[132] David Gripman, "Electronic Document Certification: A Primer on the Technology Behind Digital Signatures" [1999] John Marshall Journal of IT and Privacy Law 769; ACLU and EFF, *Brief for Amicus Curiae in Support of the Defendant-Appellee in Commonwealth of Massachussets v. Leon Gelfgatt, Supreme Court of Massachussets* (techspace rep, ACLU and EFF 2015); Abelson and others (n 131).

[133] Bailey, Bhandari, and Rahman (n 6).

[134] *WhatsApp LLC v Union of India*, WP (C) No. 7284/21 (Delhi High Court). See also the challenges in *Live Law Media Pvt Ltd v Union of India*, WP (C) No. 6272/2021 (H) (Kerala High Court) and *T.M. Krishna v Union of India*, WP (C) No. 12515/21 (Madras High Court).

[135] Richa Banka and Deeksha Bhardwaj, "WhatsApp moves High Court against new IT Rules" (May 2021) <https://www.hindustantimes.com/india-news/whatsapp-moves-high-court-against-new-it-rules-101622073962404.html>.

Notices (TCNs).[136] TCNs, which are to be issued in case of serious criminal investigations, are directions to implement new capacities in a platform/service. This allows the interception and decryption of communications that are encrypted, as long as "systemic weakness" or "systematic vulnerability" are not created.

TOLA has however come in for significant criticism including on grounds of being anti-privacy, facilitating mission creep, and for lacking adequate date retention related safeguards.[137] Keeping in mind the possibilities of misuse, the Independent National Security Legislation Monitor has recommended that powers under TOLA should only be exercised by an independent judicial authority.[138]

### 4.3.5 Mass surveillance programs

Independent of the powers of surveillance under the IT Act, the government runs a number of surveillance programs, such as the Central Monitoring System (Central Monitoring System (CMS)), National Intelligence Grid (National Intelligence Grid (NATGRID)), Lawful Monitoring and Intercept Program (Lawful Intercept and Monitoring Project (LIMP)) and Network Traffic Analysis (Network Traffic Analysis (NETRA)), which have been initiated solely through executive action.

For example, the CMS was announced by the Minister of State for Communications and Information Technology in the Rajya Sabha in November 2009.[139] Similarly, NATGRID was implemented by the government following approval from the Cabinet Committee on Security.[140]

[136] TARs are voluntary requests under which designated communication providers can voluntarily provide data or assistance in respect of criminal investigations or national security matters. TANs are similar to TARs, but they are in the nature of an 'order', and not a request. They do not require service providers to change system architecture any way, but only require compliance to the extent possible. See Sections 317A till 317ZT of the Telecommunications Act, 2017 as amended by TOLA.

[137] Keiran Hardy, "Australia's encryption laws: practical need or political strategy?" [2020] Internet Policy Review; Andrew Tillett, "Encryption laws leave local tech industry in a 'chokehold'" (March 2019) <https://www.afr.com/politics/federal/encryption-laws-leave-local-tech-industry-in-a-chokehold-20190326-p517ri>; Eric Jjemba and Jochai Ben-Avie, "Australian watchdog recommends major changes to exceptional access law TOLA" (July 2020) <https://blog.mozilla.org/netpolicy/2020/07/27/australian-watchdog-recommends-major-changes-to-exceptional-access-law-tola/>.

[138] Independent National Security Legislation Monitor, *Trust but Verify: A Report concerning the Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 and related matters* (techspace rep, INSLM 2020).

[139] CMS is "a system to "monitor communications on mobile phones, landlines and the internet in the country" (Press Information Bureau, "Centralised System to Monitor Communications" (November 2009) <https://pib.gov.in/newsite/PrintRelease.aspx?relid=54679>). Telecom service providers are required by their licenses, to provide LEAs with real time access to their networks (thereby enabling government agencies access to virtually all traffic on telecom networks) (Udbhav Tiwari, "The Design & Technology behind India's Surveillance Programmes" (January 2017) <https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes>). The program is used to carry out analysis of call data records, data mining, machine learning and also uses predictive algorithms to enable agencies to take preemptive law enforcement action (ibid).

[140] NATGRID is a mechanism to connect multiple databases of government entities, thereby allowing the analysis of records/data to decipher trends and provide real time (and even predictive) analysis to government agencies (ibid; PTI, "National Intelligence Grid to finally see light of day" (December 2021) <https://www.thehindu.com/news/national/national-intelligence-grid-to-finally-see-light-of-

Given the absence of statutory backing to any of these programs, each falls foul of the first of the *Puttaswamy* tests of legality. In addition, these programs collect the data of all individuals, at all times irrespective of whether or not a person has committed an offence. As noted in Bailey and others,[141] "Any form of bulk surveillance essentially reduces everyone to a suspect in the eyes of the law, therefore reshaping the behaviour of individuals." This position is backed up by a number of international instruments and texts, notably the UN's General Assembly Resolution on the Right to Privacy in the Digital Age, 2018, which recognises that the use of mass surveillance is inconsistent with international law as it involves systemic and indiscriminate invasion of privacy on a society wide scale.[142] It also difficult to check or place safeguards on as such practices, as they involve granular collection and analysis of data without any oversight mechanisms or the involvement of any intermediaries.[143]

Existing mass surveillance programs therefore fail the proportionality and safeguards tests in *Puttaswamy*. Indeed, the existence of such programs implies that the IT Act must bar the use of any interception mechanisms and programs that are not permitted by any specific law or that are not arise through the specific surveillance related provisions therein. It is also notable, that various foreign jurisdictions such as the US, UK, Australia, etc., largely carry out mass surveillance only on foreign citizens. Domestic surveillance is typically required to be targeted.

## 4.4 Recommendations

We summarise the discussion from the previous sections and suggest various steps to improve the current surveillance framework in India below.

### 4.4.1 Implement a comprehensive surveillance framework

It is clear there is a need for comprehensive review of the entire surveillance ecosystem in India. Ideally, this would take the form of a new legislation specifically setting out the powers of LEAs to carry out surveillance and implementing checks and balances/oversight mechanisms, etc. This would streamline the legal framework and implement a unitary standard across LEAs. Harmonisation at the union level could also provide a best practice document for states to follow.[144] This would also accord with practice seen in a number of democratic countries.[145]

day/article36414741.ece>). NATGRID provides access to 21 data points such as bank details, telephone records, passport data, vehicle registration, etc., to 10/11 government agencies (Tiwari, "The Design & Technology behind India's Surveillance Programmes" [n 139]).

[141] n 5.

[142] Privacy International, *PI's Guide to International Law and Surveillance* (techspace rep, Privacy International 2021); Privacy International, "Mass Surveillance" (September 2022) <https://privacyinternational.org/learn/mass-surveillance>; Privacy International, *PI's Guide to International Law and Surveillance* (n 142).

[143] Privacy International, "Mass Surveillance" (n 142); Chinmayi Arun, "Paper-Thin Safeguards and Mass Surveillance in India" (2014) 26 National Law School of India Review 105.

[144] Vipul Kharbanda, "Policy Paper on Surveillance in India" (August 2015) <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india>.

[145] Bailey and others, *Use of personal data by intelligence and law enforcement agencies* (n 5); Committee of Experts under the Chairmanship of Justice BNSrikrishna (n 103).

There has been a previous attempt to implement a law to regulate intelligence agencies in the form of the Intelligence Services (Powers and Regulations) Bill, 2011.[146] While this private members bill was not enacted, it demonstrates not only the need for reform but a possible route towards putting in place an overarching framework. Such a move was also recommended by the Srikrishna Committee, which noted that "we also recommend that the Central Government carefully scrutinise the question of oversight of intelligence gathering and expeditiously bring in a law to this effect".[147]

In the alternative, reform could be brought in through other legislation such as a data protection or privacy law. There have been two such attempts, the Data Privacy and Protection Bill, 2017, and the Personal Data and Information Privacy Code Bill, 2019, neither of which were however enacted.

As a final option, the surveillance frameworks under the IT Act could also be reviewed. We suggest various options towards this end in the sections below. In this context however, it is important to note that the government has recently released a draft Telecommunications Bill, 2018, (the "Telecom Bill"). The Telecom Bill is an attempt to update and modernize the legislative framework under the Telegraph Act, 1885, the Wireless Telegraph Act, 1933, and Telegraph Wires (Unlawful Possession) Act, 1950. To this end, it brings within its ambit all "telecommunication services". This phrase is defined extremely broadly to include all services and applications on the content layer of the Internet including video and data communication services, internet based communication services, over-the-top communication services, etc. Section 3 of the Telecom Bill subjects all such services to a licensing requirement.[148] Extending a licensing requirement to all telecommunication services would enable the government to extend a range of onerous surveillance related obligations across the Internet stack.[149] In addition, Section 24 of the Telecom Bill empowers the Central and State governments to carry out interception of messages transmitted/received through telecom services on various grounds listed therein. This is concerning given that the Bill provides for very limited safeguards for use of these powers. Further, given that Section 40 of the Telecom Bill gives it an overriding effect over all other laws, surveillance related provisions in IT Act are to all practical purposes rendered otiose. This appears a clear case of overreach given that the purpose of the IT Act is to specifically regulate the digital ecosystem.

Accordingly, the Telecom Bill must be revised to ensure:

- that its scope is limited to the content layer of the Internet. In any event, the Telecom Bill should not seek to impose licensing or related obligations on applications and services on the content layer;

- that Section 40 of the Telecom Bill be revised so that the Telecom Bill does not

[146]The bill sought to implement prior authorisation and warrant based systems for surveillance, established a tribunal for investigation of complaints, and also sought to create oversight institutions in the form of a committee and an ombudsman. The Bill also sought to implement various transparency and accountability mechanisms for intelligence agencies such as reporting requirements.

[147]Committee of Experts under the Chairmanship of Justice BNSrikrishna (n 103).

[148]Which may be waived by the government

[149]As discussed previously, present telecom licenses are used impose obligations pertaining to mass surveillance programs such as CMS as well as to limit the use of strong encryption.

have overriding effect over laws such as the IT Act.

In the alternative, given that the Telecom Bill in its current form will become an omnibus legislation governing the entire digital ecosystem (viz. the content layer as well as the telecom and infrastructure layers of the Internet stack), the law should be revised to include the various surveillance related safeguards discussed below.

### 4.4.2 Revisions in the IT Act

The IT Act could be revised to narrow the scope of the surveillance related provisions, prevent unauthorised and bulk surveillance and to implement safeguards through statute.

1. **Narrow the scope of Sections 69, Section 69B and Section 67C:** Sections 69, 69B and 67C allow the government a significant amount of latitude, which does not accord with principles of necessity and proportionality. Accordingly, these provisions must be revised.

    - Section 69 should include the phrases "on the occurrence of a public emergency" or "in the interests of public safety" as conditions precedent to invocation of surveillance powers. These terms are well recognised in Indian jurisprudence, and also used in the Telegraph Act.[150] The phrase "defence of India" must be deleted and surveillance must be permitted for the "prevention, investigation or prosecution of any cognisable offence". These changes remove ambiguity, and clarify that extraordinary powers can only be used in case of relatively serious offences.[151] Section 69 should also do away with the test of expediency. The phrase "enhancing cybersecurity" must be revised or clarified in Section 69B. Powers must only be exercised when necessary, and not when expedient to do so.

    - Entities to whom powers (to carry out surveillance or access data) are granted must be restricted, based on their specific functions. For instance, only cyber security related agencies need be given powers under Section 69B.

    - Retention norms for intermediaries must be issued only under Section 67C of the IT Act. The provision must also mention (a) the power of the government to notify different retention norms for different categories of intermediaries; (b) lay down specific grounds on which retention may be required; (c) specify that any retention norms specified in the form of rules be necessary and proportionate to the need for retention, for instance by differentiating between traffic data and content; (d) clarify that any data retained under the provision must be deleted upon completion of the retention period. Further, LEA access to retained data should follow approval processes that contain safeguards, such as judicial review.

2. **Implement statutory safeguards:**

[150] These are also retained under the draft Telecommunications Bill, 2022.

[151] A higher bar could also be used by restricting the power of surveillance to offences which are punishable with imprisonment of 3 years and above (indicating the more serious nature of the offence)(Bailey and others, "Comments on the draft Personal Data Protection Bill, 2019" [n 92]).

The IT Act itself should provide for safeguards over surveillance. Leaving this to the executive defeats the purpose of having safeguards in place. Safeguards should be made applicable to all statutory powers regarding surveillance activities, as well as any powers exercised through rules (such as in the context of the Security Rules, the Cyber Cafe Rules or the 2021 IT Rules).

It is notable that three private members bills brought before Parliament also sought to create various procedural safeguards to prevent misuse of surveillance powers by LEAs.[152] Importantly, each suggested independent oversight and authorisation mechanisms in the form of prior review by either a judicial entity or by an independent authority together with post-facto oversight mechanisms. Similarly, the Srikrishna Committee suggests a system of judicial authorisation of interception requests as well as post-facto oversight by a Parliament committee.[153] These systems are also de-rigeur in a number of foreign jurisdictions as illustrated in A.1.

The statute should therefore ensure:

- **Prior judicial authorisation for surveillance**: Prior judicial authorisation of surveillance requests should be mandatory. In the alternative, authorisation could be given by an independent regulatory entity such as a Data Protection Authority.
- **Greater transparency and accountability of LEAs, including by establishing oversight mechanisms:** Mechanisms for appropriate oversight of surveillance activities by independent entities are essential. LEAs must provide such entities with appropriate information to enable them to carry out detailed scrutiny of surveillance practices.
- **Notice of surveillance:** Individuals must be informed after surveillance is completed, subject to relevant exceptions as may be required in the interests of crime prevention, etc.
- **Accessible grievance redress mechanisms:** Systems should be established to ensure that individuals and intermediaries can seek redress for illegal surveillance and that punitive action is taken as appropriate.
- **Implement time limits for surveillance:** Specific time-limits for surveillance must be specified, as well as norms for deletion of data following expiry.
- **Bar on use of illegally acquired evidence:** A significant check that could be brought into the IT Act would be in the form of restrictions against the use of illegally acquired information in court. To this end, a limited statutory bar could be brought in prohibiting the use of illegally acquired communications under Section 69 of the IT Act. Appropriate exceptions could also be provided to such a prohibition, for instance, if illegal interception is conducted

[152] Refer to the Intelligence Powers and Services Bill, 2011, Data Privacy and Protection Bill, 2017, the Personal Data and Information Privacy Code Bill, 2019. The safeguards envisaged in these bills are noted in A.1.

[153] Committee of Experts under the Chairmanship of Justice BNSrikrishna (n 103).

in good faith or in the context of emergencies, etc.

- **Bar on unauthorised surveillance:** The IT Act should bar the use of surveillance mechanisms and programs that do not comply with the specific powers accorded to the State under the legislation.Further, as the IT Act does not contemplate the issuance of orders enabling bulk or mass surveillance, all such programs must be discontinued.[154] In the alternative, specific laws should be put in place with respect to each.

3. **Retain Section 43A:** Section 43A must not be revised, but must continue to penalise (non-consensual) breach of computer resources, whether by State entities or private parties.

4. **Bar creation of systemic weaknesses in platforms:** Any requirement to weaken encryption or force creation of back doors to encrypted platforms is a disproportionate invasion of privacy rights and also casts undue obligations on intermediaries. Accordingly, the provisions in the 2021 IT Rules may need to be revised in this regard.[155]

   That said, should there be a need for such a power to be granted to the government, this should be done through statutory mechanisms rather than through the route of rules issued under Section 79. Statutory provisions should also ensure appropriate safeguards are implemented, as the exercise of this power should not be done solely at the behest of the executive.

### 4.4.3 Other legislative changes

In addition to the above, improvement of the surveillance framework will require changes to other legal frameworks, including:

- placing the establishment, powers, functions and independence of LEAs on sound legal footing. This will limit misuse of agencies, ensure they act within the scope of well defined powers, and help implement appropriate internal organisational safeguards.
- revision of whistle blower protection frameworks to ensure that illegal acts of LEAs can be exposed.
- appropriate amendments under the evidence act and other criminal legislation pertaining to access and use of biometrics, passwords, and other digital evidence.
- ensuring that LEAs are not provided blanket exemptions from right to information,

[154] Bailey and others, *Use of personal data by intelligence and law enforcement agencies* (n 5); Gautam Bhatia, "State surveillance and the right to privacy in India: A constitutional biography" [2014] National Law School of India Review 128; Bhandari and others (n 88); Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, "India's communication surveillance through the Puttaswamy lens" (May 2018) <https://blog.theleapjournal.org/2018/05/indias-communication-surveillance.html>.

[155] TRAI has also suggested any regulation that requires changes in platform architecture, or would otherwise lead to vulnerabilities being introduced in communication systems be avoided (TRAI, *Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services* (techspace rep, Telecom Regulatory Authority of India 2020)).

data protection or other such frameworks.

- revising the telecom licenses, which currently cast extremely broad obligations on service providers to facilitate interception and monitoring by LEAS. The restrictions on the use of certain types of encryption must also be done away with, while data retention norms must be necessary and proportionate.[156]

# 5 Cybersecurity

**Summary of recommendations**

The IT Act has substantive provisions that define "cybersecurity" and prescribe various offences, such as that of unauthorised access to computer resources. The statute also establishes an institutional framework to deal with cybersecurity, in the form of CERT-in and NCIIPC.

- While the cybersecurity offences prescribed in the law are broadly in consonance with international standards, they could be improved by limiting the scope of offences by providing certain exceptions. For instance, the statute should not penalise ethical hacking and data scraping.
- Institutional frameworks established under the IT Act must be revised to clarify the role and powers of CERT-in and NCIIPC. In particular, their rule-making powers should be clarified. The law should also avoid duplicating functions of each agency.
- Mandatory incident reporting requirements should be limited to large and systemically important systems and entities.
- Mechanisms should be established to enable coordination between cybersecurity agencies, sectoral regulators and other relevant authorities, as well as the private sector.

## 5.1 Background

Section 2(1)(nb) of the IT Act defines "cybersecurity" to mean:

> "... protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction."

As indicated in Figure 1 below, the main goals of a cybersecurity framework are to identify, protect against, detect, respond to and recover from threats.[157]

With increasing digitisation in our societies, it is vital to ensure that computer systems, particularly those controlling critical aspects of our economies and infrastructure, are

[156] Note that TRAI has also recommended re-examining restrictions on the use of encryption in telecom services.TRAI, *Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector* (techspace rep, Telecom Regulatory Authority of India 2018)

[157] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (2018).

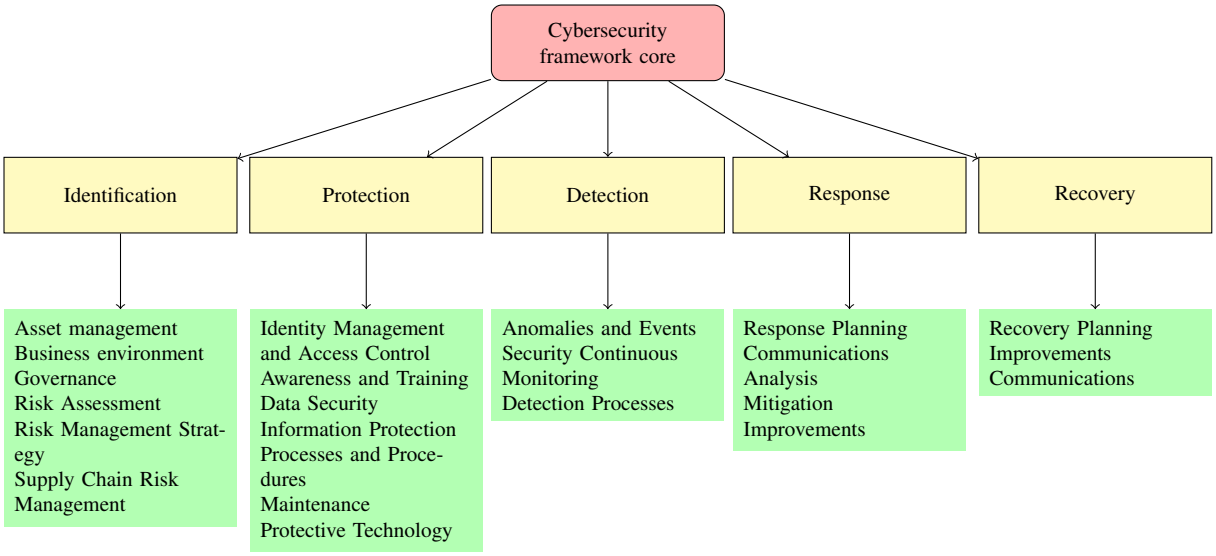


Figure 1: Source: National Institute of Standards and Technology[158]

adequately protected. The scale and economic cost of cybersecurity incidents in India have increased greatly over the last decade. While CERT-in handled 13301 cybersecurity incidents in 2011, this number has increased to 1.4 million in 2021.[159] The average total organisational cost of data breach was INR 53.5 million in 2011 (INR 102.92 million, inflation-adjusted for 2021) — this has increased to INR 185.23 million in 2021.[160]

Cybersecurity incidents also threaten our strategic strength. However, it has been observed that the culture of cybersecurity in India "lacks depth" when it comes to policy coordination. India is a "third-tier" cyber power when compared to its "second-tier adversaries like China"[161]. There is a "dire need" to strengthen the cybersecurity framework and institutions to meet the challenge of the digital age[162].

In this context, this section examines India's legal framework on cybersecurity, and points to four key infirmities: (a) an unclear foundation and design of CERT-in and NCIIPC; (b) poor coordination among these agencies and other sectoral bodies; (c) poorly defined scope of work and delegated powers with CERT-in; and, (d) issues with the agencies' capacity. We therefore suggest revisions in the design, structure, functions and scope of CERT-in and NCIIPC in order to prepare these institutions to address the challenges posed by the new generation of cyber threats.

## 5.2 Statutory framework

The IT Act framework concerning cybersecurity comprises "substantive" provisions and "institutional" provisions. Among the "substantive provisions" are provisions that define

[159] Indian Computer Emergency Response Team (CERT-in), *CERT-in Annual Report 2011* (2012).

[160] *Cost of a Data Breach Report* (2022).

[161] International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment" [2021] .

[162] Data Security Council of India, *Submission of comments for the National Cyber Security Strategy 2020* (2020).

terms such as “cybersecurity” and “computer resoures”, as well as provisions that craft offences of both a civil and criminal nature. Notable civil offences relate to the wrongful loss of personal data, while criminal offences relate to dishonest receipt of stolen devices, identity theft, impersonation, privacy violation and cyber terrorism. Importantly, the IT Act places the responsibility of safeguarding personal and sensitive personal data on the (public or private) entity that handles/collects the data.[163] The duty to safeguard a “protected system” lies on the designated private or public entities who operate such a system.[164]

The institutional provisions enable the central government to monitor traffic data for cybersecurity purposes, declare certain computer systems as “protected systems”,[165] and establish two institutions - first, a national nodal agency for protection of critical information infrastructure, the NCIIPC, and second, the CERT-in as the national agency for incident reporting and response.

We examine the institutional framework under the IT Act below. We also briefly examine the role of other central and sectoral institutions that deal with cyber security.

### 5.2.1 CERT-in

CERT-in was officially established in 2004 as a body within the Ministry of Electronics and Information Technology (MEITY).[166] Prior to this, it was functioning as a technical body within the Department of Information Technology where its primary functions were to block illegal online content, and coordinate information sharing and incident response with regard to cybersecurity incidents.

Through amendments to the IT Act in 2009, CERT-in was designated as the national agency to perform the following functions in the area of cybersecurity:

1. collect, analysis and disseminate information on cybersecurity incidents
2. forecast and issue alerts of cybersecurity incidents
3. coordinate cybersecurity incident response activities
4. enhance technical capacities on information security practices, processes, preventive measures, etc., pertaining to cybersecurity incidents.

In order to carry out these functions, CERT-in was empowered to call for information from, and give directions to, any person. A failure to comply with CERT-in’s directions

[163] This is done through Rule 8 of *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules*, 2011 which *inter alia* prescribes certain standards to be followed in protecting personal and sensitive personal data. Further, Section 43A penalises entities for failing to take appropriate care in maintaining security practices.

[164] No additional standards or security measures appear to have been laid down for such systems under the IT Act framework.

[165] “Protected” systems are those which operate a “critical information infrastructure”, which in turn is “a computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety”.

[166] Press Information Bureau, “Shourie inaugurates national facility “CERT-In" to handle computer security incidents” (19 January 2004) <https://archive.pib.gov.in/newsite/PrintRelease.aspx?relid=744>.

can lead to criminal sanction.

The *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013* ("CERT-In Rules") lay out the functions/duties, composition and procedures pertaining to CERT-in. Under Rule 12 of these Rules, all persons *may* report cybersecurity incidents to CERT-In. The CERT-In Rules also prescribe certain types of cybersecurity incidents, for which reporting is *mandatory*.[167] Mandatory reporting must be done "within a reasonable time period" of the incident. The CERT-In Rules prohibit the agency from disclosing incident information and identities of any specific person or group without their explicit written consent.[168]

Rule 11(1) of the *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013* acknowledges the limited capacity of CERT-in to deal with all cybersecurity incidents and devises an order of priority for incident response in decreasing order:

1. threats to the physical safety of human beings,
2. cyber incidents of "severe nature" e.g. DoS/ DDoS, intrusion, spread of contaminant etc.
3. large-scale or most-frequent incidents like ID theft, defacement, intrusion etc.
4. compromise of individual user accounts on multiple systems.
5. all other incidents.

In April 2022, CERT-in issued the *Directions under section 70B(6) of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted internet* ("2022 Directions") in order to augment and strengthen cybersecurity in India. The directions impose the following requirements on all persons:

1. Compulsory syncing of servers with NIC's NTP server.
2. Mandatory reporting of cybersecurity incidents within six hours of detection.
3. Mandatory maintenance of metadata and logs for 180 days.
4. Data centers, VPS and VPN providers to compulsorily register and identify/validate all subscribers with the same information that is required by the Know your customer (KYC) norms laid down by the Reserve Bank of India (RBI).
5. Expansion in the list of cybersecurity incidents that are to be mandatorily reported.

The list of types of cyber incidents which are to be reported has been expanded to cover newer forms of cybersecurity incidents involving mobile phone apps, Internet of things

[167] These incidents include targeted scanning, unauthorized access, defacement, malicious code, ID theft, denial of service and attacks on e-governance services.

[168] This restraint does not apply if there is a court order instructing them otherwise. The statutory power to seek information also can be exercised only by an official of a rank equal to or higher than a Deputy Secretary.

(IOT) devices etc.

### 5.2.2 NCIIPC

Established in 2014, the NCIIPC is designated as a nodal agency for protection of critical information infrastructure. NCIIPC is an agency under the National Technical Research Organisation (NTRO), which itself reports to the National Security Advisor and the Prime Minister.

Under section 70(1) of the IT Act "any computer resource which directly or indirectly affects the facility of critical information infrastructure" is a protected system. The MEITY is empowered to decide which systems are "protected".[169] NCIIPC is then responsible for ensuring these systems are adequately protected from cyber threats.

Unlike the case of CERT-in, the IT Act does not confer any specific statutory powers on NCIIPC. Its powers come solely from the *Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013*. These enable it to give directions to organisations with protected systems and coordinate response with CERT-in in case of a cybersecurity incident concerning a critical information infrastructure. It is not clear if NCIIPC is authorized to respond to cybersecurity incidents by itself. As is the case with CERT-in, the NCIIPC also has a priority waterfall which helps streamline its work.

Unlike Section 70B(7) of the IT Act, which penalizes failure to report to CERT-in, there is no such provision in the *Information Technology Act* for failing to report an incident to NCIIPC. This may explain why, as of March 2022, no cybersecurity attack on critical infrastructure systems have ever been reported to NCIIPC.[170]

In addition to its general functions mentioned above, NCIIPC has two more roles. The first is to appoint its nominee to the Information Security Steering Committee (ISSC) set up by an entity operating a protected system. The second is to coordinate with the entity operating a protected system, through its Chief Information Security Officer (CISO), to oversee changes to cybersecurity systems, networks, security policies and to approve periodical security audit reports.

### 5.2.3 Understanding the broader cybersecurity ecosystem:

The IT Act does not restrict sectoral regulators from formulating their own security and incident response rules. Figure 2 gives a description of the various institutions in India involved in incident reporting and response. For example, financial sector regulators such as RBI, SEBI and IRDAI have prescribed specific standards for entities under their regulatory ambit. Similarly, the armed forces have their own cybersecurity agency (which

[169] Note that while NCIIPC can frame guidelines on how to identify what is a "protected system" that is part of the "critical information infrastructure", the final determination of which organisation should be identified as such rests with MEITY. The MEITY has designated the systems of Unique Identification Authority of India (UIDAI), Long Range Tracking System of the Ministry of Shipping, NPCI, ICICI Bank and HDFC Bank as "protected systems".

[170] Lok Sabha, "Cyber attack on critical infrastructure" in *Starred question* (299, 23 March 2022).

may apprise CERT-in of threats and responses but are not mandated to do so). The Ministry of Power, under the Central Electricity Authority (CEA), also maintains its own cybersecurity apparatus and regulations to safeguard the power grid infrastructure. For cyber crime reporting, the Ministry of Home Affairs maintains a set of agencies to accept complaints and coordinate between state-level police agencies. Some states like Andhra Pradesh have their own CERT for incident reporting and response when it comes to cybersecurity issues involving state government organisations.

We can therefore see that the regulatory landscape concerning cybersecurity is not centralized. This in itself is not a cause for concern. In section 5.3.4 we see that the academic literature favours a multiplicity of specialized CERTs.

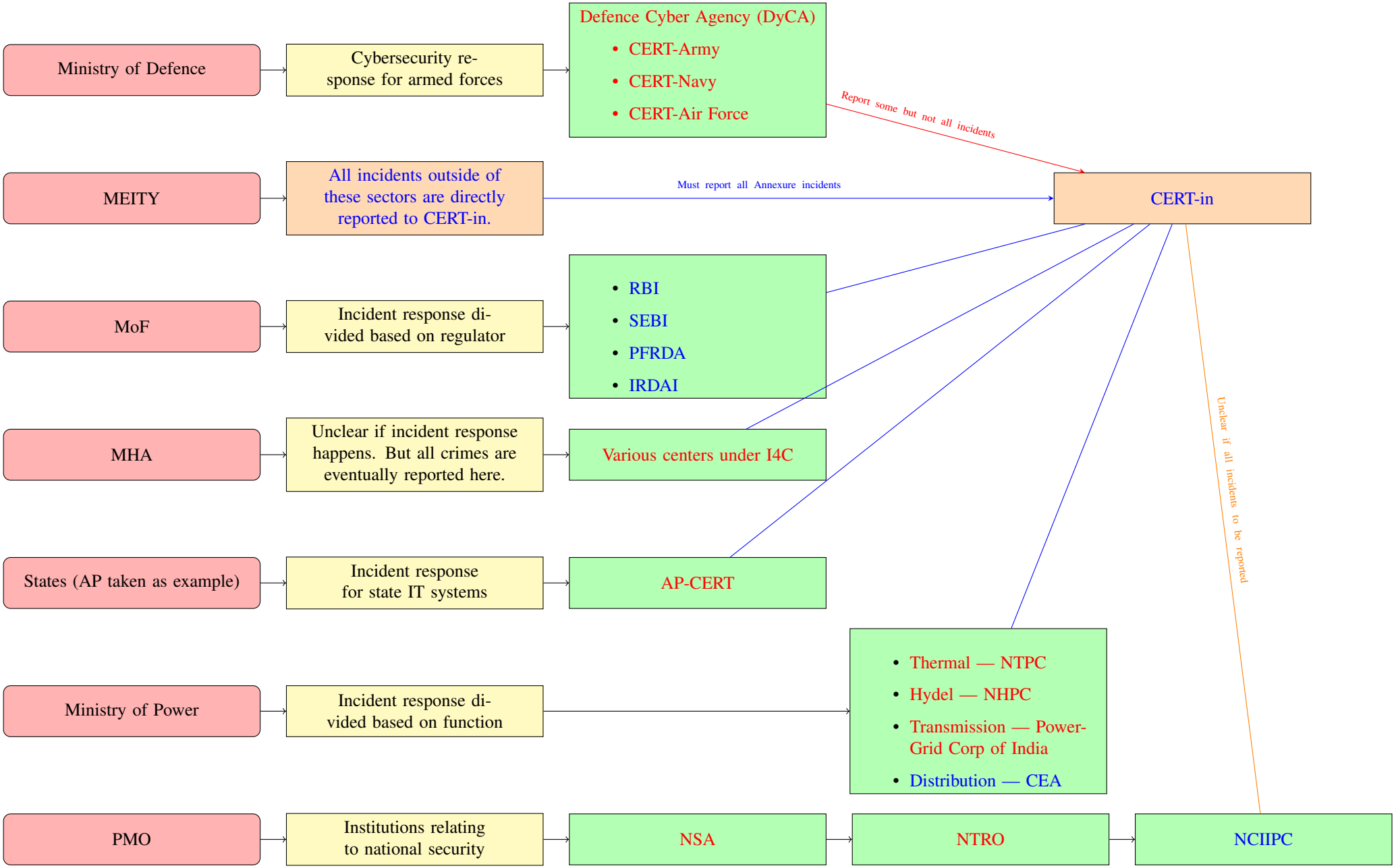


Figure 2: Where should cyber incidents be reported. Red text denotes executive bodies. Blue text denotes statutory bodies. The institutions under the Indian Cybercrime Coordination Centre (I4C) scheme are linked here.

## 5.3 Analysing the cybersecurity framework

As mentioned earlier, the IT Act has "substantive" provisions and "institutional" provisions. We highlight two significant shortcomings with the substantive provisions and thereafter discuss the infirmities in the institutional provisions.

### 5.3.1 Shortcomings in substantive provisions

There are two primary issues with the substantive provisions — the lack of general exceptions (or statutory defences) to the prescribed offences and the outdated position taken by section 43(b).

We can see from Appendix A.2 that the definitions of cybersecurity across the United States of America (USA), United Kingdom (UK) and Singapore, are similar to that in India. The nature of offences covered by the Indian legislation are also in line with international practices. However, unlike the UK and the USA, the IT Act does not specify any statutory defences that are available to individuals accused of cyber offences.

Such exemptions are useful in certain contexts such as that of "ethical hacking". Encouraging ethical hacking is in the broader public interest as this enables shortcomings in security frameworks to be exposed. Such practices should therefore be encouraged, as long as done with a bona fide ethical/public interest purpose.[171] In this respect, it is also notable that Section 81 of the Indian Penal Code, 1860, recognises that an act should not be considered a criminal offence if committed without intent to cause harm and done in good faith to prevent or avoid harm to person or property. Crafting an exception for ethical hacking would therefore accord with existing criminal law principles.

The second issue concerns that of data scraping. The practice of data scraping i.e. the "automated collection of data" is widely used in the IT industry to perform analyses of different kinds. The large-scale collection of text on websites to examine patterns and provide insights is referred to as "big data analytics". Data scraping is also an important tool for researchers to study trends on the internet. Section 43(b) of the IT Act makes it an offence to "download, copy, extract data without permission of the owner of the computer system". It is unclear if scraping is covered by the wording of this sub-section. If it is, not only would it be onerous to seek permission from the website developers but also it would inhibit the growth of the field of "big data analytics" in India.

The United States of America adopts a different position compared to India. It has been clarified by the United States Supreme Court that the use of information from a computer system is legal as long as the user had legitimate access to the system.[172] This applies to the context of data scraping as well.[173]

[171] "Ethical hackers" are individuals who "employ the same tools and techniques as intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them." CC Palmer, "Ethical hacking" (2001) 40(3) IBM Systems Journal 769

[172] *Van Buren v. United States* 593 US 1 (2021).

[173] *HiQ Labs v. LinkedIn Corporation*, 31 F.4th 1180 (2022).

### 5.3.2 Lack of inter agency coordination

The IT Act fails to clarify the roles of different government agencies, thereby leading to incoherence in their actions. For example, the NCIIPC has issued guidelines on which systems to categorise as "protected". However, the final decision in this regard is made by the MEITY upon whom these guidelines are not binding. In practice, only five systems have been designated as such.[174] This raises questions about arbitrariness in application of the law. Why have other systems in the same class of firms, not been chosen, for instance why only chose ICICI and HDFC Bank and not say, an SBI? Equally, why have systems in other critical sectors such as power and transportation, etc. been excluded? This incoherence stems from the lack of clarity in the functioning of and coordination between NCIIPC and MEITY.

The absence of proper designation of "protected systems" also implies that for all practical purposes, CERT-in is the only relevant cybersecurity agency in the government. Indeed, it is notable that in March 2022, the Minister of Electronics and IT stated in Parliament that no cyber attacks were reported to NCIIPC.[175]However, public record indicates that a number of entities such as power plants, etc., have been targets of cyber attacks.[176]

To explain with an example, a ransomware attack took place at All India Institute of Medical Sciences (AIIMS) on 23 November 2022. The CERT-in was involved in cybersecurity response for this incident since it emerged that AIIMS is not designated as "protected system" that would have brought it under NCIIPC's jurisdiction.[177] Later it emerged that AIIMS did not maintain a centralized security system despite the fact that it stores sensitive personal data of patients who range from the common person to multiple Prime Ministers of India.[178] A week after the incident, AIIMS had not been able to retrieve the lost data and it enlisted the help of the Defence Research and Development Organisation (DRDO) for this purpose. This is not provided for in the operating procedures given by either CERT-in or NCIIPC.[179] The AIIMS ransomware incident is one among many incidents that have persistently shown breakdowns in incident response at all levels of incident management.

Similarly, a number of sectoral regulators such as CEA, RBI, Securities and Exchanges

[174]The computer systems of UIDAI, Long Range Tracking System of the Ministry of Shipping, NPCI, ICICI Bank and HDFC Bank.

[175]Lok Sabha (n 170).

[176]Tata Power CoLtd, "Cyber Attack" (14 October 2022) <https://www.bseindia.com/xml-data/corpfiling/AttachHis/cd21ff9a-0414-48b5-a1c2-3ef514776924.pdf>; Nuclear Power Corporation of India Ltd, "Press Release" (30 October 2019) <https://www.npcil.nic.in/writereaddata/Orders/201910301239083808622News_30102019_01.pdf>.

[177]The Print, "AIIMS server down for 7th straight day; two system analysts suspended" (30 November 2022) <https://theprint.in/india/aiims-server-down-for-7th-straight-day-two-system-analysts-suspended/1241850/>.

[178]India Today, "AIIMS Cyberattack: Lack of centralized security system makes it tough to restore all processes online" (1 December 2022) <https://www.indiatodayne.in/national/story/aiims-cyberattack-lack-centralized-security-system-makes-it-tough-restore-all-processes-online-477372-2022-12-01>.

[179]Moneycontrol, "Ransomware attack: Diverting personnel, seeking DRDO's help, AIIMS tries to control damage" (30 November 2022) <https://www.moneycontrol.com/news/trends/ransomware-attack-diverting-personnel-seeking-drdos-help-aiims-tries-to-control-damage-9627811.html>.

Board of India (SEBI), etc. have their own regulations on incident reporting & response mechanisms. It is not clear to what extent these organisations coordinate with CERT-in and NCIIPC to address cybersecurity issues. The absence of proper coordination mechanisms also becomes relevant due to the possible enactment of a data protection law, and the possibility of imposition of data breach reporting requirements under the same. Currently, all data breaches in India have to be reported to CERT-in. This position may therefore need to be revised based on obligations imposed under a new data protection framework. In any event, appropriate coordination mechanisms must be created to ensure that the a proposed data protection authority and cybersecurity agency can work together, without imposing excessive reporting costs on the ecosystem.

### 5.3.3 Excessive delegated powers

The IT Act fails to properly elucidate the manner in which CERT-in is to perform its functions, and in the process gives it very broad powers to issue directions. This has resulted in the notification of a number of onerous legal obligations through executive action, leading to litigation and legal uncertainty. For example, some service providers have challenged the 2022 Directions before the High Court of Delhi. In particular, the petition alleges that the 2022 Directions force them to collect information on their users which they would not have otherwise collected in the normal course of business. Accordingly, the petition argues that the 2022 Directions violate the privacy rights of users, while restricting business rights and imposing disproportionate costs on service providers.

The position under the IT Act is in contrast to many other jurisdictions, which typically provide narrow powers to the regulators to call for information. For instance, under Regulation 15(2)(a) of the *Directive (EU) 2016/1148 of the European Parliament and Council concerning measures for a high common level of security of network and information systems across the Union* in the European Union, national regulators have the power to call for information from service providers, but only when such information is reasonably required to "assess either the security of the service provider's network and information systems, and the implementation of the operator's security policies". Essentially, regulators should not be provided carte blanche to issue directions or call for information. Obligations imposed on service providers must be directly related to a specific purpose and be proportionate in nature. In this respect, it must also be kept in mind that the IT Act mandate is to provide information to CERT-in *in case of a cyber incident* when CERT-in seeks information *regarding that cyber incident*.[180] The purpose of the information seeking provisions is to prevent "contagion" i.e. to assess the impact of a specific vulnerability or attack on the internet and to ensure the internet functions smoothly after response. The 2022 Directions therefore appear to be disproportionate in their scope.

While the Delhi High Court is yet to decide on the constitutionality of the 2022 Directions, the broader problem is the lack of clarity caused by the wide wording in Section 70B of the IT Act, which enables the agency to "call for information and give directions" in respect of all the functions listed in Section 70B(4).

[180] Rule 13(1) Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 2014.

### 5.3.4 Flaws in institutional design

The lack of clarity around the functioning of NCIIPC and CERT-in can also be traced back to the initial design of these entities.

**The idea of a CERT**:

The first incident response team was created in the United State, as a response to the first computer virus in 1988. Defense Advanced Research Projects Agency (DARPA) along with Carnegie Mellon University created the world's first CERT with the objective of co-ordinating responses to attacks on computer systems. The CERT was to be a community of highly qualified volunteers who respond to security breaches "like firefighters". Even at the early stages DARPA recognized the fact that cyber users are a large constituency and each separate constituency (e.g. defence, medical, universities etc.) should have their own CERT.[181]

The key design principles of the very first CERT include a strong network of volunteer contacts, and in-house technical expertise to handle a reasonable portion of day-to-day security incidents. The repository of information should include vulnerability details, security incident reports, etc. The security features for these repositories must be beyond reproach — preferably stored in an offline system not accessible via network connections. The idea is to include not only technical experts but also site managers, security officers, industry representatives and government officials etc.[182]

To provide more context on what domains CERTs cover and what responsibilities they undertake, we examine the institutions created in the US, the UK and Singapore.

**Practices followed in US, UK and Singapore**:

In A.2 we see that the differences among the three jurisdictions under study, lies is the extent of the applicability of the reporting requirements. We find two distinct forms of reporting.

First, a *certain class of entities* designated as critical information systems or essential services etc. have to report all cybersecurity incidents. The basis of this requirement is to aid in ensuring *national security*. The government identifies certain sectors as "critical" and their continuous provision is deemed to be vital towards ensuring national economic and military security. Critical infrastructure providers also have to follow heightened security measures.

For example, in the USA, reporting cybersecurity incidents affecting critical information infrastructure was first mandated by §1016 of the USA Patriot Act of 2001. Telecommunications, energy, financial services, water and transportation sectors were designated as critical, based on how important they are towards national security and their vulnerability to disruption by terrorist actors.

Second, there are entities which have to report incidents but only *if they are above a cer-*

[181] William L Scherlis, Stephen L Squires, and Richard D Pethia, "Computer Emergency Response" in Peter J Denning (ed), *Computers under attack: intruders, worms, and viruses* (ACM Press 1990).
[182] Ibid.

*tain threshold* in impact. There are two kinds of incidents which are above this threshold. The first is that of *breach of personal data*. In some countries like the USA, state-level laws require reporting of data breaches containing personal information. In California, for example, a breach affecting more than 500 Californian residents has to be reported to the state's Attorney General. In the European Union (EU), the General Data Protection Regulations (GDPR) (as translated into local legislations) requires data controllers to report breaches to the member state's data protection authority. The second is that of *breaches of systemically important services*. The UK captures this group as "Relevant digital service provider (RDSP)" i.e. online marketplaces, search engines and cloud computing services. The definition of RDSP is based on the EU's NIS Directive.[183]

Legislative documents in the US, UK and Singapore all also recognise the intrinsic linkage of cybersecurity with issues of privacy and data protection. These countries therefore create a harmonised institutional framework to address these issues. Cybersecurity related institutions do not issue directions or rules but are empowered to call for information.[184] Rule-making and other forms of regulation are left to sectoral regulators, union governments and privacy regulators.

**Problems with CERT-in**:

An evaluation of the institutional framework of CERT-in leads to the following conclusions:

1. *Unclear institutional design*: As mentioned earlier, the primary function of a CERT is to coordinate responses to cybersecurity incidents and ensure that the internet remains operational and accessible to all users. However, the genesis of the CERT-in's functions show that its institutional purpose was unclear from the start.

   CERT-in was set up in January 2004 as a group within the Ministry of Communications. The stated objective of the new organisation included "... enhancing awareness among the cyber community regarding information and computer security by issuing security guidelines and informing them of latest security threats, prevention measures and solutions by issuing advisories, vulnerability notes and incident notes."[185] It gained statutory powers in 2009 and its current strength of 130 was finalized in 2017.[186]

   However, we note some major issues and decisions that deviate from this stated objective. For example, even before CERT-in was formally established it received its very first assignment which was to block websites, admittedly without the legal powers to do so.[187] While CERT-in has been given more functions as the years have

[183]Directive (EU) 2016/1148 of the European Parliament and Council concerning measures for a high common level of security of network and information systems across the Union 2016.

[184]Explanatory Memorandum to the Network and Information Systems Regulations 2018 2018; Wall Street Journal, "U.S. Cyber Agency Hopes to Avoid the 'Regulator' Label" (12 October 2021) <https://www.wsj.com/articles/u-s-cyber-agency-hopes-to-avoid-the-regulator-label-11634031001>.

[185]Press Information Bureau, "Shourie inaugurates national facility "CERT-In" to handle computer security incidents" (n 166).

[186]See 2 Indian Computer Emergency Response Team (Group A and Group B officials recruitment) Rules 2017.

[187]Procedure to block websites 2003.

passed, its manpower is insufficient to handle the exponential increase in cybersecurity incidents that have been reported. The 2022 Directions have only widened the CERT-in's remit but no announcements on increasing its capacity to exercise its ambit, such as budget and manpower increases, have been announced so far. We can see from examples like the AIIMS breach (mentioned in Section 5.3.2) that CERT-in had to engage with other agencies like NCIIPC and DRDO, yet the full resumption of online services has not taken place as of writing on 1 December 2022, eight days after the incident.

The biggest consequence of its unclear design is its diminished capacity. CERT-in has too few people and too many roles in order to deliver incident response of good quality. To begin with, we know that close to 150 people work at CERT-in full-time. Table 2 shows the budget of CERT-in.

| Year | Capital | Revenue | Total |
|---|---|---|---|
| 2021 | 370 | 547.3 | 917.3 |
| 2020 | 299.8 | 0 | 299.8 |
| 2019 | 299 | 0 | 299 |

Table 2: Figures are in INR millions. Source: Union Budget documents.

For comparison, the Cybersecurity and Infrastructure Security Agency (CISA) in the USA has a budget of USD 3.6 billion and a staff of 2392 professionals in 2021. This requires that capacity and functions be streamlined to ensure effective incident response. The USA also has 108 other CERT teams registered with FIRST. India has only one — CERT-in. China has 12 CERT teams and Brazil has six.

2. *Insufficient in-house technical expertise*: CERT-in is a completely executive body housed inside MEITY. It is staffed entirely by full-time government officials. It has a sanctioned strength of 125 scientists, one legal officer and ten officers in administrative roles.[188] While these officers are scientists and they have technical qualifications, they are ultimately civil servants. A CERT should function like an ecosystem and not like any other government department.

3. *Network of volunteer contacts*: It is not clear if CERT-in engages with external consultants on a day-to-day basis. This is not to say that the government does not engage at all with stakeholders in the private sector on building better cybersecurity frameworks.[189] However, it is unclear if the service rules of the central government allow for a deputation or consultation system to bring in expertise from the private sector for more active roles within CERT-in.

4. *Repository of incidents*: CERTs should keep in a secure form, a repository of incidents as well as the experts who are best suited to solve for the specific incident. This information should be stored in a highly secured manner, disconnected from the internet. The CERT-in does maintain this information. It also has rules on maintaining confidentiality of the affected persons and their security measures.

[188] Indian Computer Emergency Response Team (Group A and Group B officials recruitment) Rules 20 November 2017.

[189] *Securing our cyber frontiers: report of the Cyber Security Advisory Group* (2012).

5. *Need for multiple CERT groups*: The CERT-in considers its constituency to be all internet users in India.[190] This constituency, as of 2021, is 45% of India's population. All persons as well as sectoral CERTs have requirements to report their cybersecurity incident to CERT-in. The views of the private sector representatives like Data Security Council of India (DSCI) and NASSCOM were that Information Sharing and Analysis Centres (ISACs) should be created at the level of sectoral and organizational CERTs. ISACs would fulfill only the information reporting function of a full-fledged CERT while incident response is done by CERT-in.[191] This view however was ten years ago and today the private sector has better capacity to do its own incident response. On the other hand, it appears that CERT-in in its current form might fall short of the capacity it needs to respond to a significant number of incidents.

## 5.4 Recommendations

In view of the discussion above, we recommend that the IT Act be revised as follows.

1. Add general exceptions to cybersecurity offences:

   Specific exceptions should be added to section 43 of the IT Act to clarify that ethical hacking should not be penalised. This would incentivise testing of security standards, and therefore aid in enhancing cybersecurity. In addition, it should be clarified that scraping of publicly available data from websites should not fall foul of Section 43(b) of the IT Act. This would promote innovation and reduce arbitrariness in prosecution of individuals for accessing publicly available information for productive purposes.

2. Clarify the role of CERT-In and NCIIPC: The domains of CERT-in and NCIIPC are unclear. This has led to a lack of clarity on the roles and obligations between these organisations. Most jurisdictions have only one entity that oversees incident reporting as well as critical infrastructure. A similar structure could be followed in India, where the functions of CERT-in and NCIIPC could be combined into one organisation. This amalgamanted organisation can focus on ensuring *internet availability and access* for critical infrastructure, digital and internet service providers, etc. *National security* functions such as threat detection could be left to a dedicated intelligence agency.

3. Clarify incident reporting obligations: The mandate of incident reporting in India is extremely broad. There may be no gains by requiring all firms to report all incidents. In fact excessive reporting requirements may be counterproductive. Excessive information provision can lead to less focus on significant threats, particularly in the context of low state capacity. It is also important to remember that most sectoral regulators will also have reporting obligations on their respective regulated entities. Firms should therefore only be required to report to the sectoral regulator or CERT-in. In sectors where a regulatory requirement exists, the sectoral regulator

[190] Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 16 April 2014.

[191] *Salient Features of the JWG Report on Engagement with Private Sector on Cyber Security* (2012).

should co-ordinate information sharing with CERT-in. The rationale for incident reporting is for the CERT to assess impact on the broader internet infrastructure and prevent damage to critical infrastructure.It may, therefore, be useful to only require the obligations of incident reporting on firms designated as *critical infrastructure*. There is also a need to conduct a periodic review of the sectors and firms covered under the definition of "critical infrastructure."

4. Clarify the process of rule making: All rules imposing substantive obligations on entities must be subject to Parliamentary oversight. Appropriate revisions should therefore be made in Section 87 of the IT Act to clarify the rule making power with regard to cybersecurity incidents.

5. Clarify coordination mechanism: There is a need to clarify the co-ordination mechanisms between CERT-in and the various sectoral regulators. The system of a MoU can cover processes for co-ordination and reporting between CERT-in, NCIIPC, MEITY and sectoral regulators. The MOU could also operate in conjunction with a centralized, anonymized reporting system e.g. Automated Indicator Sharing in the USA.[192]

[192]The AIS uses open standards and encoding for participants to share threats of a specific nature with specific information without the need to divulge their identity. This information is accessible on a dashboard to all participants.

# A Appendices

## A.1 Appendix A: Comparison of surveillance safeguards

| | Authorisation[193] | Review/Oversight | Grievance Redress[194] | Other Safeguards |
|---|---|---|---|---|
| **UK** | | | | |
| Investigatory Powers Act, 2016 | Authorisation by Secretary of State followed by a Judicial Commissioner | Investigatory Powers Commissioner, Intelligence and Security Committee of Parliament | Information Commissioner's Office, Investigatory Powers Tribunal | Penalises surveillance carried out without lawful authority; Extra safeguards for surveillance over members of parliament, journalists, etc.; Safeguards for retention and access to intercepted communications |
| **Canada** | | | | |
| Security Intelligence Services Act, 1985, Criminal Code | Designated judges in Federal Court approve warrants | Intelligence Commissioner, which also submits reports to the Prime Minister | Intelligence Commissioner | Notice to be provided to individual of surveillance |
| **Australia** | | | | |
| Telecommunications (Interception and Access) Act, Criminal Code | Judicial warrant required to access content of communications, not metadata | Commonwealth Ombudsman, Inspector General of Intelligence and Security | NA | Notice to be provided to individual of surveillance |
| **USA** | | | | |
| Electronic Communications and Privacy Act, 1986 etc. | Court approval for domestic surveillance, special FISA courts to authorise foreign surveillance | US Congress and its committees, President's Intelligence Advisory Board, Privacy and Civil Liberties Oversight Board, Office of Inspector General of the Intelligence Community | NA | Special authorisation processes where surveillance target is a member of congress, a federal judge, etc.(requiring approval of Department of Justice) |
| **Germany** | | | | |

[193] Under general circumstances, i.e. not emergency situations

[194] Specific mechanisms, that is, outside normal court processes

| | | | | |
|---|---|---|---|---|
| Code of Criminal Procedure, Control Panel Act, 2009, Federal Intelligence Services Act | Committee of Parliamentary members authorises requests of intelligence agencies, Court orders for regular law enforcement | Parliamentary panel carries out oversight, reporting by intelligence agencies to federal chancellory, reporting by law enforcement to Federal Office of Justice | NA | NA |
| **India** | | | | |
| Srikrishna Committee Report | Judicial authorisation through designated district judges | Parliamentary Committee | Data Protection Authority in case of breach of the data protection law | NA |
| Intelligence Services (Powers and Regulation) Bill, 2011 | By an executive authority (Secretary to the Government of India or above) | (Independent) National Intelligence and Security Oversight Committee | National Intelligence Tribunal and Intelligence Ombudsman | NA |
| Data Privacy and Protection Bill, 2017 | Chief Privacy Commissioner (quasi-judicial authority) | NA | Privacy Commissioner | Bar on surveillance without lawful authority; Bar on mass surveillance; Notice to be provided to individual upon conclusion of surveillance; Restrictions on data retention, subject to extension |
| Personal Data and Information Privacy Code, 2019 | Surveillance division of Privacy Commission (quasi-judicial authority) | NA | Privacy Commissioner | Scope of exemptions from data protection obligations for law enforcement to be decided by Privacy Commission, on application; Evidence procured illegally not admissible in court; Bar on surveillance without lawful authority; Notice to be provided to individual of surveillance; Restrictions on data retention |

## A.2 Appendix B: Comparing cybersecurity laws across jurisdictions

| Category | India | USA | UK | Singapore |
|---|---|---|---|---|
| Definition of "cyber security" | | | | |
| What does the definition seek to do | Protection | Efforts against adverse impact | Resist, at a given level of confidence | Protected from unauthorized access or attack |
| What does it seek to protect | Information, equipment, devices, computer, communication device and information stored therein | An information system and the information that is stored, processed by, or transiting through it | Network and information systems | Computer system |
| How is this protection compromised? | Any unauthorised access, use, disclosure, disruption, modification or destruction | An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system. | Any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems | An act carried out without lawful authority on or through a computer system that jeopardises or adversely affects the integrity and confidentiality of information stored in, processed by or transmitted through the computer system. |
| Laws regarding cyber offences | | | | |
| Name of law | IT Act and relevant rules | Computer Fraud and Abuse Act at federal level along with state laws.[195] | Cyber Misuse Act, 1990 | Cybersecurity Act, 2018 |
| Hacking | ✓ | ✓ | ✓ | ✓ |
| Phishing | ✓ | ✓ | ✓ | Penalised by Singapore Penal Code. |
| DOS | ✓ | ✓ | ✓ | ✓ |
| Infection of IT system | ✓ | ✓ | ✓ | ✓ |
| Possession of hardware/software to commit cybercrime | ✓ | ✓ | ✓ | ✓ |
| Distribution of hardware/software to commit cybercrime | ✓ | ✓ | ✓ | ✓ |

[195] For the purpose of this section in the table we consider only federal law.

| | | | | |
|---|---|---|---|---|
| Identity theft | ✓ | ✓ | ✓ | ✓ |
| Electronic theft | ✓ | ✓ | ✓ | ✓ |
| Unsolicited penetration testing | Penalised | Valid defence | Unclear | Penalised |
| Extra-territorial application | ✓ | ✓ | ✓ | ✓ |
| General exceptions | None | ✓ | Unclear | Unclear |
| Incident reporting and response | | | | |
| Name of law | IT Act and relevant rules | Various rules at both federal and state levels.[196] For the purpose of this part we take Department of Health and Human Services' (DHHS) CSIRC as an example which is empowered by the Federal Information Security Modernization Act of 2014 to provide incident response services. | Network and Information Systems Regulations, 2018 | Cybersecurity Act, 2018 |
| Name of incident response organisation | CERT-in | Various e.g. DHHS CSIRC at federal level, New York Department of Financial Services at state level etc. | NCSC, GCHQ | Commissioner of Cybersecurity |

[196] Only incidents relating to health data, personal credit data and critical infrastructure sectors are to be reported to the federal government. For other sectors there are state-level sectoral regulators.

| | | | | |
|---|---|---|---|---|
| Roles and responsibilities of incident response organisation | Collection, analysis and dissemination of information, forecasting and alerts, emergency measures for cyber incidents, coordination and research. | DHHS CSIRC — performing periodic risk assessments, developing and maintaining cybersecurity response infrastructure and providing security training. | Monitoring, early warning, alerts, announcements and dissemination of information, incident response, dynamic risk and incident analysis and situational awareness, establish relationships with the private sector to facilitate co-operation, promote the adoption and use of common or standardised practices. | Monitoring, response, identify and regulate critical information infrastructure, license and establish standards in relation to cybersecurity service providers as well as prosecution of cybercrimes. |
| Statutory/ legal powers | Issue directions to any person and collect information relating to cybersecurity incidents. | DHHS CSIRC — define high value assets and call for information from the relevant office within the DHHS. | (i) Direct the RSDP to inform the public about the security incident, (ii) power of inspection and (iii) power to impose penalty after hearing | Calling for information, issuing administrative summons, search and seizure under warrant and prosecutions. |
| Regulated entities | All persons | Sector/department specific. | Relevant Digital Services Provider (RDSP). RSDPs are online marketplaces, search engines and cloud computing services | Only critical infrastructure and cybersecurity service providers. |
| How does the entity bind to the regulator | No registration. All entities are bound by statute. | Federal entities identified by the Federal Information Security Modernization Act of 2014. Others bound by sectoral rules at state/federal level. | (a) Duty to register as an RDSP with the sectoral regulator, (b) nominate a UK-resident person to represent them with the regulator if the RDSP is registered elsewhere | Registration required for critical instructure and cybersecurity service providers. |

| | | | | |
|---|---|---|---|---|
| What to report | Any incident mentioned in the Annexure of the IT (CERT-in manner of functioning and response) Rules. | Any situation that could compromise the confidentiality, availability or integrity of data. | Any cybersecurity incident which has a significant impact on the continuity of the RDSP's service. This is based on the following thresholds (a) affected number of users, (b) duration of incident and (c) geographical area affected. | All incidents. |
| When to report | Within six hours of the incident. | "As soon as possible". Suggested time is one hour. | Within 72 hours of the incident | Submit the name of infrastructure affected, nature of incident and effect observed within 2 hours. Submit report on causes, impact and damage: 14 days. |
| Whom to report to | CERT-in | CERT of relevant sector. | Information Commissioner | Commissioner of Cybersecurity |
| Civil penalties for not reporting | Fine of INR 100,000 | Report is prepared and submitted to US Attorney General (if federal) or state Attorney General for filing civil suit. | Not a "material contravention" - up to GBP 1 million. "Material contravention" - up to GBP 8.5 million. "Material contravention" which causes significant risk to service provision - up to GBP 17 million. Regulator must furnish decision within 28 days of initiation. | Fine up to SGD 100,000 |
| Criminal penalties for not reporting | Imprisonment of up to one year. Can be levied even if civil remedies are complied with. | Only if civil remedies are not complied with. | Only if civil remedies are not complied with. | Imprisonment of up to two years. Can be levied even if civil remedies are complied with. |
| Critical information infrastructure | | | | |

| | | | | |
|---|---|---|---|---|
| Name of law | IT Act and relevant rules | This is done at federal level by the Cybersecurity Information Sharing Act, 2015 read with relevant Presidential Orders and the Homeland Security Act. | Network and Information Systems Regulations, 2018 | Cybersecurity Act, 2018 |
| Name of regulator | NCIIPC | CISA | Sectoral regulators for OES | Commissioner of Cybersecurity |
| Statutory/ legal powers | NCIIPC has to nominate its member on the firm's ISSC. CERT-in has powers to issue directions to call for information regarding a specific breach | CISA can issue "administrative subpoena" to obtain information on "covered system" | Sectoral regulator can (i) direct the OES to inform the public about the security incident, (ii) inspect OES systems and (iii) impose penalty after hearing | Calling for information, issuing administrative summons, search and seizure under warrant and prosecutions. |
| Regulated entities | Protected systems operating critical information infrastructure | All "covered systems" — this is defined as "a device or system commonly used to perform industrial, commercial, scientific, or government functions or processes related to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers." Does not include personal devices or systems. | Operators of essential services (OES). Sectors classified as OES are identified in the schedule of the NIS Regulations. | All critical infrastructure and cybersecurity services providers. |
| How does the entity bind to the regulator | MEITY selects which system is "protected" under NCIIPC | 16 sectors chosen as "critical infrastructure" by law. All entities within that sector have to report. | All OES have to register with the relevant sectoral regulator. If they are registered outside the UK, they have to nominate a UK-resident representative | Registration required |

| | | | | |
|---|---|---|---|---|
| What to report | Any incident mentioned in the Annexure of the IT (CERT-in manner of functioning and response) Rules. | Unauthorized system access, DDoS of more than 12 hours, malicious code, targeted and repeated scans, phishing, ransomware | Any incident which has "significant impact on the continuity of the essential service." This is based on the following thresholds (a) affected number of users, (b) duration of incident and (c) geographical area affected. | All incidents |
| When to report | Within six hours of the incident. | "Significant cyber incident" within 72 hours, ransomware within 24 hours | Within 72 hours of the incident | Name of infrastructure affected, nature of incident and effect observed: 2 hours. Report on causes, impact and damage: 14 days. |
| Whom to report to | CERT-in | CISA | Sectoral regulator, who in turn shares info with the NCSC | Commissioner of Cybersecurity |
| Civil penalties for not reporting | Fine of INR 100,000 | Reference to Attorney General of the United States to file federal civil suit. | Not a "material contravention" - up to GBP 1 million. "Material contravention" - up to GBP 8.5 million. "Material contravention" which causes significant risk to service provision - up to GBP 17 million. Regulator must furnish decision within 28 days of initiation. | Fine up to SGD 100,000 |
| Criminal penalties for not reporting | Imprisonment of up to one year. Can be levied even if civil remedies are complied with. | None mentioned | Only if civil remedies are not complied with | Imprisonment of up to two years. Can be levied even if civil remedies are complied with. |
| Law on data protection | | | | |

| | | | | |
|---|---|---|---|---|
| Name of law | IT Act and relevant rules | Varies by state. For the purpose of this part only we take California Consumer Privacy Act of 2018 as an example | Network and Information Systems Regulations, 2018 | Personal Data Protection Act 2012 |
| Regulated entities | All persons | All persons and businesses | Relevant Digital Services Provider (RDSP) and controllers of personal data | All organisations that collect personal data |
| Name of regulator | Enforcement mechanism under section 43A. Unclear whether the state level mechanism works well. Data Protection Authority of India proposed. | Attorney General of California | Information Commissioner for RDSPs. | Personal Data Protection Commission |
| How are breaches reported? | All breaches of the types specified in the Annexure have to be reported. | If data includes personal information and if more than 500 Californian residents are affected, disclosure of breach is mandatory. | Only OES and RDSPs have to report breaches of all data. "Controllers" of personal data also have to report breaches | Notifiable data breaches to be reported. A data breach is notifiable if it is likely to lead to significant harm (e.g. personal data breaches and other specific circumstances) or is of significant scale (measured by number of individuals affected) |
| Civil penalties for breach | Compensation based on actual losses. No cap mentioned. | In California - every count of violation (per person) up to USD 7500 | If not a "material contravention" - up to GBP 1 million. "Material contravention" - up to GBP 8.5 million. "Material contravention which causes significant risk to service provision" - up to GBP 17 million. Regulator must furnish decision within 28 days of initiation. | Maximum penalty for companies – SGD 10 million or 10% of turnover in Singapore, whichever is higher. For individuals it is SGD 200,000. |

| | | | | |
|---|---|---|---|---|
| Criminal penalties for breach | 3 years imprisonment in case intermediary contravenes the information storage rule or refuses government access to certain information | Only if civil remedies are not complied with | Only if civil remedies are not complied with | 2 years imprisonment. Can run concurrently with civil case. |
| Other details | | | | |
| Public-private groups | NASSCOM | Cyber Safety Review Board | UK Cybersecurity Council | GovWARE |
| New issues being discussed | NA | Supply chain security, zero trust maturity model, Automated Indicator Sharing | Rules for managed services, self-financing models for the regulator | National Cybersecurity R&D Program, Cybersecurity Development Program. |