V

CYBERSECURITY, DATA PROTECTION & NATIONAL SECURITY

B&J | BHATT & JOSHI ASSOCIATES

LEGAL DISCLAIMER

This booklet is published by Bhatt & Joshi Associates, Advocates & Solicitors, for general educational and informational purposes only. It does not constitute legal advice, and no attorney-client relationship is formed by reason of this publication. The content is based on primary legislative sources, official gazette notifications, regulatory instruments, and judicial decisions available as of the date of publication. Readers should not act on the basis of this publication without obtaining specific professional advice tailored to their circumstances. This publication complies with the Bar Council of India Rules on Standards of Professional Conduct and Etiquette. © Bhatt & Joshi Associates. All rights reserved.

TABLE OF CONTENTS

CHAPTER 1

Constitutional Framework: Privacy, Expression and National Security

1.1 The Puttaswamy Judgment: Right to Privacy as a Fundamental Right

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, decided by a nine-Judge Constitution Bench of the Supreme Court, is the foundational constitutional decision for the entire edifice of privacy, data protection, and telecommunications surveillance law in India. The unanimous holding — that the right to privacy is a fundamental right intrinsic to the right to life and personal liberty under Article 21 of the Constitution — overruled the earlier decisions in M.P. Sharma v. Satish Chandra, AIR 1954 SC 300, and Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295, which had held that the Constitution did not recognise a fundamental right to privacy. The Puttaswamy judgment established the right to privacy as a core constitutional value, applicable to both private individuals and to corporations, and recognised its application in the telecommunications and digital communications context with explicit force.

The Puttaswamy Court articulated a three-part test for justifying restrictions on the right to privacy: first, the restriction must have a valid law backing it (the "legality" requirement, meaning not merely executive action but a specific statutory provision); second, the restriction must pursue a "legitimate state aim" (including public order, national security, and public health, but not arbitrary governmental interest); and third, the restriction must be proportionate to the aim pursued (meaning that less intrusive alternatives must not be available and that the degree of intrusion must not exceed what is necessary to achieve the legitimate aim). This three-part test — generally known as the "Puttaswamy proportionality standard" — has become the primary constitutional benchmark against which all telecommunications surveillance law, data protection law, and restrictions on digital communications in India are assessed.

The Puttaswamy judgment's recognition of privacy in the telecommunications context was explicit. The Court held that informational privacy — the right to control information about oneself, including information about one's communications, location, and digital activities — is a dimension of the fundamental right to privacy. The collection, processing, and disclosure of subscriber data by telecom operators; the monitoring of communications by government agencies; and the processing of digital traffic data for law enforcement or commercial purposes all engage the constitutional right to informational privacy. Any such activity that has the effect of restricting or interfering with a subscriber's privacy must satisfy the Puttaswamy proportionality

standard — meaning that it must be authorised by a specific statutory provision, must pursue a legitimate aim, and must be necessary and proportionate to the aim pursued.

The implications of the Puttaswamy judgment for the telecommunications regulatory framework have been profound and far-reaching. The judgment prompted the government to commission a comprehensive data protection legislation (ultimately enacted as the Digital Personal Data Protection Act, 2023, discussed in Chapter 4). It also prompted scrutiny of the interception and surveillance framework — the legal basis for government access to subscriber communications and data — under the Indian Telegraph Act, 1885 and its successor provisions in the Telecommunications Act, 2023. Several petitions challenging the constitutional validity of the interception framework, and the adequacy of its procedural safeguards against the Puttaswamy standard, are pending before the Supreme Court and are among the most significant pending constitutional litigations in India.

1.2 Anuradha Bhasin and Freedom of Expression Online

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637, decided by a three-Judge Bench of the Supreme Court in January 2020, applied the Puttaswamy proportionality standard to the specific context of telecommunications service shutdowns — colloquially known as internet shutdowns or internet blackouts. The case arose from the suspension of internet and mobile telephone services in Jammu and Kashmir following the revocation of the state's special constitutional status in August 2019. The Court held that the right to access the internet is a fundamental right, protected as part of the right to freedom of speech and expression under Article 19(1)(a) and as part of the right to practise one's profession under Article 19(1)(g), since many livelihoods and businesses in the modern economy depend on internet access for their functioning.

The Court's directions in Anuradha Bhasin established specific requirements for the exercise of the government's power to suspend telecommunications services. First, every order suspending telecommunications services must be in writing, specifying the reasons for the suspension. Second, suspended orders must be published or otherwise made available so that affected parties can access and challenge them before courts. Third, every order must have a finite duration and must be subject to periodic review — an indefinite suspension without review is unconstitutional. Fourth, the suspension must be proportionate to the specific threat or emergency it is designed to address — a blanket, area-wide suspension is disproportionate if more targeted measures can address the specific concern. Fifth, courts must be able to examine the basis for and proportionality of the suspension on judicial review.

The post-Anuradha Bhasin litigation in various High Courts and before the Supreme Court has continued to develop the jurisprudence on internet shutdowns. High Courts in Kashmir, Rajasthan, and other states have struck down specific shutdown orders as failing to meet the Anuradha Bhasin requirements — either because the written orders were not published, because the reasons given were insufficient to justify the scope of the suspension, or because the suspension continued beyond the period justified by the specific emergency. The litigation has had a modestly constraining effect on the government's use of internet shutdowns: while India continues to account for a large proportion of global internet shutdowns by number, the duration and geographic scope of shutdowns have tended to be more limited than in the pre-Anuradha Bhasin era, reflecting both judicial pressure and the government's desire to avoid further adverse court judgments.

The Anuradha Bhasin judgment also addressed the legal basis for internet shutdowns — specifically, whether the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 provided adequate statutory authority for internet shutdowns. The Court held that the Rules did provide a valid legal basis, but that the substantive and procedural requirements they prescribed must be strictly complied with. The Telecommunications Act, 2023's provisions on service suspension under Section 5 are the successor legal framework to the 2017 Rules, and will be subject to the same constitutional requirements established in Anuradha Bhasin. The adequacy of the 2023 Act's framework against the Anuradha Bhasin constitutional standard — including whether the rules prescribed under Section 5 incorporate the transparency, proportionality, and periodic review requirements — is a subject of ongoing legal scrutiny.

1.3 National Security and Constitutional Limitations

The constitutional framework for national security-motivated restrictions on telecommunications and digital communications involves a careful balance between the state's legitimate security interests and the fundamental rights of citizens. The Supreme Court has consistently held that national security is a legitimate aim for restricting constitutional rights, but has equally consistently held that national security cannot serve as a blanket justification for disproportionate restrictions — each specific restriction must be necessary for, and proportionate to, the specific security threat it addresses. The "national security" exception to constitutional rights protection is not unlimited: it does not authorise measures that are disproportionate to the threat, that affect rights beyond the scope necessary to address the threat, or that are based on no more than speculative or unparticularised concerns about security.

The tension between national security and constitutional rights in the telecommunications context arises in several specific areas. Bulk surveillance programmes — government collection of large quantities of subscriber communications data without targeted, individuated suspicion — raise proportionality concerns that have not been fully addressed in Indian jurisprudence. Requirements for operators to retain subscriber communications data for extended periods (to enable retrospective access by security agencies) similarly engage privacy concerns that must be justified against the Puttaswamy standard. Requirements for operators to incorporate specific government-mandated security vulnerabilities (such as "backdoors" for government access) in their network infrastructure engage both privacy and security concerns — since backdoors created for government access can be exploited by malicious actors as well as by the government.

The international human rights law framework — including the International Covenant on Civil and Political Rights (ICCPR), to which India is a party — supplements the constitutional analysis. The ICCPR's Article 17 (protection against arbitrary interference with privacy) and Article 19 (freedom of expression) are interpreted by the UN Human Rights Committee as imposing requirements broadly consistent with the Puttaswamy proportionality standard: legality, legitimate aim, necessity, and proportionality. The UN Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression have both published reports on surveillance and internet shutdowns, drawing attention to India's record in these areas and urging greater compliance with international human rights standards.

CHAPTER 2

The Information Technology Act, 2000: Telecom Dimensions

2.1 Overview of the IT Act's Telecom-Relevant Provisions

The Information Technology Act, 2000 (Act 21 of 2000), as amended significantly by the Information Technology (Amendment) Act, 2008, is India's primary legislation governing computer and internet-related activities. While the IT Act and the Telecommunications Act, 2023 occupy distinct but overlapping regulatory spaces — the IT Act primarily addresses computer-related offences, digital signatures, data protection, and electronic governance, while the 2023 Act primarily addresses telecommunications services and infrastructure — several provisions of the IT Act have direct and significant implications for telecom operators and their regulatory obligations. The most important of these are: Section 69 (power to issue directions for interception, monitoring, or decryption of information); Section 69A (power to block online content); Section 69B (power to authorise monitoring and collection of traffic data); Section 70 (protection of critical information infrastructure); Section 70B (CERT-In: functions and powers); and the intermediary liability provisions of Section 79.

Section 69 of the IT Act authorises the Central Government or a State Government (through the Home Secretary or equivalent) to issue directions to any agency of the government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence. Unlike the interception framework under the Indian Telegraph Act, 1885 (or its successor, Section 24 of the Telecommunications Act, 2023), which applies specifically to telecommunications messages, Section 69 of the IT Act applies to "information in any computer resource" — a broader category that encompasses messages stored in servers, data at rest in cloud storage, and information in any digital form. The relationship between Section 69 of the IT Act and the telecommunications interception framework is an important legal question for operators who receive both types of interception directions.

Section 69A, added by the 2008 amendment, authorises the Central Government (through the Secretary, Ministry of Electronics and Information Technology) to issue directions to any government agency or intermediary to block access to any information on any computer

resource in the interest of specified public interest grounds, including sovereignty and integrity of India, national security, public order, and maintaining friendly relations with foreign states. This "blocking" power is the legal basis for the government's orders requiring internet service providers to block access to specific websites, mobile applications, and online content. Telecom operators (as internet service providers) are "intermediaries" within the meaning of the IT Act and are therefore subject to Section 69A blocking directions. The most commercially significant application of Section 69A in the telecom context has been the blocking of Chinese mobile applications (including TikTok, PUBG Mobile, and approximately 300 others) in June-November 2020 — orders that affected hundreds of millions of Indian users and several major technology companies.

Section 69B authorises the Central Government to direct any agency of the government or any intermediary to collect, monitor, or analyse internet traffic data for the purpose of enhancing cybersecurity. This power — to access internet traffic data in bulk (not merely the content of specific communications) — enables the government to monitor internet traffic patterns for cybersecurity threat intelligence purposes. The relationship between Section 69B bulk data collection and the privacy protections of the Puttaswamy framework is legally contested: while traffic data (metadata) is less intrusive than content data, the Supreme Court in Puttaswamy explicitly recognised that metadata (including location data, time of communication, and communication patterns) engages the right to privacy and must satisfy the proportionality standard.

2.2 Section 70: Critical Information Infrastructure

Section 70 of the IT Act, 2000 (as amended in 2008) provides for the designation of "protected systems" — systems of strategic importance to national security, public safety, public health, or the economy — as "critical information infrastructure" (CII). The Central Government may designate any computer resource as a protected system and may prescribe rules governing the access and protection of protected systems. Any unauthorised access to a protected system is a criminal offence under Section 70 punishable with imprisonment of up to ten years and a fine. The designation of telecommunications network elements as CII under Section 70 — particularly core network elements, national internet exchanges, and submarine cable landing stations — creates a comprehensive legal framework for the protection of these systems from cyber attack.

The National Critical Information Infrastructure Protection Centre (NCIIPC), established under Section 70A of the IT Act, is the nodal body for the protection of critical information infrastructure in India. NCIIPC's mandate covers: developing policies, guidelines, and best

practices for CII protection; coordinating with sector-specific Computer Emergency Response Teams (Sector CERTs) in critical sectors including telecommunications, power, banking, and transportation; conducting vulnerability assessments of CII; and providing technical assistance to CII operators in implementing protective measures. The telecommunications sector CII protection framework — coordinated between NCIIPC, CERT-In, and DoT — is one of the more mature sector-specific CII frameworks in India, reflecting the strategic importance of telecommunications infrastructure to all other critical sectors.

The relationship between the IT Act's Section 70 CII framework and the Telecommunications Act, 2023's critical telecommunication infrastructure (CTI) framework is an important legal question. Both frameworks can apply to the same infrastructure: a telecommunications operator's core network elements may be designated as both CII under Section 70 (because they fall within the telecommunications critical information infrastructure category designated by NCIIPC) and as CTI under Section 23 of the 2023 Act (because their disruption could cause national security or economic security risk). The compliance obligations under the two frameworks are broadly similar but not identical, and operators must ensure that they are meeting the requirements of both frameworks. The government's intention appears to be to maintain both frameworks in a complementary rather than exclusive relationship, with NCIIPC providing the cybersecurity-focused CII framework and the Telecommunications Act providing the telecommunications-specific CTI framework.

The offences for unauthorised access to CII under Section 70 apply not only to external attackers (hackers) but also to employees, contractors, and other insiders who access CII without authorisation or who exceed their authorised access. This makes insider threat a significant compliance concern for telecommunications operators whose employees have access to CII systems as part of their job functions. Security vetting of personnel with access to CII, segregation of access rights on a need-to-know basis, and robust audit logging of CII access are compliance measures that operators must implement both to comply with CII protection requirements and to demonstrate that they have taken adequate security precautions against insider threats. CERT-In's guidelines on CII protection provide detailed technical guidance on these measures.

2.3 Intermediary Liability and Telecom Operators

The intermediary liability provisions of the IT Act — Section 79 (safe harbour for intermediaries) read with the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the Intermediary Guidelines) — are relevant to telecom operators in their capacity as internet service providers. Section 79 provides that an intermediary is not liable for third-party

information or content hosted or transmitted through its platform if the intermediary: acts as a conduit for information (without selecting or modifying the content); observes due diligence in its operations; and upon actual knowledge of illegal content, expeditiously removes or disables access to it. Telecom operators acting as ISPs (carrying internet traffic without selecting or modifying content) generally qualify for the Section 79 safe harbour for the content they transmit.

However, the Intermediary Guidelines, 2021 impose significant compliance obligations on "significant social media intermediaries" (those with more than 5 million registered users in India) and on intermediaries generally. The general compliance obligations include: publication of privacy policies and rules; grievance redressal mechanisms; user account removal processes; and cooperation with government orders. Operators who provide social media or OTT messaging services (in addition to access services) may face the enhanced compliance obligations applicable to significant social media intermediaries. The legal status of telecom operators as "intermediaries" for the purpose of the Intermediary Guidelines — specifically, whether they are subject to the guidelines in their capacity as access providers (through which users access third-party platforms), or only in their capacity as direct service providers (if they provide their own messaging or content services) — is an important regulatory question with significant compliance implications.

The constitutional validity of the Intermediary Guidelines, 2021 — specifically the provisions requiring identification of the "first originator" of viral messages on encrypted messaging platforms — has been challenged before High Courts in India. The challenge raises fundamental questions about the compatibility of mandatory message traceability with: the constitutional right to privacy (since traceability requires breaking end-to-end encryption); the constitutional right to freedom of speech and expression (since traceability creates a chilling effect on anonymous speech); and the constitutional right to equality (since the traceability obligation is imposed only on significant social media intermediaries, creating asymmetric obligations). Telecom operators whose messaging services may qualify as significant social media intermediaries have a direct stake in the outcome of these constitutional challenges.

CHAPTER 3

CERT-In: Mandate, Powers and Incident Reporting

3.1 CERT-In's Establishment and Functions

The Indian Computer Emergency Response Team (CERT-In) is India's national cybersecurity agency, established under Section 70B of the Information Technology Act, 2000 as amended in 2008. CERT-In functions under the Ministry of Electronics and Information Technology (MeitY) and serves as the national nodal agency for cybersecurity incident response, coordination, and capacity building. Its primary functions include: collection, analysis, and dissemination of information on cyber incidents; forecast and alerts on cybersecurity threats; emergency measures for handling cybersecurity incidents; coordination of cybersecurity incident response activities; issuance of guidelines, advisories, vulnerability notes, and white papers relating to information security; and training and capacity building for cybersecurity professionals in government and critical sectors.

CERT-In's relationship with the telecommunications sector is particularly close, since telecommunications networks are both critical infrastructure in their own right and the medium through which most cyber attacks are conducted and detected. Telecom operators are major sources of cyber threat intelligence — their network monitoring capabilities (including anomaly detection, traffic analysis, and malware signature identification) provide early warning of cyber attacks that may affect other sectors. CERT-In coordinates with telecom operators' Security Operations Centres (SOCs) to share threat intelligence and to coordinate responses to large-scale cyber incidents (such as distributed denial-of-service attacks, ransomware outbreaks, or nation-state-sponsored advanced persistent threat campaigns) that affect multiple sectors simultaneously.

CERT-In's directions — issued under Section 70B(6) of the IT Act — are legally binding on service providers and intermediaries and must be complied with expeditiously. CERT-In directions may require: blocking of malicious IP addresses or domains; implementation of specific security patches or configuration changes; reporting of specified categories of cyber incidents; and cooperation with CERT-In's technical investigations of specific incidents. Non-compliance with CERT-In directions is an offence under the IT Act, punishable with imprisonment and fine. Telecom operators must have processes and technical capabilities in place to implement CERT-In directions within the prescribed timelines, which are often very short for genuinely urgent cybersecurity threats.

CERT-In's role in the telecommunications sector is formally coordinated with DoT and TRAI through inter-agency mechanisms including the Cyber Security Coordination Committee and the National Cyber Coordination Centre (NCCC). The NCCC, established by the Intelligence Bureau, operates a 24/7 cyber surveillance facility that monitors internet traffic for threat intelligence, sharing findings with CERT-In, law enforcement agencies, and telecom operators' SOCs. The legal basis for the NCCC's traffic monitoring activities — which involves large-scale access to internet traffic data without individualised authorisation — is the subject of legal scrutiny in the context of Puttaswamy and Section 69B of the IT Act. Practitioners advising telecom operators on NCCC-related compliance must carefully assess the scope and validity of specific NCCC access requests against the applicable legal framework.

3.2 The April 2022 CERT-In Directions: Compliance and Controversy

The CERT-In Directions issued in April 2022 under Section 70B(6) of the IT Act — requiring service providers, intermediaries, data centres, and cloud service providers to implement a comprehensive set of cybersecurity measures — generated significant industry debate about their scope, implementability, and legal basis. The Directions require, among other measures: synchronisation of ICT system clocks with government-designated NTP (Network Time Protocol) servers; mandatory reporting of specified cybersecurity incidents to CERT-In within six hours of discovery; maintenance of logs of all ICT system activities for a period of 180 days within Indian jurisdiction; and specific incident reporting formats and procedures. The six-hour reporting requirement — significantly more stringent than the 72-hour reporting requirement under the GDPR and most international frameworks — was the most controversial aspect of the Directions.

The legal controversy around the 2022 Directions centred on several issues. First, the scope of the Directions extended to a very large range of entities — essentially all organisations that operate ICT systems — without distinguishing between different categories of organisation based on their risk profile or systemic importance. Cybersecurity regulatory proportionality principles suggest that more stringent requirements should apply to higher-risk, higher-impact entities (such as telecom operators, banks, and critical infrastructure operators) rather than to all organisations regardless of their risk profile. Second, the requirement for ICT log retention within Indian jurisdiction raised data localisation concerns, potentially requiring multinational companies to replicate their global log management infrastructure within India. Third, the requirement to report cybersecurity incidents to CERT-In within six hours raised practical concerns about the feasibility of accurate incident reporting within such a short timeframe.

The telecommunications sector's response to the 2022 Directions highlighted the intersection of cybersecurity compliance with existing telecom regulatory obligations. Telecom

operators were already subject to extensive cybersecurity and incident reporting obligations under their licence conditions (carried forward under the 2023 Act's authorisation framework) and under the Trusted Telecom Portal framework. The 2022 CERT-In Directions added a further layer of obligation, with some overlap and some inconsistency with the existing licence-based requirements. The need for better coordination between MeitY (which issued the CERT-In Directions), DoT (which administers licence-based cybersecurity conditions), and NCSC (which manages the Trusted Telecom Portal) has been identified as a systemic governance gap that the regulatory framework should address more explicitly.

The industry's representation to CERT-In and MeitY following the April 2022 Directions resulted in some clarifications and modifications, including a three-month compliance period for certain requirements and clarification that the six-hour incident reporting requirement applied to confirmed incidents (not suspected incidents). These modifications addressed some of the practical concerns but did not resolve the fundamental questions about the scope and proportionality of the Directions. CERT-In's approach — issuing highly comprehensive Directions and then modifying them in response to industry feedback — reflects the challenges of developing cybersecurity regulation for a rapidly evolving threat environment, but also illustrates the importance of thorough pre-notification consultation before issuing legally binding compliance directions.

3.3 Incident Reporting Framework for Telecom Operators

Telecom operators face a complex, multi-layered incident reporting framework. Cybersecurity incidents affecting telecommunications networks must be reported to: CERT-In within the timelines prescribed in the 2022 Directions (six hours for specified categories of serious incidents); DoT under the licence/authorisation security conditions (within timelines specified in the licence conditions); NCSC under the Trusted Telecom Portal framework (for incidents involving trusted telecom equipment); TRAI (in certain cases involving customer data breaches or service quality impact); and potentially to multiple state and central law enforcement agencies if the incident has criminal dimensions (under the Cyber Crime Reporting Portal administered by the Ministry of Home Affairs' Indian Cyber Crime Coordination Centre, I4C).

The multiplicity of reporting obligations — to different authorities, on different timelines, in different formats — creates significant compliance complexity for telecom operators' incident response teams. A single large-scale cyber incident may trigger simultaneous reporting obligations to CERT-In (within six hours), DoT (within the licence-prescribed timeline), and law enforcement (if criminal activity is suspected). The incident response process must be structured to enable rapid notification to all relevant authorities without compromising the technical

investigation of the incident or the remediation efforts that take priority in the immediate aftermath of a serious attack. Major operators have invested in Security Operations Centres (SOCs) staffed 24/7 with cybersecurity professionals trained in both technical response and regulatory compliance — an investment that reflects the increasingly stringent and multi-agency reporting requirements of India's cybersecurity regulatory framework.

CHAPTER 4

The Digital Personal Data Protection Act, 2023

4.1 Legislative History and Structure

The Digital Personal Data Protection Act, 2023 (DPDPA, Act 22 of 2023) was enacted after a lengthy legislative process that began with the Personal Data Protection Bill, 2018 (the "Srikrishna Committee Bill") and went through multiple iterations: the Personal Data Protection Bill, 2019, which was referred to a Joint Parliamentary Committee; the report of the JPC in December 2021, which recommended extensive changes; and the withdrawal of the 2019 Bill in August 2022 and the introduction of the DPDP Bill, 2023, which took a more streamlined approach than the comprehensive 2019 Bill. The DPDPA was passed by the Lok Sabha and the Rajya Sabha in August 2023 and received Presidential assent on 11 August 2023, completing a legislative process of approximately five years from the first draft bill.

The DPDPA represents a fundamental departure from the pre-existing data protection framework (Section 43A of the IT Act, 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011) by establishing a comprehensive, rights-based data protection framework. The Act establishes rights for "data principals" (individuals whose personal data is processed); obligations for "data fiduciaries" (entities that process personal data, including telecom operators); the establishment of the Data Protection Board of India as the enforcement authority; and a framework of civil and criminal sanctions for non-compliance. Telecom operators, as entities that process vast quantities of subscriber personal data (including identity data, location data, call records, and internet browsing data), are significant "data fiduciaries" subject to all the DPDPA's obligations.

The DPDPA's framework is built around the concept of "consent" as the primary legal basis for processing personal data. Data fiduciaries must obtain "free, specific, informed, unconditional and unambiguous" consent from data principals before processing their personal data, expressed through a "clear affirmative action." The Act also provides for "legitimate uses" — specific circumstances in which personal data may be processed without consent, including for compliance with legal obligations (such as law enforcement requests), for vital interests of the data principal, and for specified categories of government processing. Telecom operators process substantial subscriber data for purposes that engage both consent-based and legitimate-use processing: commercial profiling and targeted advertising require consent; compliance with lawful interception directions and subscriber verification requirements are

legitimate uses.

The Act establishes significant rights for data principals that telecom operators must be prepared to honour: the right to information (about what personal data is being processed and for what purposes); the right to correction and erasure of personal data; the right to grievance redressal (through the data fiduciary's nominated grievance officer); and the right to nomination (designating another individual to exercise data rights on behalf of the data principal in specified circumstances). Telecom operators must implement the processes and technical systems needed to respond to data principal rights requests within the timelines prescribed in the implementing rules. Given the scale of subscriber data processed by major telecom operators (potentially hundreds of millions of data records), the technical challenge of implementing erasure rights (the right to have personal data deleted) while maintaining records required by regulatory and legal obligations (such as call records for billing and law enforcement purposes) is significant.

4.2 DPDPA and Telecom Operators: Specific Implications

The intersection of the DPDPA with the telecommunications regulatory framework creates a complex compliance landscape for telecom operators. Operators collect and process subscriber personal data for multiple purposes, each governed by different legal bases: billing and account management (legitimate use, or contractual necessity); network management and quality of service monitoring (legitimate use, or contractual necessity); compliance with lawful interception and data disclosure requirements from law enforcement agencies (legitimate use, legal obligation); marketing and commercial profiling of subscribers for targeted advertising (consent required); sharing subscriber data with third parties including affiliated entities, marketing partners, and technology vendors (consent required, unless covered by a legitimate use); and data analytics and business intelligence using aggregated or anonymised subscriber data (may or may not require consent depending on whether the data remains personally identifiable after aggregation or anonymisation).

The DPDPA's requirements for "significant data fiduciaries" — entities designated by the Central Government as processing personal data at a scale or in a manner that creates significant risks to the rights of data principals — are particularly important for major telecom operators. Significant data fiduciaries are subject to enhanced obligations including: appointment of a Data Protection Officer based in India; data protection impact assessments for high-risk processing activities; and additional compliance requirements to be prescribed by the Data Protection Board. Given the scale of subscriber data processed by India's major telecom operators (involving hundreds of millions of subscribers and potentially billions of data records),

and the sensitivity of the data types involved (location data, communications data, browsing data), it is highly likely that major telecom operators will be designated as significant data fiduciaries under the DPDPA rules.

The DPDPA's financial penalties for non-compliance are substantial: up to Rs. 250 crore for failure to take adequate security measures to prevent data breaches, and up to Rs. 200 crore for failure to report data breaches to the Data Protection Board and affected data principals within the prescribed timelines. For major telecom operators processing hundreds of millions of subscriber records, a large-scale data breach could trigger penalties at these maximum levels, in addition to civil liability to affected data principals and reputational damage. Robust data security measures — including encryption of personal data at rest and in transit, access controls, regular security testing, and comprehensive incident response planning — are not merely compliance obligations but essential business risk management for entities processing personal data at scale.

The interaction between the DPDPA's consent requirements and the telecom sector's existing subscriber agreement framework requires careful legal analysis. Telecom subscribers sign subscriber agreements (Terms and Service/Terms and Conditions) when activating services, which typically include provisions authorising the operator to process subscriber data for specified purposes. The question of whether existing subscriber agreements provide adequate DPDPA-compliant consent — given the Act's requirements for free, specific, informed, unconditional, and unambiguous consent through a clear affirmative action — must be assessed on a case-by-case basis. In many cases, existing agreements will need to be updated to meet the DPDPA's consent standard, requiring operators to obtain fresh consent from their existing subscriber base for specified processing purposes — a commercially and operationally significant exercise for operators with hundreds of millions of subscribers.

4.3 Children's Data Protection in Telecom

The DPDPA contains specific provisions for the protection of children's personal data. A "child" is defined as a person below eighteen years of age for the purposes of the Act. Before processing the personal data of a child, data fiduciaries must obtain verifiable consent from the child's parent or guardian. Data fiduciaries are also prohibited from processing children's data in a manner that is likely to cause harm to the child. Telecom operators face specific challenges in implementing the children's data protection requirements: mobile subscribers include large numbers of persons under eighteen, and the process of verifying age (to distinguish adult subscribers from minors) and of obtaining verifiable parental consent for minors' data processing is both technically and practically complex.

The age verification requirement under the DPDPA connects with the telecom sector's existing subscriber verification (KYC) requirements, which require operators to verify the identity of all subscribers using government-issued identity documents. In principle, the age of a subscriber can be determined from the KYC identity documents. However, the conversion of existing KYC records into DPDPA-compliant age verification — and the development of processes for obtaining and documenting parental consent for minors' data processing across hundreds of millions of subscriber records — is a significant implementation challenge. The rules and notifications under the DPDPA (which were not yet fully enacted as of the preparation of this booklet) will prescribe the specific standards for age verification and parental consent, and telecom operators will need to implement systems complying with these standards within the prescribed timelines.

4.4 The Data Protection Board of India

The Data Protection Board of India, established under the DPDPA, is the enforcement authority for the Act's provisions. The Board adjudicates complaints from data principals about violations of their rights under the Act; inquires into suspected breaches of the Act's provisions by data fiduciaries; and imposes financial penalties for non-compliance. The Board's powers include the ability to conduct inquiries (with access to relevant documents and records), to impose financial penalties in the amounts prescribed in the Schedule to the Act, and to direct remedial action (including the correction of data processing practices that violate the Act). Appeals from the Board's orders lie to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) — a significant allocation of jurisdiction that makes TDSAT the appellate authority for both telecommunications regulatory disputes and data protection enforcement decisions affecting telecom operators.

The allocation of Data Protection Board appeals to TDSAT reflects a recognition that data protection and telecommunications regulation are closely connected for a major sector like telecom, and that the same specialised forum should adjudicate both. It also creates practical complexity: TDSAT's existing docket (of telecom regulatory disputes) will now be supplemented by DPDPA enforcement appeals, potentially across all sectors. The workload implications for TDSAT — and the need for TDSAT Members with expertise in data protection law (in addition to telecommunications engineering, economics, and regulatory law) — are significant. TDSAT reform (discussed in Booklet IV, Chapter 15) must specifically address the expanded mandate conferred by the DPDPA.

CHAPTER 5

Telecom Security Obligations: Licence Conditions and the 2023 Act

5.1 Security Conditions in Unified Licences

The security conditions in India's Unified Licences are among the most operationally demanding and commercially significant compliance obligations faced by telecom operators. These conditions — which were substantially updated in 2022 in the context of the Trusted Telecom Portal framework — impose comprehensive security obligations covering: subscriber verification (KYC/e-KYC requirements for all new and existing subscribers); lawful interception capability (the technical and procedural framework for enabling government-authorised interception of subscriber communications); network equipment security (compliance with the Trusted Telecom Portal's approved equipment requirements); data retention (maintaining specified categories of subscriber and network data for specified periods for law enforcement access); and cooperation with security agencies (providing access to network infrastructure and data as required by lawful directions from designated national security authorities).

The subscriber verification requirements in telecom licence security conditions are among the most extensive identity verification requirements applicable to any commercial sector in India. Telecom operators are required to verify the identity and address of every subscriber before activating mobile or internet services, using government-issued identity documents (Aadhaar-linked e-KYC, or alternative identity documents for persons without Aadhaar). The Aadhaar-based e-KYC system — which enables real-time verification of subscriber identity against the UIDAI's (Unique Identification Authority of India's) biometric and demographic database — has dramatically reduced the time and cost of subscriber verification while improving the accuracy and comprehensiveness of verification. The legal basis for Aadhaar-based e-KYC in the telecom context has been addressed by the Supreme Court's Aadhaar judgment (Justice K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1, the nine-Judge Bench judgment on the constitutional validity of the Aadhaar Act), which permitted the use of Aadhaar-based e-KYC for telecom subscriber verification as a proportionate exercise of the State's authority to regulate telecommunications.

The data retention requirements in telecom licence security conditions require operators to maintain detailed records of subscriber communications — including call detail records (CDRs), internet connection logs, location data, and SMS records — for specified periods, typically

ranging from one year (for CDRs) to two years (for subscriber registration records). These records must be made available to designated national security and law enforcement agencies upon receipt of lawful directions or court orders. The data retention obligations engage the Puttaswamy privacy framework (since they involve the systematic retention of detailed information about subscribers' communications activities without individuated justification) and must be assessed against the proportionality standard — are the retention periods, the categories of data retained, and the access mechanisms proportionate to the legitimate security aims they serve?

The lawful interception capability requirements are technically the most complex security obligations. Telecom operators must deploy and maintain Lawful Interception (LI) equipment throughout their networks — enabling authorised government agencies to intercept (listen to or copy) specific subscribers' communications in real-time or from stored records. The LI framework is standardised internationally through the 3GPP specifications for 3GPP LI (for mobile networks) and the ETSI LI specifications (for other access technologies), and operators' LI implementations must meet the technical specifications prescribed by DoT and the designated national security agencies. LI equipment must be capable of intercepting any subscriber's communications within the time prescribed in an interception direction (typically very rapidly — in some cases within minutes of a direction being issued), and must interface with the designated target collection facilities of the authorised agencies.

5.2 Security Conditions under the Telecommunications Act, 2023

The Telecommunications Act, 2023 carries forward and strengthens the security conditions framework through multiple provisions. Section 22 empowers the Central Government to prescribe security standards for telecommunications equipment and networks, providing the statutory basis for the technical security standards (including the Trusted Telecom Portal framework and equipment type approval standards) that operators must comply with. Section 23 enables the designation of specific network elements as critical telecommunication infrastructure (CTI), with enhanced security obligations applicable to CTI including mandatory security audits, enhanced monitoring, and the possibility of government supervision in emergency situations. Section 24 addresses the interception framework (discussed in Chapter 7). Section 20 provides emergency powers over telecommunications infrastructure (discussed in Chapter 8 in the context of internet shutdowns).

The rules prescribed under Section 22 of the 2023 Act will be the primary legal instrument defining the detailed security compliance obligations for telecom operators under the new framework. These rules will address: the specific security standards for different categories of

network equipment (access network, transmission, core network, OSS/BSS systems); the approved equipment lists and the process for equipment security evaluation under the Trusted Telecom Portal; the requirements for security audits (including the frequency of audits, the qualifications of auditors, and the scope of audit coverage); the incident reporting timelines and formats; and the penalties for security non-compliance. The development of these rules — through a transparent consultation process involving TRAI, CERT-In, NCSC, and industry stakeholders — is one of the most important regulatory development priorities under the 2023 Act.

CHAPTER 6

The Trusted Telecom Portal: Law and Implementation

6.1 The Security Concern and Policy Response

The Trusted Telecom Portal (TTP) was established in 2021 as India's response to growing global concerns about the security of telecommunications equipment, particularly equipment supplied by Chinese vendors. The policy context was the heightened India-China geopolitical tensions following the Galwan Valley clash in June 2020, the prohibition of approximately 300 Chinese mobile applications (under Section 69A of the IT Act) in the same period, and India's alignment with a growing international consensus about the national security risks posed by certain telecom equipment vendors. The UK, US, Australia, Canada, and Sweden had banned or restricted Huawei and ZTE equipment from their 5G networks; India's approach — rather than an outright ban — was to establish an equipment evaluation process (the TTP) through which equipment from all vendors would be assessed for security compliance before being approved for deployment.

The TTP requires telecom operators to obtain approval from the National Cyber Security Coordinator (NCSC), under the Prime Minister's Office, before deploying new telecommunications equipment in their networks. Equipment is evaluated against prescribed security criteria covering hardware security (tamper evidence, secure boot, physical security features), firmware security (code signing, secure update mechanisms, minimality of exposed attack surface), software security (vulnerability scanning, code review, absence of known malware or backdoors), and supply chain security (documentation of the provenance of hardware and software components). Equipment that passes the evaluation is placed on the Trusted Products List (TPL), from which operators may freely procure. Equipment from vendors not on the approved list, or equipment that has not been individually evaluated, may not be deployed in Indian telecom networks.

The implementation of the TTP has required significant coordination between multiple agencies: the NCSC (which administers the TTP and chairs the evaluation committee); CERT-In (which provides technical cybersecurity expertise for equipment evaluations); the Telecom Engineering Centre (which provides technical telecom expertise for evaluations); and DoT (which incorporates TTP compliance into licence conditions and authorisation requirements). Telecom equipment vendors seeking TTP approval must submit detailed technical documentation (including hardware schematics, firmware source code, and supply chain documentation) for

evaluation — a process that raises significant intellectual property concerns for vendors who regard these materials as highly confidential. The TTP's intellectual property protection mechanisms — designed to ensure that submitted documentation is used only for security evaluation purposes and is not disclosed to competitors — are an important aspect of the framework's credibility with international vendors.

The TTP's treatment of existing non-approved equipment — the vast quantities of 2G, 3G, and 4G network equipment deployed in Indian networks before the TTP was established, some of which may be from vendors not on the approved list — has been one of the most commercially contentious aspects of the framework. Operators with large quantities of non-approved legacy equipment face the prospect of significant capital expenditure on equipment replacement over the TTP's phase-out timelines. The government has acknowledged the financial burden and has sought to manage it through phased timelines, but the ultimate obligation to replace non-approved equipment remains. Practitioners advising operators on TTP compliance should carefully assess the scope of phase-out obligations applicable to specific equipment categories and the financial implications for operators' capital expenditure planning.

6.2 Legal Basis and Enforceability

The TTP was initially established on an administrative basis — through NCSC orders and licence condition amendments — rather than through a specific statutory provision. The Telecommunications Act, 2023's Section 22 (power to prescribe security standards for telecommunications equipment) provides the statutory basis for the TTP framework, replacing the previous administrative-only basis with a clear statutory authorisation. This statutory backing strengthens the legal enforceability of TTP obligations and reduces the risk of successful legal challenges to the TTP framework on the ground that it lacks adequate legal authority. Operators who deploy non-approved equipment in breach of TTP requirements will face civil penalties under the 2023 Act's enforcement framework, potentially including forfeiture of bank guarantees and suspension of authorisations in serious cases.

The compatibility of the TTP framework with India's international trade obligations — particularly under the WTO's Agreement on Technical Barriers to Trade (TBT Agreement) — has been raised as a legal question by international telecom equipment vendors. The TBT Agreement requires that technical regulations be based on international standards (where they exist), be non-discriminatory between domestic and imported products, and be no more trade-restrictive than necessary to fulfil legitimate objectives (including national security). India's position is that the TTP is justified by national security — an exception explicitly recognised in the TBT Agreement and in the GATT — and that the evaluation process is non-discriminatory

(applying equally to domestic and imported equipment). Whether the TTP's practical implementation — which has been perceived as affecting Chinese vendors more than others — meets the non-discrimination standard of international trade law is a question that has been raised in bilateral trade discussions.

CHAPTER 7

Lawful Interception and Surveillance: Legal Framework

7.1 Historical Development: PUCL to Puttaswamy

The legal framework for lawful interception in India has evolved through a series of landmark judicial decisions and legislative instruments, from the Supreme Court's foundational judgment in People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (the PUCL Case) to the Puttaswamy judgment and the provisions of the Telecommunications Act, 2023. The PUCL Case arose from a petition challenging the practice of telephone tapping by government agencies — specifically, the revelation that telephone lines of political leaders, journalists, and civil society activists had been tapped without adequate legal authority or procedural safeguards. The Supreme Court held that the right to privacy of telephone conversations is protected under Article 21 and Article 19(1)(a) of the Constitution, and that telephone tapping is a serious invasion of an individual's privacy which cannot be countenanced unless it is permitted by a procedure established by law which is just, fair, and reasonable.

The PUCL Court directed the Central Government to prescribe specific procedural safeguards for telephone interception, which were subsequently incorporated in Rule 419A of the Indian Telegraph Rules, 1951. The Rule 419A framework established: a requirement for written orders signed by the Home Secretary (Union or State level), with grounds for interception specified; a prohibition on disclosure of intercepted information except to the authorized recipients; review of interception orders by a Review Committee (comprising the Cabinet Secretary, Legal Affairs Secretary, and Telecommunications Secretary at the Union level, and equivalent officials at the State level); a maximum duration of 60 days per interception order (extendable by a further 60 days, with a total maximum of 180 days); and destruction of intercepted material after it is no longer required. These safeguards — while improving on the pre-PUCL framework — were criticised by civil liberties organisations as insufficient, primarily because they did not require prior judicial authorisation for interception orders.

The Puttaswamy judgment (2017) raised the constitutional stakes for the interception framework by establishing privacy as a fundamental right subject to a more demanding proportionality standard. Under the Puttaswamy standard, the interception framework must satisfy not only the PUCL requirement of "just, fair and reasonable" procedure but the more specific requirements of legality, legitimate aim, necessity, and proportionality. The question of whether prior judicial authorisation — a requirement in the interception frameworks of many

democratic countries including Germany, France, and the United States (for certain categories of interception) — is constitutionally required under the Puttaswamy standard has been raised in petitions before the Supreme Court and is one of the most significant pending constitutional questions in Indian law.

The Telecommunications Act, 2023's Section 24 — which replaces Section 5(2) of the Indian Telegraph Act, 1885 as the statutory basis for telecommunications interception — preserves the executive authorisation framework while delegating the specific procedural safeguards to rules. The absence of explicit judicial oversight requirements in Section 24 has been challenged before the Supreme Court in petitions that are pending as of the preparation of this booklet. The outcome of these challenges will determine whether Section 24 satisfies the Puttaswamy proportionality standard in its current form, or whether legislative amendment will be required to incorporate judicial oversight or other enhanced safeguards.

7.2 Operational Framework for Interception

The operational framework for lawful interception in India involves multiple agencies with distinct roles. At the authorization level, the Home Secretary (Union or State level, depending on the category of the target) issues written interception orders for specific telephone numbers, email accounts, or internet connections. At the execution level, the telecom operator receives the interception direction through a secure government interface, validates it against the prescribed format and authorization, and enables the interception on the specified communication endpoints using its LI (Lawful Interception) infrastructure. Intercepted communications are transmitted to the Central Monitoring System (CMS), operated by the Centre for Development of Telematics (C-DoT) on behalf of the government, which collects and manages intercept data from all operators' LI systems. From the CMS, designated authorized agencies (the Intelligence Bureau, the Research and Analysis Wing, the National Investigation Agency, and other specified agencies) access the intercepted data for their respective purposes.

The Central Monitoring System (CMS) was established by the government as a centralized interception infrastructure that enables real-time, remote access to intercepted communications from any operator's network, without requiring the operator to manually implement each specific interception request. The CMS model has significant implications for the accountability of interception: in the pre-CMS model, operators had visibility of each specific interception order they implemented, providing them with a degree of independent verification of the interception's authorization. In the CMS model, interception is initiated remotely by the government through the CMS interface, and the operator's role is reduced to maintaining the technical LI infrastructure. This reduction in operator visibility of specific interceptions — and the corresponding reduction in

the operator's ability to identify and flag potentially unauthorised or disproportionate interceptions — has been a concern raised by civil liberties advocates.

CHAPTER 8

Internet Shutdowns: Law, Jurisprudence and Reform

8.1 The Scale of India's Internet Shutdown Problem

India has consistently recorded the highest number of internet shutdowns globally, according to tracking data compiled by organizations such as Access Now (through its KeepItOn campaign) and the Software Freedom Law Centre. The number of shutdowns annually has ranged from dozens to over a hundred in peak years, affecting a wide range of geographic areas from district-level shutdowns in states dealing with localized communal or political unrest to large-scale shutdowns covering entire states or regions (as in Jammu and Kashmir following the revocation of its special constitutional status in August 2019, where an internet shutdown lasted for approximately 18 months in various forms). The economic cost of India's internet shutdowns — estimated by various economic analyses at billions of dollars annually, reflecting the direct losses to digital businesses, e-commerce, fintech, and remote work enabled by internet connectivity — has attracted growing attention from business communities and international economic bodies.

The legal basis for internet shutdowns in India evolved from the colonial-era Indian Telegraph Act, 1885 (whose Section 5(2) was the original authority for suspending telegraph services in public emergency) through the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (which specified the procedure for internet and other telecom service suspensions) to the Telecommunications Act, 2023's Section 5 (which is the successor statutory framework). The 2017 Rules were enacted by the Central Government under Section 7 of the Indian Telegraph Act, 1885, which empowered the government to make rules for carrying out the purposes of the Act. The Rules prescribed the process for issuing suspension orders: only the Home Secretary of the Union (or authorized officers of equivalent rank) could issue orders for national security reasons; State-level orders were issued by State Home Secretaries; orders had to specify the geographic area and duration; and orders were subject to review by a Review Committee within 5 working days.

The 2017 Rules were challenged in the Anuradha Bhasin case and were found by the Supreme Court to be legally valid in their structure, though their application in the Kashmir shutdown was found to be deficient in several respects (including the failure to publish the shutdown orders and the absence of a proportionate justification for the extended geographic and temporal scope of the shutdown). The Court's directions in Anuradha Bhasin effectively

added constitutional requirements to the statutory procedure: publication of orders, proportionality assessment, temporal limitations, and periodic review. Post-Anuradha Bhasin, the government has continued to use internet shutdowns but with greater (though not complete) adherence to the constitutional requirements established by the Court.

The Telecommunications Act, 2023's Section 5 framework for service suspension — and the rules to be prescribed under it — provides an opportunity to codify the Anuradha Bhasin constitutional requirements in formal regulatory instruments, ensuring that the statutory framework for internet shutdowns explicitly incorporates the proportionality, transparency, and periodic review requirements mandated by the Supreme Court. Whether this opportunity is realized in the implementing rules will be one of the key tests of the 2023 Act's commitment to constitutional compliance in the national security and emergency powers domain.

8.2 Economic Consequences and Policy Arguments

The economic consequences of internet shutdowns have been extensively documented by researchers, business associations, and international bodies, and are increasingly being incorporated into the legal and policy arguments against disproportionate shutdowns. A 2021 study by the Indian Council for Research on International Economic Relations (ICRIER) estimated that India's internet shutdowns between 2012 and 2017 cost the economy approximately USD 3.04 billion. A 2021 report by the Internet Society and NetBlocks estimated that each day of a state-wide internet shutdown in India costs the economy between USD 17.6 million and USD 20 million. These economic costs — which fall disproportionately on small businesses, independent workers, students, and individuals in the affected areas who depend on internet connectivity for their livelihoods — are directly relevant to the proportionality assessment: a shutdown measure that imposes disproportionate economic harm on the population it purports to protect, relative to the security benefit it achieves, fails the constitutional proportionality test.

The policy argument for internet shutdowns — that they prevent the spread of misinformation, incitement to violence, or coordination of criminal activity during sensitive periods — has been critically assessed by researchers who have found limited evidence for these effects and significant evidence for harmful consequences, including: displacement of social media activity to less-well-regulated channels; inability to access emergency services, banking, healthcare information, and government services; economic harm to local businesses and workers; and political harm through the silencing of legitimate political expression. These findings inform the proportionality analysis: where the claimed justification for a shutdown is not demonstrably effective at achieving its stated goal, the proportionality requirement — that the

measure must be necessary to achieve the legitimate aim — cannot be satisfied.

CHAPTER 9

National Security and Telecom: Institutional Framework

9.1 Key National Security Agencies in the Telecom Context

The national security dimensions of telecommunications regulation involve multiple agencies with distinct mandates. The National Cyber Security Coordinator (NCSC), located in the Prime Minister's Office, is the apex coordinator for India's cybersecurity policy, overseeing both the Trusted Telecom Portal and the broader national cybersecurity strategy. The Intelligence Bureau (IB), under the Ministry of Home Affairs, is responsible for domestic intelligence gathering, including the collection of telecommunications intelligence relevant to internal security threats. The Research and Analysis Wing (R&AW;), under the Cabinet Secretariat, is responsible for foreign intelligence, including signals intelligence (SIGINT) gathered through the monitoring of foreign communications. The National Technical Research Organisation (NTRO), under the Prime Minister's Office, is India's technical intelligence agency responsible for SIGINT collection and technical operations. The Defence Intelligence Agency (DIA), under the Ministry of Defence, handles defence intelligence including the security of military communications networks.

Each of these agencies has access to telecommunications networks for intelligence collection purposes, under the authorization frameworks of the Telecommunications Act, 2023 (Section 24, for interception of specific communications) and the Information Technology Act, 2000 (Section 69, for interception and monitoring of information in computer resources). The coordination between these agencies — ensuring that multiple agencies are not simultaneously intercepting the same targets, that collected intelligence is shared appropriately, and that the total scale of surveillance is within constitutional proportionality limits — is managed through the National Intelligence Coordination Committee and the Joint Intelligence Committee at the highest levels, and through inter-agency technical protocols at the operational level. The legal framework for this inter-agency coordination is not fully publicly disclosed, raising transparency concerns that have been noted by civil liberties advocates and international human rights bodies.

The telecommunications sector's obligations towards national security agencies extend beyond lawful interception to include: providing network access for monitoring and testing purposes to designated security agencies; notifying security agencies of any planned network changes that might affect security capabilities; cooperating with network security audits conducted by authorised government security assessment bodies; and implementing any security modifications or upgrades directed by the designated authority in the interests of

national security. These obligations — which go beyond the formal interception framework — represent a significant ongoing relationship between telecom operators and national security agencies that must be managed carefully to maintain both compliance and commercial operations.

CHAPTER 10

Encryption Law and Telecom

10.1 The Regulatory Framework for Encryption

Encryption — the mathematical transformation of data into a form unreadable without the appropriate key — is both a critical cybersecurity tool (protecting sensitive data from unauthorised access) and a significant regulatory challenge for law enforcement and national security agencies (since encrypted communications cannot be monitored even with a valid interception order). India's approach to encryption regulation has been shaped by the tension between these competing imperatives: the government has a strong interest in preserving its ability to monitor communications for national security and law enforcement purposes, while businesses, citizens, and cybersecurity professionals have an equally strong interest in using robust encryption to protect sensitive data, financial transactions, and private communications from malicious actors including criminals, foreign intelligence services, and commercial data thieves.

India does not have a comprehensive encryption law, unlike some countries that have enacted specific legislation governing the use of encryption (such as Australia's Assistance and Access Act, 2018 and China's Cryptography Law, 2019). Encryption regulation in India is primarily addressed through telecom licence conditions (which historically imposed a restriction on the use of encryption with key lengths exceeding 40 bits without the encryption key being deposited with a designated authority — a restriction that was widely ignored and is now obsolete given the universal use of AES-256 and other strong encryption standards) and through CERT-In's guidelines on information security (which recommend the use of strong encryption but do not specify a mandatory encryption standard). The practical reality of encryption regulation in India is that strong end-to-end encryption — as used in WhatsApp, Signal, and other messaging applications — is widely used by hundreds of millions of Indian users without any regulatory restriction, notwithstanding the licence conditions that nominally restrict encryption.

The question of whether the government can compel telecom operators and messaging application providers to provide "backdoor" access to encrypted communications — or to weaken their encryption to enable government monitoring — is one of the most contested issues in global technology policy. India's government has at various times expressed interest in requiring messaging platforms to provide traceability of encrypted messages (enabling identification of the "first originator" of viral messages) without necessarily decrypting message

content, as a middle ground between preserving end-to-end encryption for ordinary users and maintaining a degree of law enforcement access for serious security threats. The TRAI's consultation on the traceability framework and the legal challenges to the IT (Intermediary Guidelines) Rules' traceability requirement (discussed in Chapter 2) illustrate the ongoing regulatory debate about the appropriate balance between encryption and lawful access in India.

The Telecommunications Act, 2023 does not directly address encryption regulation, leaving this to the implementing rules and to TRAI's regulatory framework. The Act's interception provisions (Section 24) assume that the government can access the content of intercepted communications — an assumption that becomes increasingly untenable in a world where most communications are end-to-end encrypted. The development of a legally coherent and constitutionally sound framework for government access to encrypted communications — one that satisfies the Puttaswamy proportionality standard while preserving effective security monitoring capabilities — is one of the most important and difficult legal challenges in Indian telecommunications and cybersecurity law.

CHAPTER 11

Cross-Border Data Flows and Localisation

11.1 Data Localisation in Indian Law

Data localisation — requirements that certain categories of data relating to Indian persons or processed in India must be stored or processed within India's geographic boundaries — has been a recurring and contentious aspect of India's data governance policy. The RBI's 2018 circular requiring all payment system operators to store payment system data exclusively in India set an important precedent for sector-specific localisation mandates. The SEBI's cloud computing circular requires financial firms to use data localisation measures for regulated activities. The DPDPA's approach to data localisation is more nuanced: rather than imposing a blanket localisation requirement, the Act empowers the Central Government to restrict the transfer of personal data to specified countries (which would effectively require localisation of data relating to transfers restricted countries' residents). The Act also enables the government to require certain data fiduciaries to store specified classes of personal data within India, as a supplementary protective measure.

Telecom operators are particularly affected by data localisation requirements because of the global nature of telecommunications networks and the international standards governing data management in telecom. Subscriber data — including call records, location data, and internet browsing data — may be processed in multiple countries as part of the operator's global operations, including for billing, network management, fraud detection, and customer care. Strict localisation requirements that mandate storage of all subscriber data within India would require significant changes to the data architectures of multinational operators with Indian operations, potentially requiring investment in India-based data centres and changes to global data management processes.

The relationship between DPDPA data localisation provisions and the telecom sector's existing data retention requirements under licence security conditions is an important interaction. Licence security conditions already require operators to retain specified categories of subscriber data within India (for law enforcement access purposes), creating a partial de facto localisation requirement for the most security-sensitive data categories. The DPDPA's provisions — if they result in further localisation requirements — would add to these existing obligations, potentially creating a comprehensive localisation framework for telecom subscriber data.

11.2 International Data Transfers and Adequacy

The DPDPA's framework for cross-border data transfers — allowing transfers to countries and territories that the Central Government specifies as providing adequate data protection — follows the model of GDPR-influenced data protection frameworks globally. Transfers to non-specified countries would require specific safeguards (such as contractual data protection clauses, binding corporate rules, or individual consent). The Central Government's power to specify "adequate" countries for data transfers creates an important regulatory tool for India's digital trade policy: India can use the adequacy designation process to negotiate reciprocal data protection arrangements with trading partners, and can withhold adequacy designations to leverage compliance with India's data localisation requirements.

For telecom operators engaged in international long-distance services, the transfer of subscriber data to foreign correspondents (international carriers, roaming partners, submarine cable operators) is an operational necessity. The legal basis for these transfers under the DPDPA framework will need to be carefully assessed: some transfers may qualify as legitimate uses under the Act (transfers necessary for the performance of contracts with foreign entities or for compliance with international treaties), while others may require specific subscriber consent or adequacy-equivalent safeguards. The telecom industry associations are actively engaging with the government on the operational implications of the DPDPA's international transfer provisions for the sector's global operations.

CHAPTER 12

Critical Information Infrastructure Protection

12.1 The Telecom Sector as CII

The telecommunications sector has been formally designated as a critical information infrastructure (CII) sector in India's national cybersecurity policy framework. This designation reflects the fundamental dependence of all other critical sectors — power, banking, healthcare, transportation, and government services — on telecommunications infrastructure for their own operations. A serious, sustained attack on India's telecommunications infrastructure could disrupt these dependent sectors simultaneously, creating cascading effects on national security, economic stability, and public welfare. The telecom sector's CII status imposes enhanced security obligations on operators and creates a framework for sector-specific cybersecurity preparedness and incident response.

NCIIPC's mandate for telecom sector CII protection involves several key activities: conducting threat and vulnerability assessments of designated CII systems; developing sector-specific guidelines and best practices for telecom CII protection; coordinating with DoT, CERT-In, and the major telecom operators on incident preparedness and response; and monitoring the global threat landscape for cyber threats specifically targeting telecom infrastructure. NCIIPC works with a Sectoral Computer Emergency Response Team (Sectoral CERT) for the telecommunications sector, which provides technical incident response support to telecom operators experiencing cyber attacks on their CII.

The practical implementation of CII protection requirements by telecom operators involves several layers of security controls: physical security of critical facilities (data centres, core network nodes, landing stations); logical security of network management systems (access controls, encryption, anomaly detection); supply chain security (trusted equipment requirements under the TTP framework, vendor security assessments); resilience and redundancy (backup power, network redundancy, disaster recovery capabilities); and incident response planning (tested incident response plans, communication protocols with NCIIPC and CERT-In, and exercised disaster recovery procedures). The cost of implementing these multi-layer security controls is substantial, particularly for small and medium-scale operators who may not have the financial resources or technical expertise of major operators.

CHAPTER 13

Cybercrime and Telecom: Investigative Framework

13.1 Telecom as Investigative Target and Tool

Telecommunications data — including call records, location data, subscriber identity information, and internet connection logs — is among the most valuable categories of evidence in criminal investigations. The reconstruction of a suspect's movements and communications through mobile network location records and call detail records has become a standard element of serious crime investigations in India, from murder and terrorism cases to financial fraud investigations and organized crime prosecutions. Telecom operators are accordingly in a position of dual significance in the investigative framework: they are both potential targets of investigation (when criminal activity involves their networks or employees) and essential investigative partners (through the provision of subscriber data and communications records to law enforcement agencies).

The legal framework governing law enforcement access to telecom subscriber data and communications records involves multiple instruments. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS, which replaced the Code of Criminal Procedure) provides the framework for search warrants, production orders, and other court-ordered access to evidence. The Telecommunications Act, 2023's security conditions (carried forward from existing licence conditions) require operators to retain subscriber data for specified periods and to provide access to that data to designated law enforcement agencies upon receipt of lawful directions. The Information Technology Act's provisions on computer-related evidence (Sections 65A and 65B) address the admissibility of electronic records in court proceedings, which is directly relevant to the use of telecom data records as evidence.

The I4C (Indian Cyber Crime Coordination Centre), established under the Ministry of Home Affairs, coordinates the investigation and prosecution of cybercrime across India's multiple law enforcement jurisdictions. The I4C's National Cyber Crime Reporting Portal (NCRP) enables citizens to report cyber crimes online, and the portal's data is used by law enforcement agencies to identify trends, allocate investigative resources, and coordinate responses to large-scale cyber crime campaigns. Telecom operators interface with the I4C framework through their cooperation with cybercrime investigations, the provision of subscriber data in response to court orders and lawful directions, and their participation in awareness campaigns about telecom fraud (including SIM swap fraud, phishing calls, and one-time password interception attacks).

CHAPTER 14

Emerging Security Challenges: AI, IoT and 5G

14.1 AI and Network Security

Artificial intelligence (AI) is transforming both the attack capabilities of malicious actors and the defensive capabilities of network defenders. On the attack side, AI-powered cyber attack tools can automate the discovery and exploitation of vulnerabilities at speeds and scales that human attackers cannot match. AI-generated phishing messages and social engineering attacks — capable of producing convincing fake communications indistinguishable from genuine operator messages or government notifications — create new vectors for subscriber fraud and unauthorized SIM swaps. AI-driven distributed denial-of-service (DDoS) attacks can adapt their traffic patterns in real-time to evade traditional signature-based defences, requiring AI-based countermeasures. The use of AI for OSINT (open-source intelligence) gathering — aggregating publicly available information about network infrastructure to identify vulnerabilities for exploitation — presents a persistent reconnaissance threat to telecom operators' network management systems.

On the defensive side, AI-based network security tools are increasingly essential for telecom operators managing the massive scale and complexity of modern telecommunications networks. Machine learning models trained on network traffic data can identify anomalous patterns (indicating DDoS attacks, botnet activity, or infiltration by advanced persistent threats) far more quickly than human analysts examining network logs. AI-powered Security Operations Centres (SOCs) can correlate security events across multiple data sources — network logs, endpoint detection systems, subscriber databases, and threat intelligence feeds — to identify complex multi-stage attacks that would be invisible to traditional event-based monitoring. The Telecommunications Act, 2023's security standards framework will need to address AI-based security tools — including both the use of AI for network security and the regulatory treatment of AI-generated threats.

The regulatory treatment of AI in telecommunications security is an emerging area where India's framework is still developing. TRAI's 2023 consultation paper on "AI in Telecom" was the first systematic regulatory engagement with the implications of AI for the sector, addressing both the use of AI by operators for network management and service personalisation and the implications of AI for cybersecurity, consumer protection, and regulatory compliance. The recommendations from this consultation — when finalised — will inform the development of rules

under the Telecommunications Act, 2023 addressing AI-specific security and compliance obligations for telecom operators.

14.2 IoT Security and Telecom

The Internet of Things (IoT) — the connection of billions of physical devices (from smart meters and industrial sensors to consumer appliances and vehicles) to the internet — creates both a massive new market for telecommunications services and a significant new security challenge. IoT devices are typically manufactured with minimal security features (due to cost and resource constraints), may run outdated or unpatched software, and are often deployed in environments where physical access is difficult and software updates are infrequent. Compromised IoT devices can be recruited into botnets for DDoS attacks, used as entry points for network infiltration, or exploited for surveillance (particularly IoT cameras and microphones). The scale of IoT device deployment — projected at tens of billions of devices globally within a decade — means that a systematic vulnerability in a widely-deployed IoT device class can create security risks of extraordinary magnitude.

Telecom operators are central to IoT security in their capacity as connectivity providers: the cellular networks (particularly NB-IoT and LTE-M technologies optimised for IoT) and fixed broadband networks through which IoT devices connect to the internet provide a potential choke point for security intervention. Operators can implement network-level IoT security measures including: network segmentation (isolating IoT device traffic from sensitive network segments); anomaly detection (identifying unusual traffic patterns from IoT devices that may indicate compromise); and DNS filtering (blocking communications to known malicious command-and-control servers). The implementation of these network-level IoT security measures is both a commercial opportunity for operators (as a value-added security service for enterprise IoT customers) and a regulatory requirement (under the security conditions of their licences and the CERT-In directives on IoT security).

CHAPTER 15

Reform Priorities and International Alignment

15.1 Consolidating the Security Regulatory Framework

The most important reform priority for India's telecommunications cybersecurity regulatory framework is consolidation and coherence. The current framework is fragmented across multiple statutes (the IT Act, the Telecommunications Act, 2023, and the DPDPA), multiple agencies (CERT-In, NCSC, NCIIPC, DoT, and TRAI), and multiple instruments (licence conditions, CERT-In directions, TTP requirements, and DPDPA obligations). This fragmentation creates duplication, gaps, and inconsistencies that impose unnecessary compliance costs on operators and reduce the overall effectiveness of the security framework. A comprehensive review aimed at consolidating the telecommunications cybersecurity framework — identifying overlaps, harmonising obligations, and creating clear institutional responsibilities — is an urgent priority.

The review should specifically address: the relationship between the IT Act's Section 70 CII framework and the Telecommunications Act, 2023's CTI framework; the coordination between CERT-In's incident reporting requirements and the licence-based security incident reporting obligations; the relationship between the DPDPA's data breach notification requirements and the telecom security incident reporting obligations; and the alignment of the TTP security evaluation standards with international standards (GSMA, 3GPP, and ETSI security specifications) to reduce the duplication of security evaluation requirements for globally-standardised telecom equipment. The goal should be a single, coherent telecommunications cybersecurity compliance framework that operators can understand, implement, and demonstrate compliance with — reducing both the cost and the complexity of security regulation.

15.2 Judicial Oversight and Privacy Protection

The introduction of meaningful judicial oversight for telecommunications interception orders — replacing or supplementing the current executive authorisation-only framework — is the most important reform for bringing India's interception framework into alignment with constitutional privacy standards and international human rights law. The specific form of judicial oversight that is most appropriate for India's constitutional and administrative context is a matter for legislative design: options include a requirement for prior judicial authorisation (issued by a designated High Court judge) for all interception orders above a minimum severity threshold; a specialised surveillance court (modelled on the US Foreign Intelligence Surveillance Court) for national

security interceptions; or a strengthened ex post review mechanism with more robust investigation capacity and transparency obligations. Whatever form judicial oversight takes, it must provide a genuine independent check on the executive's interception powers — not merely a rubber-stamp process that approves every executive request.

The development of a meaningful internet shutdown governance framework — one that gives effect to the Anuradha Bhasin constitutional requirements and that creates institutional accountability for shutdown decisions — is equally important. Specific reform measures should include: a statutory requirement for shutdown orders to be published in real-time on a government portal, accessible to the public and to courts; an express provision for emergency High Court review of shutdown orders (with a fast-track procedure enabling review within 24-48 hours); mandatory post-shutdown reporting to Parliament on the reasons, duration, and assessed effectiveness of each shutdown; and a data collection requirement enabling comprehensive analysis of shutdown impacts on the economy and on fundamental rights. These measures would not eliminate internet shutdowns but would create the transparency and accountability mechanisms needed for meaningful constitutional oversight.

15.3 India's International Alignment

India's telecommunications security framework should be aligned with the growing body of international standards and best practices for telecommunications cybersecurity. The Budapest Convention on Cybercrime — which India has not yet acceded to — provides a framework for international law enforcement cooperation on cybercrime, including mutual legal assistance for access to electronic evidence. India's accession to the Budapest Convention (or to its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence) would improve India's ability to cooperate with international partners in cybercrime investigations while also requiring India to align its domestic cybercrime and telecommunications investigation framework with the Convention's standards. The accession process would itself be a valuable exercise in assessing the alignment of India's domestic legal framework with international cybercrime law standards.

India's engagement with international telecommunications security standards — through the ITU, GSMA, 3GPP, and ETSI — is already substantial and should be deepened. The adoption of internationally harmonised security standards for telecommunications equipment (rather than India-specific standards that diverge from international norms without adequate security justification) would reduce the compliance burden for global equipment vendors and operators, improve the international interoperability of India's telecommunications networks, and facilitate India's participation in global trusted ecosystem discussions. The goal of making India's

telecommunications security framework not only domestically effective but internationally credible — recognised by trading partners, investment destinations, and allied governments as meeting world-class security standards — is a strategic objective that should guide the ongoing development of India's cybersecurity regulatory framework for the telecommunications sector.

SUPPLEMENTARY NOTE A

Cybersecurity Compliance: Advanced Analysis

A.1 Incident Response Planning for Telecom Operators

Effective incident response planning is both a regulatory requirement (under CERT-In directions, licence security conditions, and the DPDPA's data breach notification framework) and an essential operational capability for telecommunications operators managing complex, large-scale networks. A mature incident response plan for a major telecom operator should address the full incident lifecycle: preparation (establishing the incident response team, defining roles and responsibilities, implementing monitoring tools and detection capabilities, conducting regular drills and exercises); detection and analysis (identifying security incidents from network monitoring alerts, user reports, and threat intelligence feeds; classifying incidents by severity; analysing the scope and impact of identified incidents); containment and eradication (isolating affected network segments to prevent further spread, removing malware or restoring compromised systems to a known good state); recovery (restoring affected services and verifying the integrity of restored systems); and post-incident review (analysing the root cause, identifying lessons learned, and updating security controls and response procedures to prevent recurrence).

The regulatory notification requirements for cybersecurity incidents create specific timing and content obligations that must be built into the incident response plan. Under CERT-In's 2022 Directions, specified categories of serious cybersecurity incidents must be reported to CERT-In within six hours of discovery. The "discovery" threshold — at what point an operator has "discovered" an incident sufficient to trigger the reporting obligation — is an important interpretive question: does discovery occur when the first anomalous log entry is observed (which may be hours before the full nature of the incident is understood), or when enough information has been gathered to confirm that a reportable incident has occurred? The answer has significant practical implications for incident response teams: if the six-hour clock starts from the first anomalous observation, there may be insufficient time to gather the information needed for an accurate initial report. CERT-In's guidance suggests that the reporting obligation is triggered by

reasonable belief that a reportable incident has occurred, and that initial reports can be updated as further information becomes available — a reasonable interpretation that reduces the risk of operators either under-reporting (by delaying beyond six hours until the full picture is available) or over-reporting (by submitting premature reports on events that turn out not to be reportable incidents).

The coordination of cybersecurity incident responses with commercial operations decisions — specifically the decision of whether and when to notify the public about a cybersecurity incident, and whether to take operational network actions (such as blocking specific IP address ranges or disconnecting specific network elements) that may affect service quality for subscribers — creates complex governance questions for telecom operators. The DPDPA's data breach notification requirements create an obligation to notify affected data principals "as soon as possible" following a data breach, but the specific timeline and the threshold of harm that triggers the notification requirement are to be prescribed in rules. Where a cybersecurity incident involves both a potential security breach (requiring CERT-In notification within six hours) and a personal data breach (requiring DPDPA notification to the Data Protection Board and potentially to affected subscribers), operators face simultaneous notification obligations to different authorities on different timelines. The development of integrated incident notification workflows — covering all regulatory notification obligations in a single coordinated process — is an important component of mature incident response capability for telecom operators.

A.2 Supply Chain Security for Telecom Equipment

Supply chain security — the protection of the telecom network equipment supply chain from deliberate compromise (through the insertion of malicious hardware or software components) or inadvertent security degradation (through poor security practices in the manufacturing or distribution process) — is one of the most complex and commercially sensitive cybersecurity challenges for the telecommunications sector. The concern about supply chain compromise is not merely theoretical: intelligence agencies in multiple countries have reported that advanced persistent threat (APT) groups have targeted telecom equipment supply chains, inserting malicious firmware or hardware implants in equipment destined for specific customer networks. The scale and sophistication of these supply chain attacks — which exploit the complexity of the global electronics manufacturing industry (with components typically sourced from dozens of countries and assembled in highly specialised facilities) — makes traditional perimeter-security approaches inadequate for supply chain protection.

The Trusted Telecom Portal framework addresses supply chain security through a security evaluation process that covers not only the functional security of finished equipment but also the

security of the supply chain that produced it. TTP evaluators assess: the vendor's supply chain risk management programme (the procedures used to vet component suppliers, manufacturing partners, and software development subcontractors); the bill of materials for submitted equipment (identifying all hardware and software components and their sources); the firmware signing and update mechanisms (verifying that firmware updates can only be installed if they are cryptographically signed by the vendor using a secured signing key); the hardware security features (including physical security measures that prevent or detect tampering with the physical device); and the vendor's software development life cycle (including security review processes, vulnerability disclosure and patching procedures, and the security of the source code management environment). This comprehensive evaluation approach — going beyond traditional functional testing to assess the security of the entire development and manufacturing process — reflects the sophisticated threat model that drives supply chain security concerns.

The cost implications of comprehensive supply chain security evaluation for telecom equipment are significant. Equipment vendors must invest in their supply chain security programmes (developing processes, documentation, and auditing capabilities that meet TTP requirements), in the security evaluation process itself (engaging approved evaluation laboratories, preparing evaluation documentation, and supporting the evaluation team during the assessment), and in the post-evaluation maintenance of approved status (updating security documentation when hardware or software changes are made, reporting and remediating discovered vulnerabilities, and undergoing periodic reassessment). These costs are ultimately reflected in equipment prices — making TTP-approved equipment potentially more expensive than non-evaluated alternatives — and in longer time-to-market for new equipment models (since evaluation takes time that delays commercial deployment). The regulatory framework must balance the security benefits of comprehensive evaluation against the commercial costs of lengthy, expensive evaluation processes that may delay the deployment of innovative new equipment and may deter smaller equipment vendors from seeking approval.

A.3 Data Protection Compliance Programme

Implementing a comprehensive Data Protection Compliance Programme (DPCP) for a major telecom operator under the DPDPA, 2023 framework requires systematic attention to all dimensions of the data protection obligations: governance (establishing a Data Protection Officer, a data protection committee, and clear accountability for data protection compliance throughout the organisation); policy (developing and maintaining data processing policies, consent management procedures, data retention schedules, and data subject rights response procedures that meet the DPDPA's requirements); technical controls (implementing encryption,

access controls, anonymisation, pseudonymisation, and other technical measures that protect personal data against unauthorised access and use); process (embedding data protection requirements in all business processes that involve personal data — including subscriber onboarding, service delivery, marketing, billing, and network management); and supplier management (ensuring that third-party processors of personal data on behalf of the operator meet equivalent data protection standards through contractual data processing agreements and regular assessments).

The Data Protection Impact Assessment (DPIA) process — required for "significant data fiduciaries" under the DPDPA and recommended for all high-risk data processing activities — is an important tool for systematic identification and mitigation of data protection risks in new products, services, and processing activities. A DPIA for a new telecom service (such as a 5G IoT connectivity service that collects detailed real-time location and usage data from connected devices) should systematically assess: the nature and scope of the personal data to be processed; the purposes and legal bases for the processing; the risks to data principals arising from the processing (including risks of misuse, unauthorised access, discrimination, and loss of control over personal information); the measures implemented to mitigate those risks; and the residual risk after mitigation measures are in place. The DPIA process should involve privacy law specialists, technical security experts, and business stakeholders — ensuring that privacy considerations are integrated into product design from the outset ("privacy by design") rather than addressed as an afterthought after the product has been developed.

The consent management framework under the DPDPA is one of the most operationally challenging aspects of compliance for telecom operators with hundreds of millions of subscribers. The Act requires "free, specific, informed, unconditional and unambiguous" consent expressed through a "clear affirmative action" before processing personal data for purposes beyond those directly necessary for the service contracted for. In practice, this means that operators cannot rely on pre-ticked boxes, bundled consent clauses in general terms and conditions, or implied consent from continued service usage as valid consent under the DPDPA. Instead, operators must implement purpose-specific consent mechanisms — clearly communicating to subscribers what data is to be processed, why, and with what consequences, and providing a clear, active mechanism (clicking a button, checking a box, providing a written response) to express consent. The development of subscriber-facing consent management interfaces that are both legally compliant (meeting the DPDPA's consent standard) and commercially effective (not creating so much friction that they drive subscribers away from valuable services) is a significant product design and compliance challenge that operators are

currently addressing through digital consent management platforms.

A.4 The DPDPA and Law Enforcement Access to Subscriber Data

One of the most legally complex aspects of the DPDPA's application to telecom operators is the interaction between the Act's data protection obligations and the obligations of operators to provide access to subscriber data to law enforcement agencies and national security authorities. Telecom operators regularly receive requests — some in the form of court orders, some in the form of statutory directions from designated authorities, and some in less formal forms — to provide subscriber data including call records, location data, subscriber identity information, and internet connection logs. Under the previous (pre-DPDPA) framework, operators' obligations to respond to such requests were governed primarily by their licence conditions and by Section 69B of the IT Act, with limited regulatory guidance on the procedural requirements that must be met before compliance.

Under the DPDPA framework, the provision of subscriber data to law enforcement and national security authorities falls within the "legitimate use" category of Section 7 of the Act — specifically, the legitimate use for "compliance with any obligation under any law." This means that operators are legally authorised to provide subscriber data to law enforcement in response to lawful requests without subscriber consent, provided that the request meets the requirements of the "applicable law" — i.e., the specific statutory provision (such as Section 69 of the IT Act, or the provisions of the Bharatiya Nagarik Suraksha Sanhita governing production of documents) that authorises the access. The DPDPA's "legitimate use" exception does not, however, authorise operators to provide subscriber data in response to informal requests (without statutory authority) or to requests that exceed the scope of the applicable statutory provision. Operators must therefore develop robust internal review processes for evaluating law enforcement data requests — verifying the statutory authority cited, confirming that the request is within the scope of that authority, and maintaining records of all requests and responses for audit purposes.

SUPPLEMENTARY NOTE B

Cybersecurity and Privacy: Advanced Analysis

B.1 Zero-Day Vulnerabilities and Telecom Network Security

Zero-day vulnerabilities — software or hardware flaws that are unknown to the vendor and for which no patch has been developed — represent the highest-severity category of cybersecurity risk for telecommunications networks. Because no patch exists for a zero-day

vulnerability until it is discovered and a fix is developed (a process that can take days to months), networks remain exposed to exploitation for an indefinite period. Zero-day vulnerabilities in core network equipment — such as flaws in the routing software of backbone routers, the authentication mechanisms of core network functions, or the protocol implementations of base station firmware — can enable sophisticated attackers to intercept communications, redirect traffic, or disrupt service at a fundamental level that cannot be defended against by perimeter security measures alone. The discovery and exploitation of zero-day vulnerabilities in telecommunications equipment by nation-state actors has been documented in multiple publicly reported incidents, and is considered by intelligence agencies globally to be one of the primary vectors for telecommunications network compromise.

India's regulatory framework for zero-day vulnerability management in telecommunications networks is developing but not yet comprehensive. CERT-In's guidelines on vulnerability disclosure and patch management provide general direction, and the TTP framework's requirement for vendors to maintain vulnerability management programmes (including defined processes for vulnerability discovery, disclosure, patch development, and customer notification) creates a baseline expectation for vendor-side vulnerability management. However, the operator-side requirements for zero-day response — the procedures that operators must follow when informed of a zero-day vulnerability in deployed equipment — are less clearly defined. The critical question is: when a zero-day vulnerability is discovered in deployed network equipment, what must the operator do? The options range from immediate network shutdown (catastrophically disruptive but maximally protective) to continued operation with enhanced monitoring pending patch availability (operationally sustainable but leaving the vulnerability exposed). The development of a graduated zero-day response framework — specifying different response requirements based on the severity of the vulnerability, the availability of compensating controls, and the imminence of active exploitation — would provide operators with clearer guidance on their regulatory obligations while maintaining the flexibility needed for practical vulnerability management.

The Coordinated Vulnerability Disclosure (CVD) framework — a widely adopted international best practice for managing the responsible disclosure of newly discovered vulnerabilities — has not been formally incorporated into India's telecommunications security regulatory framework. Under CVD, a researcher who discovers a vulnerability in telecommunications equipment is expected to notify the vendor privately before publicly disclosing the vulnerability, giving the vendor time to develop and deploy a patch before the vulnerability is publicly known. The vendor is expected to acknowledge the report, develop a patch within a reasonable period, and

coordinate the public disclosure with the researcher. India's adoption of a formal CVD framework for telecommunications equipment — potentially administered by CERT-In in coordination with the TTP and the WPC Wing — would improve the security of India's telecommunications infrastructure by incentivising responsible vulnerability disclosure and ensuring that patches are developed and deployed before vulnerabilities are publicly exploited.

B.2 The Privacy-Security Tension in Telecom Data

The tension between privacy protection and national security access to telecommunications data is one of the defining regulatory challenges of the digital age, and India's constitutional and statutory framework for managing this tension is still evolving in important ways. The Puttaswamy judgment's establishment of privacy as a fundamental right subject to the proportionality standard creates constitutional constraints on government surveillance that apply directly to the telecommunications sector's data retention and disclosure obligations. But the same constitutional framework recognises national security as a legitimate aim that can justify restrictions on privacy — the question is always whether the specific surveillance measure is proportionate to the security objective it serves. The answer to this question depends on the specific measure: targeted interception of a specific suspect's communications (highly proportionate) is very different from bulk collection of all subscribers' location data for general intelligence purposes (potentially disproportionate if less intrusive alternatives are available).

The data minimisation principle — a core principle of data protection law that requires collecting and retaining only the personal data that is necessary for the specific purpose — creates a constraint on telecommunications security data retention requirements. The current licence condition requirement to retain call detail records for twelve months and internet connection logs for two years represents a significant quantity of personal data retained about every subscriber, regardless of whether they are subject to any security investigation. The proportionality of these blanket retention requirements — compared to a more targeted approach (retaining data about specific persons subject to security investigation, rather than retaining data about all subscribers) — has been the subject of legal challenge in several European jurisdictions, where courts have struck down mandatory blanket data retention as disproportionate under the EU Charter of Fundamental Rights. India's Puttaswamy-based proportionality framework raises similar questions about the constitutional adequacy of blanket data retention requirements for all telecommunications subscribers.

The development of a proportionate telecommunications data retention framework for India — one that satisfies both the security access requirements of law enforcement and intelligence agencies and the privacy rights of subscribers — is a complex regulatory design challenge.

Potential elements of a proportionate framework include: targeted data retention (retaining detailed records only for specific categories of subscribers subject to investigation, with general retention of aggregate traffic data that cannot identify individual subscribers); expedited preservation orders (requiring operators to preserve specific data relating to specific investigations for defined periods, rather than retaining all subscriber data indefinitely); and a defined legal process for access to retained data (requiring judicial authorisation or equivalent oversight for access to retained personal data, rather than executive-only access). The design of such a framework must also address the practical operational requirements of law enforcement agencies, who need reliable and timely access to telecommunications data for time-sensitive investigations — a requirement that constrains the extent to which data minimisation principles can be applied without compromising investigative effectiveness.

B.3 Geopolitical Dimensions of Telecom Security

The geopolitical dimension of telecommunications security — the use of telecommunications infrastructure as an instrument of statecraft, intelligence collection, and economic competition by nation-states — has become a dominant consideration in telecom regulatory policy globally. India's telecommunications security framework, including the Trusted Telecom Portal and the broader national security provisions of the Telecommunications Act, 2023, must be understood in the context of India's geopolitical situation: a large, technologically sophisticated democracy with complex relationships with its neighbours (particularly China and Pakistan), significant strategic partnerships with Western democracies (the US, UK, Australia, France, and others), and growing technological capacity that makes India both a potential target and a participant in the global contest for technological leadership.

The Indo-China technology competition — which has accelerated significantly since the 2020 border confrontation — has directly shaped India's telecommunications security policy. India's progressive restriction of Chinese telecom equipment vendors (through the Trusted Telecom Portal's evaluation process) from India's 5G network rollout, combined with the prohibition of hundreds of Chinese applications and the investment restrictions on Chinese companies in sensitive sectors, reflects a strategic decision to reduce India's technological dependence on China and to align India's digital infrastructure with the security standards of its democratic partners. The Commercial, Economic, and Industrial Communications Security (CEIS) framework — an emerging concept in India's national security policy that treats economic and industrial security concerns alongside traditional military security concerns — encompasses the protection of India's telecommunications infrastructure from Chinese vendor risk as a strategic national security objective, not merely a commercial risk management question.

India's participation in the "clean network" framework promoted by the United States — which seeks to build a global ecosystem of trusted telecommunications equipment and services from vendors that share democratic values and security standards — reflects this strategic alignment with Western security frameworks. The Quad's telecommunications working group — coordinating spectrum policy, supply chain security, and technology standards among India, the US, Australia, and Japan — provides a multilateral forum for India to harmonise its telecommunications security framework with that of its strategic partners. The practical implications for India's TTP and telecom security regulations include: alignment of India's trusted equipment standards with the common standards being developed by the Quad partners; mutual recognition of security evaluations conducted by partner countries' evaluation laboratories (reducing duplication of vendor evaluation effort); and coordinated diplomatic pressure on non-democratic countries to meet minimum security standards for their telecommunications exports.

B.4 Cybersecurity Insurance and Telecom

Cybersecurity insurance — financial insurance products covering the financial losses arising from cybersecurity incidents including data breaches, ransomware attacks, business interruption, regulatory fines, and liability claims from affected customers — is an emerging market that is particularly relevant for telecommunications operators given their exposure to both large-scale cyber attacks (as operators of critical digital infrastructure) and significant regulatory and legal liability (for failure to protect subscriber data in compliance with the DPDPA and the IT Act). The global cybersecurity insurance market has grown rapidly in recent years, driven by increasing awareness of cyber risk and by regulatory requirements (in some sectors and jurisdictions) for minimum cyber insurance coverage. India's cybersecurity insurance market is developing but remains less mature than in Western markets — premiums are lower, coverage terms are less standardised, and insurer capacity is smaller than in the US and European markets.

The relationship between cybersecurity insurance and regulatory compliance is complex and evolving. From the regulatory perspective, cyber insurance is a risk transfer mechanism that can complement (but not substitute for) technical security controls and regulatory compliance. An operator that relies on insurance to cover the financial consequences of cyber incidents without implementing adequate technical security measures is likely to find its insurance insufficient, since insurers are increasingly conditioning coverage on the implementation of specified security controls (such as multi-factor authentication, endpoint detection and response, regular patch management, and penetration testing). From the insurance perspective, the regulatory environment affects the scope of insurable losses: DPDPA financial penalties may or may not be

insurable (depending on whether Indian law permits insurance against regulatory penalties, and on the specific policy terms); liability claims from subscribers whose data is breached are generally insurable; business interruption losses from cyber attacks are generally insurable subject to policy terms.

B.5 The National Cyber Security Strategy and Telecom

India's National Cyber Security Strategy (NCSS) — updated most recently in 2020 and expected to be further updated in the context of the Telecommunications Act, 2023 and the DPDPA's enactment — provides the overarching policy framework within which all of India's sector-specific cybersecurity regulatory frameworks, including the telecommunications security framework, operate. The NCSS articulates India's cybersecurity objectives across five pillars: secure (making India's digital infrastructure and systems secure); strong (building India's cyber defence capabilities); steadfast (maintaining India's resolve to respond decisively to cyber attacks); sovereign (asserting India's digital sovereignty); and sensitive (protecting sensitive data and critical systems). The telecommunications sector is central to each of these pillars: as the medium over which all digital activity occurs, telecommunications infrastructure is both an instrument for achieving each pillar's objectives and a target for attacks that seek to undermine those objectives.

The telecommunications sector's specific contributions to NCSS implementation include: providing the network infrastructure over which government cybersecurity monitoring capabilities operate (including NCCC's internet traffic monitoring and CERT-In's incident coordination communications); enabling the secure communication capabilities of national security agencies and critical infrastructure operators through dedicated, secured network paths; supporting the Digital India initiative's cybersecurity components (including cybersecurity awareness programmes, digital literacy initiatives, and the development of domestic cybersecurity technology companies); and cooperating with India's international cyber diplomacy objectives (including India's participation in UNGGE and OEWG processes on cybersecurity norms, India's bilateral cyber dialogues with strategic partners, and India's leadership of developing-country perspectives in global cybersecurity governance debates). The Telecommunications Act, 2023's security framework is thus both a domestic regulatory instrument and a component of India's broader national and international cybersecurity strategy.

SUPPLEMENTARY NOTE C

Cybersecurity Law: Applied Practice

C.1 Handling Law Enforcement Data Requests

Telecommunications operators in India receive large volumes of data requests from law enforcement agencies — police, investigating agencies, courts, and national security authorities — seeking access to subscriber data including call records, location data, subscriber identity information, and internet connection records. Managing these requests effectively requires a systematic legal and operational framework that: ensures compliance with all lawful requests while rejecting requests that lack adequate legal authority; protects the privacy rights of subscribers against requests that exceed the bounds of applicable legal authority; documents all requests and responses for audit purposes; and maintains the confidentiality of disclosure obligations (since disclosure of the existence of an interception or monitoring order may itself be a criminal offence). The volume and variety of law enforcement data requests received by major operators — potentially thousands of requests per month across different categories and from multiple authorities — makes ad hoc management of requests unsustainable and creates significant compliance risk if individual requests are not properly categorised and processed.

The legal review process for law enforcement data requests must assess: whether the requesting authority has the legal power to demand the specific category of data requested (for example, whether a police request for real-time location tracking is based on an appropriate order under the applicable provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023, or whether a data preservation request from an investigative agency is based on a valid court order); whether the procedural requirements of the applicable statutory provision have been met (for example, whether an interception direction under Section 24 of the Telecommunications Act, 2023 has been signed by the appropriate authority and complies with the prescribed format); and whether the scope of the request is within the legal authority claimed (for example, whether a request for "all communications data" relating to a subscriber is within the scope of the cited legal authority or whether it exceeds it). Legal review by qualified in-house lawyers or external law firms with telecommunications regulatory expertise is essential for operators managing high volumes of law enforcement requests — the commercial and reputational consequences of disclosing subscriber data without adequate legal authority (or of failing to comply with a lawful request in time) are both significant.

The transparency reporting framework for law enforcement data requests — publishing aggregate data on the number and types of requests received, the legal authorities cited, the response rates, and the categories of data disclosed — is an emerging practice internationally that a small number of global technology companies (Google, Microsoft, Apple, Meta) have pioneered through voluntary transparency reports. In India, telecoms operators are generally not

required by law to publish transparency reports on law enforcement data requests, and doing so raises potential legal issues (since information about specific interception orders may be subject to statutory secrecy requirements). However, aggregate transparency reporting — publishing the total number of requests received and the percentage complied with, without identifying specific requests or the authorities that made them — would provide meaningful public accountability for the exercise of government surveillance powers without creating the specific legal risks associated with disclosure of individual order details. The development of a standardised transparency reporting framework for Indian telecom operators, developed in consultation with DoT, law enforcement agencies, and civil society, would be a significant step towards greater accountability for telecommunications surveillance.

C.2 Cybercrime Investigations: Telecom's Role

Telecommunications data is central to the investigation of virtually every category of cybercrime — from online fraud and phishing to ransomware attacks, CSAM (Child Sexual Abuse Material) distribution, and nation-state cyber espionage. The digital footprints left by cybercriminals on telecommunications networks — IP address logs, session data, subscriber identity information, and location data — enable investigators to identify, locate, and build cases against cybercrime perpetrators. Telecom operators' cooperation with cybercrime investigations is both a legal obligation (under the security conditions of their licences and the applicable provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023) and a public interest responsibility: effective cooperation with cybercrime investigations directly contributes to the protection of subscribers from the financial, reputational, and personal harm caused by cybercrime.

The practical challenges of cybercrime investigation cooperation for telecom operators involve: the technical capability to rapidly retrieve and produce the specific categories of data requested by investigators (not all operators maintain all categories of data in an easily retrievable format, particularly for older records); the legal authority analysis required for each investigative request (distinguishing between requests with adequate legal authority and those that are deficient); the secure transmission of sensitive law enforcement data to investigating agencies (ensuring that the data does not become accessible to unauthorised parties in the transmission process); the handling of requests from foreign law enforcement agencies (which may require mutual legal assistance procedures rather than direct operator cooperation); and the management of the conflict between data retention obligations (which require operators to retain data for law enforcement purposes) and DPDPA data minimisation obligations (which require operators to retain personal data only for as long as necessary for the specified purpose).

C.3 Security Architecture for 5G Core Networks

The 5G core network — the centralised control and data plane infrastructure that manages subscriber authentication, policy enforcement, session management, and interconnection with external networks — represents the most security-critical component of 5G telecommunications infrastructure. A compromise of the 5G core network could enable an attacker to: de-authenticate subscribers (denying service to all users on the network); intercept communications (routing subscribers' traffic through attacker-controlled infrastructure); track subscriber locations in real-time (accessing the core network's location management functions); and potentially disrupt the critical infrastructure services (emergency communications, financial transactions, industrial control) that depend on the 5G network. The security of the 5G core therefore requires the highest level of protection — in terms of physical security of the hosting facilities, logical security of the network functions, supply chain security of the equipment and software, and operational security of the management processes.

The 3GPP security specifications for 5G — particularly TS 33.501 (Security Architecture and Procedures for 5G System) — define the security architecture for 5G core networks, including requirements for authentication (using the 5G AKA and EAP-AKA' protocols), integrity protection (protecting control plane signalling from tampering), encryption (protecting user plane data from eavesdropping), and network exposure function (NEF) security (protecting the interfaces between the 5G core and external application servers). India's TTP framework evaluates 5G core network functions against these specifications, requiring vendors to demonstrate compliance with the 3GPP security requirements and to implement additional security features specified in the TTP guidelines. The deployment of 5G core networks in cloud environments — using virtualised or containerised network functions hosted on commercial cloud infrastructure — creates additional security considerations (cloud platform security, multi-tenancy isolation, secure orchestration) that the TTP framework must address as cloud-native 5G deployments become standard in India.

C.4 Threat Intelligence Sharing

Cyber threat intelligence sharing — the exchange of information about current and emerging cyber threats between operators, government agencies, and industry bodies — is a force multiplier for cybersecurity defence: information about an attack vector that one operator has observed and defended against can enable other operators to pre-emptively defend against the same attack before they are themselves targeted. The telecommunications sector's threat intelligence sharing arrangements in India are developing but not yet comprehensive. CERT-In operates as the primary hub for threat intelligence in India, collecting incident reports from all sectors (including telecoms) and disseminating sanitised threat intelligence advisories to the

broader community. The National Cyber Coordination Centre (NCCC) operates a real-time internet traffic monitoring capability that generates additional threat intelligence, though the classification level of much NCCC intelligence limits its sharability with commercial operators.

The legal framework for threat intelligence sharing among telecom operators — particularly the question of whether sharing information about a cyber attack (which may involve personal data about affected subscribers) constitutes a violation of the DPDPA's data protection requirements — requires careful analysis. Under the DPDPA, the sharing of personal data with another entity for the purpose of cybersecurity (preventing further attacks by informing other operators about the attack vector) may be justified as a "legitimate use" under Section 7(g) of the Act (which permits processing necessary for prevention of illegal activities or for cybersecurity purposes). However, the scope of this exemption — and whether it covers the sharing of subscriber-level data (such as IP addresses of attacker-controlled systems that were accessed by specific subscribers) with other operators for threat intelligence purposes — requires clarification through DPDPA implementing rules or Data Protection Board guidance. Operators should structure their threat intelligence sharing under formal information sharing agreements that specify the categories of data shared, the purpose limitations, the retention periods, and the security standards applicable to shared intelligence.

C.5 DPDPA Enforcement: Early Guidance

The Data Protection Board of India — established under Section 18 of the DPDPA, 2023 and expected to become operational following the notification of implementing rules — will be the primary enforcement authority for data protection obligations affecting the telecom sector. The Board's enforcement approach will significantly shape the practical compliance burden on telecom operators: a risk-based, proportionate enforcement approach (focusing enforcement resources on the most serious violations with the highest consumer harm) will be very different in its practical impact from a process-focused approach (citing operators for technical procedural non-compliance regardless of whether actual consumer harm resulted). The Board's enforcement precedents — particularly its early decisions on the standards required for valid DPDPA consent, the adequacy of technical security measures against data breach liability, and the process for assessing penalties — will set the practical compliance standards that telecom operators' compliance programmes must achieve.

TDSAT's appellate jurisdiction over Data Protection Board decisions affecting telecom operators — established by the DPDPA's provision for appeals to TDSAT — creates an important institutional link between telecom regulation and data protection enforcement. TDSAT's accumulated expertise in telecommunications technology and economics will

complement its developing expertise in data protection law, enabling it to adjudicate data protection appeals affecting the telecom sector with a more complete understanding of the technical and commercial context than a generalist appellate body would have. The development of a coherent body of TDSAT jurisprudence on DPDPA issues affecting the telecom sector — addressing the intersection of data protection obligations and telecom operational requirements — will be one of the most important contributions of the expanded TDSAT mandate to India's digital governance framework.

SUPPLEMENTARY NOTE D

National Security and Cybersecurity: Practice Notes

D.1 Trusted Telecom Portal: Compliance Procedures

The operational compliance requirements of the Trusted Telecom Portal framework are one of the most significant practical challenges facing Indian telecom operators and equipment vendors in the current regulatory environment. The TTP requires that network equipment deployed in Indian telecommunications networks be evaluated and approved by CERT-In accredited testing laboratories, with approved equipment listed on the TTP's approved equipment register. The compliance process involves: vendor submission of the equipment for evaluation (including hardware, firmware, and software components); evaluation laboratory assessment against the prescribed security criteria (covering physical security, logical security, supply chain security, and vulnerability management); CERT-In review and approval of the evaluation results; and listing on the TTP approved equipment register. The timeline for TTP approval — from vendor submission to final listing — has been a significant operational concern: in the early phases of TTP implementation, approval timelines of twelve to eighteen months created significant supply chain disruptions for operators planning network upgrades and 5G deployments. CERT-In and the accredited laboratories have been working to reduce approval timelines through process improvements and additional evaluation capacity, but the timeline challenge remains an operational constraint for the sector. Operators' legal and compliance teams must maintain detailed records of all deployed equipment's TTP approval status, track the status of pending approvals for equipment in the deployment pipeline, and assess the regulatory implications of deploying equipment before TTP approval in urgent circumstances (such as post-disaster network restoration).

The legal implications of deploying non-TTP-approved equipment — whether deliberately (where the operator decides to deploy without approval for operational reasons) or inadvertently

(where the operator was unaware that the specific equipment configuration required approval) — are significant under the Telecommunications Act, 2023's civil penalty framework. A licensed operator that deploys equipment that has not received TTP approval is potentially in breach of its licence conditions and subject to civil penalties of up to Rs. 5 crore per day for ongoing violations. The proportionality analysis for such penalties — assessing the severity of the security risk posed by the non-approved equipment, the duration of non-compliance, the operator's response to the violation (whether it promptly removed the equipment or sought retroactive approval), and whether the violation caused any actual harm — should inform the Adjudicating Officer's penalty calculation. The development of clear guidance on the TTP compliance obligation — specifically addressing the treatment of legacy equipment deployed before the TTP framework's establishment, the obligations for equipment that receives an updated firmware but was approved in an earlier configuration, and the procedure for equipment deployed in emergency situations — would reduce regulatory uncertainty and improve compliance planning for operators.

The TTP framework's interaction with international trade law — specifically the question of whether TTP's de facto exclusion of certain vendors (particularly Chinese vendors Huawei and ZTE) constitutes a discriminatory technical barrier to trade in violation of India's WTO commitments — has been a subject of academic and legal analysis but has not yet resulted in a formal WTO dispute. India's position — that TTP approval requirements are applied on the basis of security standards rather than national origin, and that any vendor meeting the standards is eligible for approval — is facially non-discriminatory. However, the practical reality that certain vendors have faced significant difficulties obtaining TTP approval (whether due to the complexity of their equipment architectures, the opacity of their supply chains, or political considerations affecting the evaluation process) while others have obtained approval relatively smoothly has led to arguments that TTP is not genuinely neutral. The development of transparent, published evaluation criteria, standardised evaluation procedures, and a clear appeals mechanism for disputed approval decisions would strengthen TTP's legal defensibility as a genuinely non-discriminatory security standard rather than a disguised technical barrier to trade.

D.2 Lawful Interception: Technical and Legal Dimensions

The lawful interception (LI) capability requirement — one of the most sensitive and legally complex of all telecommunications licence conditions — mandates that licensed operators install and maintain technical systems that enable government-authorised parties to intercept specified subscribers' communications in real-time, without the knowledge of the subscriber or the called party. The LI architecture prescribed by India's licence conditions — derived from the ETSI

standards for lawful interception and adapted for the specific requirements of Indian law enforcement agencies — involves: a LEA (Law Enforcement Agency) handover interface at which intercepted communications are delivered to authorised agencies; a mediation device that formats the intercepted data for delivery; and a secure management interface through which interception orders are activated and managed. The legal framework for LI activation — requiring a written order from a designated authority (the Secretary to the Government of India in the relevant ministry, for central agencies, or the Secretary-level officer of a state government for state agencies) before interception can be commenced — is prescribed by the Telephone Tapping Guidelines and will be carried forward in the rules under Section 24 of the Telecommunications Act, 2023.

The security of the LI system — ensuring that the capability to intercept communications is not accessible to unauthorised parties (including the operator's own employees, foreign intelligence services with access to the network, or malicious actors who compromise the operator's infrastructure) — is as important as the capability itself. A compromised LI system represents one of the most serious telecommunications security risks: an attacker who gains access to LI infrastructure can intercept any subscriber's communications that are nominally under government surveillance, potentially exposing sensitive law enforcement investigations or national security surveillance activities. The "Salt Typhoon" incidents in the United States — in which suspected Chinese state-sponsored hackers gained access to LI infrastructure at major US telecommunications operators in 2024 — illustrated the catastrophic security consequences of LI infrastructure compromise and have prompted global regulatory attention to the hardening of LI systems. India's LI security framework — administered through CERT-In and the security conditions of telecom licences — must incorporate the lessons from international LI security incidents, developing specific technical standards for LI system security that exceed the baseline ETSI requirements and reflect the heightened threat level faced by LI infrastructure.

D.3 The NCIIPC Framework for Telecom

The National Critical Information Infrastructure Protection Centre (NCIIPC) — India's designated national nodal agency for the protection of critical information infrastructure under Section 70A of the IT Act — has specific relevance for the telecommunications sector, which is designated as one of the thirteen critical sectors under NCIIPC's framework. NCIIPC's role in the telecommunications sector involves: designating specific telecommunications systems as "critical information infrastructure" (CII) subject to enhanced protection requirements; issuing sector-specific cybersecurity guidelines for telecom CII operators; coordinating with sector regulators (TRAI, DoT) on cybersecurity policy for the telecommunications sector; and providing

threat intelligence and incident response support to telecom CII operators. The designation of specific telecommunications systems as CII — as opposed to merely "important" telecommunications infrastructure — triggers enhanced security obligations including: mandatory security audits by CERT-In empanelled auditors; mandatory adoption of NCIIPC's sector-specific security guidelines; mandatory incident reporting to NCIIPC (in addition to CERT-In); and potentially additional access restrictions for foreign nationals involved in the management of designated CII.

The practical challenge of the NCIIPC framework for telecom operators is determining which specific systems within their networks qualify as CII and are therefore subject to the enhanced security obligations. NCIIPC's designation criteria — which focus on the criticality of the system (the consequences of its failure or compromise for national security, public safety, or economic security) and the sensitivity of the information it processes — are applied on a case-by-case basis, with operators required to self-assess their CII exposure and potentially self-designate systems for NCIIPC oversight. The self-assessment process — without clear, published criteria or a formal designation mechanism — creates compliance uncertainty: operators may over-designate (applying CII-level security to systems that do not require it, increasing costs) or under-designate (failing to apply CII-level security to systems that should have it, creating security risk and regulatory exposure). The development of clearer, sector-specific CII designation criteria for telecommunications — building on NCIIPC's general framework but providing telecom-specific guidance on which network elements typically qualify for CII designation — would improve the consistency and accuracy of the designation process.

D.4 Data Localisation and Telecom Networks

Data localisation requirements — regulatory requirements that specified categories of data generated or processed in India must be stored within India's territorial boundaries — have significant implications for the architecture and operational costs of telecommunications networks. Indian telecom operators' compliance with data localisation requirements involves two primary categories: the localisation of subscriber data (personal data about Indian subscribers, governed by the DPDPA's data transfer provisions and the telecom licence conditions on data retention); and the localisation of specified critical data (including traffic metadata and law enforcement-related data governed by CERT-In directions and telecom security conditions). The technical implications of data localisation for telecom operators include: the deployment or use of India-based data centres for subscriber data processing; the modification of CDN (Content Delivery Network) architectures to keep specified data within Indian borders; and the development of India-specific versions of global network management and analytics platforms

that process subscriber data.

The DPDPA's approach to cross-border data transfers — prohibiting the transfer of personal data to countries or territories to which the government has not granted approval — creates specific compliance obligations for telecom operators that use global network management platforms, cloud-based operational support systems, or international subscriber data sharing arrangements (such as international roaming data exchange). The government's list of approved countries for personal data transfer — to be published by the Data Protection Board — will determine whether the network management systems and subscriber data platforms used by multinational operators can continue to process Indian subscriber data from their global operations centres, or whether Indian-specific data isolation will be required. The commercial and operational implications of data localisation for telecom operators with global operations — including the cost of establishing India-specific data processing environments and the complexity of maintaining geographically isolated data processing while operating a globally integrated network — are significant compliance planning considerations that legal and technical teams must address together.

D.5 Personal Data Processing in Network Operations

Telecommunications network operations inherently involve the processing of vast quantities of personal data as a technical necessity — call records (which reveal who called whom, when, and for how long), location data (derived from the cell towers to which a subscriber's device is connected), internet connection logs (which reveal which websites or internet services a subscriber accesses), and traffic metadata (patterns of communication that, in aggregate, can reveal sensitive personal information) are all generated automatically as by-products of the network operations that deliver telecommunications services. Under the DPDPA, 2023, this network-generated personal data must be processed in compliance with the Act's requirements — including the requirement for a lawful basis for processing, data minimisation (collecting only what is necessary), purpose limitation (using data only for the purposes for which it was collected), and data security (implementing appropriate technical and organisational measures to protect personal data against unauthorised access). The challenge for telecom operators is that network operations data serves multiple purposes — some clearly "necessary for the provision of services" (the primary lawful basis for most network data processing) and others that are less clearly within the necessity standard (such as the use of subscriber data for targeted advertising, network capacity planning, or the development of new service offerings).

The concept of "communication metadata" — data about communications (who communicated with whom, when, how long, from where) rather than the content of

communications — has been identified by courts in multiple jurisdictions (including the European Court of Justice and the US Supreme Court) as particularly sensitive, warranting stronger privacy protection than ordinary non-communication data. India's constitutional framework, following the Puttaswamy judgment's recognition of informational privacy as a component of the fundamental right to privacy, similarly treats communication metadata as sensitive personal information that requires special protection. The implication for telecom operators is that the routine processing of communication metadata for network operations purposes — which is technically necessary and clearly lawful — must be clearly distinguished from the use of that metadata for commercial purposes (advertising, credit scoring, market analysis) that goes beyond the network operations necessity. The development of clear internal data governance policies that define the permitted uses of communication metadata, the retention periods applicable to different categories of metadata, and the access controls preventing unauthorised use — and the robust technical implementation of those policies — is an essential element of DPDPA compliance for telecom operators.

SUPPLEMENTARY NOTE E

Cybersecurity Law: Forward-Looking Analysis

E.1 AI-Driven Cybersecurity: Legal Accountability

The deployment of artificial intelligence for telecommunications cybersecurity — through AI-driven threat detection, automated incident response, AI-based vulnerability assessment, and intelligent security monitoring — raises novel legal accountability questions about who is responsible when AI-driven security decisions cause harm or fail to prevent attacks. In traditional security frameworks, the accountability for security decisions is clear: human security analysts decide whether to block suspicious traffic, isolate compromised systems, or initiate incident response procedures, and those analysts (and their employers) bear responsibility for the consequences of their decisions. When AI systems make these decisions autonomously — blocking legitimate traffic that matches attack signatures, or failing to detect novel attack patterns that do not match training data — the accountability chain is disrupted. The operator that deployed the AI system is accountable for the decision to deploy and for ensuring that the system meets applicable standards; the AI system developer is accountable for the performance of the system against its specifications; and the regulatory authority is responsible for ensuring that the standards against which AI security systems are assessed are adequate. The allocation of liability among these parties — when an AI security system error causes harm (either by failing

to prevent an attack or by erroneously blocking legitimate traffic) — requires both clear contractual allocation in the operator-vendor relationship and clear regulatory standards against which AI system performance can be assessed.

The CERT-In incident reporting framework for AI-related cybersecurity incidents — specifically the obligation to report incidents attributable to AI system failures, as distinct from incidents attributable to external attackers exploiting human or software vulnerabilities — is an underdeveloped area of the regulatory framework. The current CERT-In reporting categories were designed for human-or-human-assisted attacks and software vulnerabilities; they do not specifically address AI system malfunctions or AI adversarial attacks (attacks specifically designed to deceive AI security systems). The development of AI-specific incident reporting categories — covering AI system failures, adversarial attacks on AI security systems, and unintended AI security system behaviours — would improve the quality of the incident data available to CERT-In and enable better monitoring of AI-related security risks in the telecommunications sector. This data, in turn, would inform the development of AI-specific security standards and audit requirements that CERT-In and DoT can prescribe for telecom operators' AI security deployments.

The security implications of large language models (LLMs) and generative AI in the telecommunications context are an emerging area of cybersecurity concern that India's regulatory framework must begin to address. LLMs can be used by attackers for: highly convincing social engineering attacks (using AI-generated voice or text to impersonate legitimate callers or messages); automated vulnerability discovery (using AI to analyse publicly available information about network configurations to identify potential attack vectors); and large-scale phishing and fraud operations (using AI to generate personalised fraudulent communications at scale). Telecom operators are both potential victims of LLM-based attacks (as targets of social engineering and infrastructure compromise) and potential enablers (as the networks over which LLM-generated fraud communications are transmitted). The development of specific countermeasures — AI-based detection of AI-generated fraud communications, authentication mechanisms that can detect AI-impersonated voices or messages, and cooperation between operators and LLM developers for fraud prevention — requires regulatory coordination between CERT-In, DoT, MeitY, and the operators.

E.2 The Quantum Threat to Telecommunications Security

The quantum computing threat to telecommunications security — the risk that sufficiently powerful quantum computers will break the public-key cryptographic systems that currently protect telecommunications from eavesdropping, authentication attacks, and man-in-the-middle

attacks — is not an immediate threat but is a medium-term risk that telecommunications security frameworks must address proactively. The timeline for quantum computers capable of breaking RSA-2048 (one of the most widely used public-key cryptography standards) is uncertain but is widely estimated by experts at 10-25 years under current technology trajectories. This timeline means that the "harvest now, decrypt later" threat — collecting encrypted telecommunications traffic today and decrypting it when quantum computing capability becomes available — is already relevant for long-lived sensitive data. Communications between senior government officials, classified research data, long-term financial transactions, and other information whose sensitivity will persist for decades may already be at risk from adversaries with the capability and intent to harvest current telecommunications traffic for future decryption. India's telecommunications security framework must therefore address the quantum threat now, even though the threat is not yet immediate, by planning the cryptographic migration needed to protect long-lived sensitive telecommunications against future quantum attacks.

The regulatory implications of post-quantum cryptography (PQC) migration for Indian telecommunications operators are significant. The transition from current public-key cryptography (RSA, ECDH, ECDSA) to NIST-standardised PQC algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON) requires: updating the cryptographic implementations in all network equipment (base stations, core network functions, network management systems) to support PQC algorithms; updating the subscriber authentication framework (5G AKA protocol and its successors) to incorporate PQC-resistant authentication; updating the secure management channels through which network operators remotely manage and update network equipment; and updating the end-to-end encryption implementations of OTT communication services to use PQC algorithms. This is a massive undertaking that will require coordination between equipment vendors (who must update their products to support PQC), operators (who must deploy updated equipment and configure their networks for PQC), and regulatory authorities (who must prescribe PQC standards and timelines). The development of a national PQC migration roadmap for the telecommunications sector — led by C-DoT, CERT-In, and TEC in consultation with operators and vendors — is an urgent regulatory priority.

E.3 The Security Governance Framework: Institutional Analysis

India's telecommunications cybersecurity governance framework involves multiple institutional actors with distinct but overlapping mandates: DoT (responsible for security conditions in telecom licences and the TTP framework); CERT-In (responsible for cybersecurity incident response, security standards, and accreditation of testing laboratories); NCIIPC (responsible for critical information infrastructure protection including designated telecom CII);

NTRO (the National Technical Research Organisation, responsible for technical intelligence and cyber capability); the National Cyber Security Coordinator (NCSC), in the Prime Minister's Office (responsible for coordinating national cybersecurity policy); and now the Data Protection Board (responsible for enforcing the DPDPA's data security requirements). This institutional plurality creates both a diversity of perspectives and a risk of coordination failure: when a major telecommunications cybersecurity incident occurs, the response involves multiple institutions that may have different assessments of the incident's significance, different communication protocols, and different operational responses. The development of a National Telecommunications Cybersecurity Incident Management Framework — specifying the roles, responsibilities, and coordination protocols for all relevant institutions in responding to major telecom cybersecurity incidents — is a governance priority that would improve India's collective response capability.

The coordination between India's telecommunications cybersecurity governance and international cybersecurity bodies — particularly FIRST (Forum of Incident Response and Security Teams), the ITU's cybersecurity programme, the Budapest Convention on Cybercrime (which India has not signed), and bilateral cyber cooperation arrangements with strategic partners — is an important dimension of India's cybersecurity governance that has implications for the telecommunications sector. CERT-In's membership in FIRST enables information sharing about global cyber threats with peer CERTs around the world, providing access to threat intelligence that India cannot generate domestically. The absence of India's signature on the Budapest Convention — the primary international treaty framework for cybercrime investigation and cross-border cooperation — limits India's formal access to the mutual assistance mechanisms that the Convention provides, though India has bilateral cybercrime cooperation arrangements with many countries. The development of India's international cybersecurity engagement — through active participation in international cybersecurity fora, expansion of bilateral cybersecurity cooperation arrangements, and eventual accession to relevant international instruments — would strengthen India's access to international threat intelligence and improve the effectiveness of cross-border cybercrime investigations involving Indian telecommunications infrastructure.

The regulatory framework for cybersecurity insurance in the telecommunications sector — specifically, the question of whether telecom operators should be required to maintain minimum levels of cybersecurity insurance as a condition of their authorisations — is an emerging regulatory policy question. Cybersecurity insurance requirements, where they exist in other sectors (such as for critical infrastructure operators in some European countries), serve two

functions: ensuring that operators have the financial resources to manage the consequences of cybersecurity incidents (compensating affected subscribers, funding remediation, and paying regulatory fines); and creating a market-based incentive for cybersecurity investment (since insurers condition premiums on operators' cybersecurity practices, creating a commercial incentive for operators to invest in security beyond the minimum regulatory requirements). The development of a regulatory framework for cybersecurity insurance in Indian telecommunications — in consultation with IRDAI (the insurance regulator), DoT, and CERT-In — would complement the security conditions framework and create an additional market-based incentive for cybersecurity investment.

SUPPLEMENTARY NOTE F

Security Framework: Implementation Topics

F.1 Security Audits for Telecom Networks

Security audits for telecommunications networks — systematic assessments of the security posture of a network operator's systems, processes, and people — are both a regulatory requirement (under CERT-In's empanelled auditor framework and the telecom licence security conditions) and an essential internal management tool for identifying and addressing security vulnerabilities before they are exploited by attackers. CERT-In's framework for telecommunications network security audits prescribes: the scope of the audit (which network systems must be covered, including core network functions, access network equipment, management systems, and physical security); the methodology (combining automated vulnerability scanning, manual penetration testing, security configuration review, and process assessment); the qualifications of the auditors (who must be CERT-In empanelled organisations with demonstrated telecommunications security expertise); and the reporting requirements (the format and content of the audit report, and the timeline for submitting it to CERT-In). The audit cycle — typically annual, with interim vulnerability assessments between annual audits — provides a structured framework for regular security review that supplements the operator's ongoing security monitoring activities.

The legal status of telecommunications security audit reports — specifically whether they are protected from disclosure under privilege or exemption provisions, or whether they are available to regulatory authorities, litigation parties, or the public — is an important consideration for operators that commission security audits. An audit report that identifies significant security vulnerabilities may be commercially sensitive (competitors could exploit the vulnerabilities if the

report were disclosed), legally sensitive (the report could be used as evidence in regulatory enforcement or negligence litigation against the operator), and nationally sensitive (detailed vulnerability information could be exploited by hostile state actors). The legal framework for protecting security audit reports — through contractual confidentiality provisions with the auditor, potential attorney-client privilege (where the audit is commissioned through the operator's legal department), and regulatory confidentiality protections — must be carefully constructed to ensure that the operator can commission frank security assessments without creating disproportionate legal and commercial risk. At the same time, the regulatory requirement for security audit reports to be submitted to CERT-In means that the regulator will have access to this sensitive information, creating an obligation on CERT-In to manage the information responsibly and to maintain appropriate confidentiality protections.

The integration of security audit findings into operators' corporate governance framework — specifically the reporting of significant security audit findings to the operator's Board of Directors and Audit Committee — is an important governance dimension of cybersecurity risk management in the telecommunications sector. Significant security vulnerabilities identified in security audits — particularly those that could affect the integrity of subscriber data, the availability of critical telecommunications services, or the security of national security-related communications — are material risks that must be reported to the Board under the Companies Act, 2013's disclosure obligations (which require the Board to assess and manage significant risks to the business). The development of clear internal procedures for escalating significant security audit findings to senior management and the Board, and for tracking the remediation of identified vulnerabilities, is an important component of mature cybersecurity governance for telecommunications operators. CERT-In's expectation that significant vulnerabilities identified in security audits will be remediated within specified timelines — and that CERT-In will be notified of remediation progress — creates a regulatory accountability link between the security audit cycle and the operator's internal remediation programme.

F.2 Social Engineering and Telecom Fraud

Social engineering attacks — attacks that exploit human psychology rather than technical vulnerabilities to gain unauthorised access to systems, data, or money — are among the most prevalent and damaging forms of cybercrime in the telecommunications sector. The SIM swap fraud — in which an attacker impersonates a subscriber and convinces the operator's customer care team to transfer the subscriber's mobile number to a new SIM card under the attacker's control — is perhaps the most financially damaging telecommunications-specific social engineering attack. Once the attacker controls the subscriber's mobile number, they can use it to

intercept SMS-based one-time passwords (OTPs), enabling account takeover of the subscriber's banking, financial, and other accounts that use the mobile number for authentication. The financial losses from SIM swap fraud in India — while not publicly reported with the comprehensive statistics available in some other jurisdictions — are estimated to be substantial, affecting thousands of subscribers annually with individual losses ranging from thousands to lakhs of rupees.

The regulatory framework for preventing SIM swap fraud in India involves operator obligations under the Telecom Commercial Communications Customer Preference Regulations (DND framework) and the broader telecom security conditions, as well as RBI requirements for financial institutions that rely on SMS OTPs for authentication. Operators' procedures for processing number porting requests and SIM replacement requests — which are the primary attack vectors for SIM swap fraud — must balance the legitimate needs of genuine subscribers (who may lose their phones, damage their SIMs, or change their service providers) against the fraudulent use of these procedures by attackers. TRAI's recommendations on SIM swap fraud prevention — developed in consultation with operators, financial regulators, and law enforcement agencies — address several key prevention measures: cooling-off periods after number porting (during which OTPs for banking transactions are not sent to newly ported numbers); enhanced verification requirements for SIM replacement requests (requiring biometric verification or multiple security factor confirmation before issuing a replacement SIM); and real-time fraud alerts (notifying subscribers immediately when a SIM swap is processed for their number, enabling rapid detection of fraudulent swaps).

F.3 Cybercrime Jurisdiction and Cross-Border Issues

India's jurisdiction over cybercrime — including cybercrimes committed against Indian telecommunications infrastructure, against Indian operators' subscribers, or through Indian telecommunications networks — is primarily established through the territorial and effects-based principles of the Bharatiya Nyaya Sanhita, 2023 (the replacement for the Indian Penal Code) and the Information Technology Act, 2000. The territorial principle — that India has jurisdiction over crimes committed on Indian territory, including crimes committed through telecommunications networks that are physically located in India — provides the primary basis for Indian jurisdiction over most telecommunications-related cybercrime. The effects-based principle — that India has jurisdiction over crimes committed abroad that have effects in India, including crimes that target Indian systems or subscribers from outside India — extends India's jurisdiction to cross-border cybercrimes that affect India even when the perpetrators are located abroad. The practical challenge of exercising jurisdiction over cross-border cybercrimes — obtaining evidence from

foreign jurisdictions, identifying perpetrators who operate through anonymising technologies, and coordinating with foreign law enforcement agencies for arrests and extraditions — is one of the most significant operational challenges for India's cybercrime law enforcement.

The mutual legal assistance treaty (MLAT) framework for obtaining cybercrime evidence from foreign jurisdictions — through formal requests made under applicable bilateral or multilateral treaty arrangements — is a critical but often slow mechanism for cross-border cybercrime investigation. India has MLATs with several major countries (including the United States, the United Kingdom, and many others) that provide a formal legal basis for the exchange of evidence and information for criminal investigations. The MLAT process typically involves: a request from the Indian requesting authority (typically the Ministry of Home Affairs or state police with appropriate approval); transmission through diplomatic channels; review by the requested foreign authority for compliance with its domestic legal requirements; and provision of the requested evidence (or explanation of why it cannot be provided). The timeline for MLAT requests — which can range from several months to several years — is too slow for many cybercrime investigations, where digital evidence may be deleted or systems may be reconfigured before the MLAT process is completed. The development of expedited evidence preservation procedures — under which India can request the emergency preservation of digital evidence pending a formal MLAT request — would improve the timeliness of cross-border cybercrime evidence collection.

The legal framework for cooperation between Indian telecommunications operators and foreign law enforcement in cross-border cybercrime investigations — specifically the conditions under which Indian operators can provide subscriber data and network records to foreign law enforcement agencies — is an area of significant legal complexity. Operators are generally prohibited from disclosing subscriber data to non-Indian authorities without following the required legal process, which typically involves a request through the MLAT framework or a court order in India. However, emergency circumstances (such as an imminent threat to life or critical infrastructure) may justify more expedited data sharing arrangements, and several major platforms (including US-based social media and technology companies) have established procedures for handling emergency disclosure requests that balance speed and due process. The development of an Indian framework for emergency cross-border data sharing in telecommunications — specifying the conditions that must be met for emergency disclosure, the authorities authorised to make such requests, and the documentation required — would provide clearer legal guidance for operators and improve India's ability to cooperate with international partners in time-sensitive cybercrime investigations.

F.4 Personal Data in Network Performance Analytics

Telecommunications operators' use of network performance analytics — the analysis of traffic data, network performance measurements, and subscriber usage patterns to optimise network capacity, diagnose performance issues, and plan future infrastructure investments — inevitably involves the processing of data that may be personal in character. Network performance analytics relies on data sources including: individual subscriber traffic records (aggregated to assess demand patterns and identify traffic congestion points); call detail records (analysed to identify coverage gaps and quality issues); location data derived from cell tower connections (used to understand subscriber mobility patterns and to identify areas with high demand); and device data (analysing the types of devices connected to the network and their performance characteristics). Some of this data — particularly individual subscriber traffic records and location data — is personal data under the DPDPA's broad definition (which covers any data by which an individual can be identified directly or indirectly).

The lawful basis for network performance analytics under the DPDPA requires careful analysis. The primary basis available to operators for this type of data processing is "legitimate use" under Section 7 of the Act — specifically, that the processing is necessary for the operators' legitimate interest in optimising their networks, or that it is necessary for compliance with their licence conditions (which require them to maintain specific quality of service standards). The necessary criterion is significant: network performance analytics that processes subscriber-level data is "necessary" for the legitimate purpose only if the same analytical objectives cannot be achieved through anonymised or aggregated data. Where anonymisation is technically feasible — converting individual subscriber data into aggregate statistics before analysis — the use of personally identifiable data would exceed what is necessary under the necessity criterion. The principle of "privacy-by-design" — building data minimisation and privacy protection into the design of data processing systems rather than applying them as an afterthought — requires operators to design their network performance analytics platforms to use the minimum level of personally identifiable data necessary to achieve the analytics objectives. The development of technical standards for privacy-preserving network analytics — such as differential privacy techniques that add mathematical noise to aggregate statistics to prevent individual identification — is an area where regulatory guidance from CERT-In and the Data Protection Board would be valuable.

SUPPLEMENTARY NOTE G

Security Regulation: Final Topics

G.1 Cyber Insurance for Critical Infrastructure

Telecommunications operators classified as critical information infrastructure (CII) under the NCIIPC framework face elevated cybersecurity risk exposure that creates a specific case for cyber insurance coverage beyond the general corporate liability insurance that operators typically maintain. CII operators are primary targets for sophisticated cyber attacks — including nation-state attacks, ransomware campaigns targeting high-value critical infrastructure, and advanced persistent threats (APTs) designed to establish long-term covert access to sensitive network systems. The financial consequences of a successful cyberattack on a major telecommunications CII operator could include: direct remediation costs (forensic investigation, incident response, system restoration, and customer notification); regulatory fines under the DPDPA and the IT Act for data breaches; liability claims from subscribers, enterprise customers, and interconnected operators whose services are disrupted by the attack; business interruption losses from network downtime during the attack and recovery period; and reputational damage that results in subscriber churn and reduced future revenues. The aggregate financial exposure from these combined loss categories could be substantial — potentially running to thousands of crores in a major incident — and would exceed the coverage available under most standard corporate liability policies.

The development of tailored cyber insurance products for Indian telecommunications CII operators — covering the specific loss categories and risk exposures of the sector — requires collaboration between the telecom industry (which understands its specific risk profile), the insurance industry (which must design and price appropriate coverage), IRDAI (which regulates the insurance products), and CERT-In (which can provide threat intelligence and risk assessment data to support insurance product development). The key cyber insurance coverage components for a telecommunications CII operator should include: first-party coverage (covering the operator's own costs of responding to a cybersecurity incident, including forensic investigation, system restoration, business interruption, and crisis communications); third-party liability coverage (covering claims from subscribers, enterprise customers, and other parties harmed by the operator's cyber incident); regulatory defence and penalties coverage (covering the legal costs of responding to regulatory investigations and a portion of any regulatory fines, to the extent insurable under Indian law); and media liability coverage (covering claims arising from the inadvertent disclosure of subscriber data through a cyber breach). The development of industry-standard exclusions — defining the categories of cyber loss that are not insurable (such as losses resulting from deliberate fraud or wilful neglect of basic security requirements) — is equally important for creating a sustainable cyber insurance market for the sector.

The moral hazard implications of cyber insurance — the risk that insurance coverage reduces operators' incentives to invest in cybersecurity, since some of the financial consequences of a successful attack are transferred to the insurer — must be managed through the design of cyber insurance products and the broader cybersecurity regulatory framework. Insurance products that require policyholders to meet minimum security standards as a condition of coverage (similar to the safety standards required for property insurance) create a positive incentive for security investment rather than a disincentive. The development of a minimum cybersecurity standard for telecommunications CII operators — potentially aligned with the NIST Cybersecurity Framework or the ISO 27001 standard for information security management — that would be required for cyber insurance coverage would create a market-based incentive for security improvement that complements the regulatory requirements. CERT-In's involvement in defining these minimum standards — drawing on its threat intelligence and incident response experience — would ensure that the standards reflect the actual threat landscape faced by Indian telecommunications operators rather than generic international frameworks that may not capture India-specific threats.

G.2 Data Breach Notification: Compliance Practice

Telecommunications operators' data breach notification obligations — the requirements to notify CERT-In, the Data Protection Board (once operational), and affected subscribers when a personal data breach occurs — are among the most operationally demanding compliance requirements of the DPDPA and the IT Act framework. The CERT-In notification requirement — currently the most immediate obligation, with a 6-hour notification window for specified categories of incident — requires operators to maintain robust breach detection capabilities (so that breaches are identified promptly), clear internal escalation procedures (so that the breach is reported to the appropriate authority quickly), and pre-drafted notification templates (so that the required notification information can be assembled and submitted within the tight timeframe). The legal analysis of breach notification obligations involves several threshold questions: does the incident constitute a "data breach" as defined in the applicable regulation? Does the breach involve "personal data" as defined in the DPDPA? Is the breach of a severity and nature that triggers the specific notification obligation? These questions must be analysed quickly, in the immediate aftermath of a breach when operational response to limit the damage is also ongoing, requiring clear internal legal guidance and pre-established decision trees for breach notification assessment.

The content requirements for data breach notifications — specifying what information must be included in the notification to each required recipient — differ between the CERT-In

notification (which requires technical details about the incident, the affected systems, and the impact) and the Data Protection Board notification (which will likely require information about the categories and volume of personal data affected, the likely consequences for data subjects, and the remediation measures taken). Operators must develop separate notification templates and processes for each notification recipient, ensuring that the technical and regulatory teams coordinate effectively to assemble the required information within the prescribed timelines. The notification to affected subscribers — informing them that their personal data has been breached and providing guidance on protective measures they should take — creates specific consumer protection and reputational management challenges: the notification must be clear, actionable, and honest about the nature and extent of the breach without creating unnecessary alarm, and must be delivered through channels (SMS, email, app notification) that reach the affected subscribers reliably and quickly.

The post-breach regulatory engagement — the interaction with CERT-In and (once operational) the Data Protection Board in the weeks and months following a significant breach, including supplementary notifications, regulatory interviews, document production, and compliance with remediation directions — requires dedicated regulatory response teams with clear responsibilities and protocols. CERT-In's post-breach follow-up typically includes: requests for additional technical information about the incident; assessment of the operator's breach response and remediation activities; and directions to implement specific security improvements to prevent recurrence. The operator's engagement with CERT-In in this follow-up process — while potentially exposing the operator to regulatory scrutiny of its pre-breach security practices — is also an opportunity to demonstrate proactive remediation and to seek regulatory guidance on best practices for preventing similar incidents. The development of a collaborative regulatory engagement model — in which CERT-In works with operators to understand breaches and improve security, rather than treating all breaches as enforcement matters — would improve both the quality of the regulatory response and the broader security posture of the sector.

G.3 Insider Threat Management in Telecom Networks

The insider threat — the risk of harm to telecommunications infrastructure, subscriber data, or national security caused by malicious or negligent actions of employees, contractors, or other trusted individuals with legitimate access to sensitive systems — is one of the most difficult cybersecurity risks to manage and one of the most serious threats to the security of telecommunications networks. Insiders have a fundamental advantage over external attackers: they have legitimate access to systems, understand the network architecture, and can operate within normal operational patterns that automated security monitoring may not flag as

suspicious. Telecommunications networks are particularly vulnerable to insider threats because of: the large number of people with privileged access to network management systems; the distributed nature of network operations (with field technicians having physical access to infrastructure across large geographic areas); the presence of contractors and vendor support staff who have access to sensitive systems but are not subject to the same vetting and monitoring as direct employees; and the sensitivity of the subscriber data (call records, location data, and content of communications) accessible through network management systems.

The regulatory framework for insider threat management in Indian telecommunications — as prescribed in the security conditions of the Unified Licence and evolving under the Telecommunications Act, 2023's security rules — includes requirements for: background verification of employees with access to sensitive systems (including criminal record checks and security clearances for staff with access to lawful interception and national security-related systems); access control (role-based access controls that limit each individual's access to only the systems required for their specific job functions); audit logging (maintaining comprehensive audit trails of privileged access to sensitive systems, enabling retrospective investigation of suspicious activity); and separation of duties (ensuring that no single individual can make significant changes to security-sensitive configurations without a second person's authorisation). These technical and procedural controls are supplemented by behavioural monitoring (using user and entity behaviour analytics to identify anomalous access patterns that may indicate insider threat activity) and by culture and training programmes that build security awareness and create an environment where employees report suspicious behaviour.

G.4 Regulatory Framework for Encrypted Communications

The regulatory framework for encrypted communications — the balance between protecting users' right to private communication (through strong encryption) and enabling government-authorised access to communications for law enforcement and national security purposes (through lawful interception) — is one of the most contested policy and legal questions in the telecommunications and digital governance domain globally, and India's framework for managing this tension is still evolving. Strong encryption — the default use of end-to-end encryption (E2EE) for messaging applications and voice over IP communications — provides essential privacy protection for hundreds of millions of Indian users and enables the secure use of digital services (banking, healthcare, government services) that depend on secure communications. Lawful interception — the authorised monitoring of specific suspects' communications for criminal investigation or national security purposes — is an essential law enforcement tool that has been used to prevent terrorist attacks, solve serious crimes, and

protect national security.

The tension between strong encryption and lawful interception has been addressed in different ways by different regulatory frameworks globally. Some countries have mandated "backdoors" or "exceptional access" mechanisms — technical features built into encryption systems that enable law enforcement to decrypt communications with appropriate authorisation. The cryptographic and security communities have broadly rejected this approach, arguing that any backdoor weakens encryption for all users (not just those targeted by law enforcement) and creates vulnerabilities that can be exploited by malicious actors as well as authorised law enforcement. Other countries have adopted a more nuanced approach: accepting the use of strong encryption for consumer communications while requiring that encrypted communications services maintain the capability to comply with lawful interception orders through means that do not require breaking the encryption itself (such as through client-side scanning of plaintext before encryption, or through retention of encryption keys under escrow arrangements that can be accessed with appropriate legal authority). India's current framework — which requires licensed telecommunications operators to provide lawful interception capability — was designed for circuit-switched and traditional packet-switched networks where operators have access to the content of communications. The extension of LI obligations to OTT communication services using E2EE requires either a modification of the technical LI framework (to address the E2EE architecture) or a policy decision on the extent to which E2EE is permissible for OTT services subject to Indian regulation.

G.5 Security Certification: International Mutual Recognition

The mutual recognition of telecommunications security certifications — arrangements between countries to accept each other's security evaluations of network equipment without requiring duplicate testing — is an important efficiency mechanism for the global telecommunications supply chain and a potential accelerant for India's TTP framework. Currently, a telecommunications equipment vendor seeking to sell in multiple markets must typically undergo separate security evaluations in each country or jurisdiction (since national security evaluation frameworks, while often based on the same international standards such as Common Criteria, are administered independently and may have different implementation requirements). Mutual recognition arrangements — under which each participating country accepts the results of another participating country's evaluation without requiring re-evaluation — reduce this duplication, lowering the cost and time required for market entry for compliant vendors.

India's TTP framework has been developed primarily as a national security measure, and the initial focus has been on establishing robust domestic evaluation capability rather than on international integration. However, as the TTP framework matures and as India seeks to attract compliant, non-adversary vendors to serve India's 5G market, the development of mutual recognition arrangements with strategic partner countries — potentially including the US, UK, EU, Australia, Japan, and South Korea, all of which have developed their own network equipment security frameworks (NESAS, GSMA's security accreditation, FCC's Covered List, and others) — would reduce compliance costs for trusted vendors and improve the speed with which approved equipment can be deployed in India's networks. The development of mutual recognition arrangements requires both technical alignment (harmonising evaluation methodologies and security standards between the participating frameworks) and political agreement (confirming that the participating countries have sufficient confidence in each other's evaluation processes). India's diplomatic engagement on 5G security — through the Quad's telecommunications working group and bilateral security cooperation arrangements — provides a pathway for developing the political agreements that underpin mutual recognition.

SUPPLEMENTARY NOTE H

Cybersecurity Regulation: Final Perspectives

H.1 The Critical Infrastructure Resilience Framework

India's critical infrastructure resilience framework — the regulatory and institutional architecture for ensuring that critical telecommunications infrastructure can withstand and rapidly recover from major disruptions, whether caused by cyber attacks, natural disasters, or deliberate physical attacks — is a multi-dimensional challenge that involves DoT, NCIIPC, CERT-In, state disaster management authorities, and the operators themselves. The resilience framework encompasses several distinct dimensions: physical resilience (ensuring that telecommunications infrastructure can withstand the physical threats most relevant to India's diverse geography, including cyclones, floods, earthquakes, and extreme heat); cyber resilience (ensuring that telecommunications systems can withstand cyber attacks and rapidly restore service after a successful attack); operational resilience (ensuring that network operations can continue under disrupted conditions, including with reduced staff, impaired management systems, or partial infrastructure failure); and supply chain resilience (ensuring that operators can obtain replacement components and equipment in a timely manner following major infrastructure damage, without dependence on single suppliers or supply routes).

The measurement and assessment of telecommunications critical infrastructure resilience — determining whether specific operators and specific network elements meet the resilience standards prescribed by the regulatory framework — requires a combination of design review (assessing whether the network architecture has sufficient redundancy, diversity, and recovery capability), testing (including regular emergency response exercises and recovery drills), and monitoring (continuously tracking the status of resilience-relevant systems including backup power, redundant transmission routes, and security monitoring capabilities). The Telecommunications Act, 2023's critical infrastructure protection framework provides the regulatory basis for requiring operators to conduct and report on resilience assessments, but the specific standards and assessment methodologies must be developed through implementing rules. The development of a telecommunications resilience assessment framework — specifying the key resilience indicators, the assessment methodology, the frequency of assessments, and the reporting requirements — is an important regulatory priority that DoT should develop in consultation with NCIIPC, CERT-In, and industry.

The cross-sector resilience dependencies of telecommunications infrastructure — the fact that telecommunications networks depend on electrical power (from the power grid), physical security (from law enforcement and emergency services), and financial system access (for commercial operations), while other critical sectors (banking, healthcare, transport) depend on telecommunications — create complex interdependencies that require multi-sector resilience planning. A major telecommunications outage does not only affect telecommunications subscribers: it disrupts the digital payment infrastructure (UPI, card payments), the emergency communications capability of hospitals and emergency services, the logistics coordination of supply chains, and the remote working capability of millions of office workers. Conversely, a major electrical grid failure disables telecommunications infrastructure (which depends on grid power with only limited battery backup). India's Critical Infrastructure Protection framework must address these interdependencies through: joint resilience planning between critical sector operators; information sharing arrangements that enable operators in one sector to anticipate and prepare for disruptions caused by failures in interdependent sectors; and coordinated emergency response plans that account for cascading failures across dependent critical sectors.

H.2 Cybersecurity Governance: Board-Level Responsibility

The corporate governance framework for cybersecurity in India's telecommunications sector — specifically the obligations of boards of directors and senior management for ensuring adequate cybersecurity governance — is evolving rapidly in response to regulatory requirements, judicial developments, and international governance standards. India's Companies

Act, 2013 does not specifically address cybersecurity governance, but its general provisions on directors' duties (Section 166) and the board's oversight of risk management (Regulation 21 of the SEBI Listing Obligations and Disclosure Requirements for listed companies) create a legal basis for board-level cybersecurity responsibility. CERT-In's cybersecurity guidelines and the telecom security conditions create specific regulatory obligations for telecommunications operators that the board must ensure are met. The intersection of these obligations — companies law duties, securities regulation risk disclosure requirements, and sector-specific security conditions — creates a multi-dimensional cybersecurity governance responsibility for the boards of listed telecom companies that requires both legal awareness and technical literacy at the board level.

The specific board-level cybersecurity governance responsibilities for a major Indian telecommunications operator include: ensuring that the operator has a comprehensive cybersecurity strategy aligned with its business risk profile; overseeing the adequacy of cybersecurity investment relative to the threat environment and regulatory requirements; receiving and acting on regular reports from management on cybersecurity risk status, incident history, and compliance with regulatory requirements; ensuring that significant cybersecurity incidents are promptly disclosed in accordance with securities market disclosure obligations and regulatory reporting requirements; and ensuring that the board itself has sufficient cybersecurity competence (through board-level training, specialist board members, or access to independent expert advice) to exercise meaningful oversight of management's cybersecurity activities. The development of a governance standard for board-level cybersecurity oversight in the telecommunications sector — potentially issued jointly by DoT, CERT-In, and SEBI — would provide clearer guidance for boards of directors on their cybersecurity responsibilities and improve the consistency of cybersecurity governance across the sector.

H.3 Regulatory Sandbox for Security Innovation

The application of the regulatory sandbox concept to telecommunications security innovation — creating a defined environment where operators and security technology companies can test novel security technologies and approaches with relaxed compliance obligations during the testing period — is an emerging regulatory tool that India's security framework should explore. Security innovation is particularly important in the telecommunications sector because the threat landscape evolves rapidly: new attack techniques emerge faster than traditional regulatory frameworks can update security standards, creating a persistent gap between the state of the art in security technology and the minimum standards prescribed by regulation. A security innovation sandbox would enable: the testing of AI-based threat detection systems that use

machine learning techniques not captured in current security evaluation standards; the deployment of novel authentication mechanisms (quantum-resistant cryptography, biometric authentication, zero-trust architecture) in limited operational environments before full-scale deployment; and the assessment of novel active defence techniques (honeypots, deception technology, automated threat hunting) in real network environments. The legal framework for a security innovation sandbox must address the specific challenges of security testing in live networks — ensuring that sandbox participants cannot use the sandbox as cover for deploying insecure systems that harm subscribers — while providing meaningful regulatory flexibility for genuine security innovation.

SUPPLEMENTARY NOTE I

Cybersecurity: Final Perspectives

I.1 Emerging Threats to Mobile Networks

The threat landscape for India's mobile telecommunications networks is evolving rapidly as adversaries — ranging from criminal organisations seeking financial gain to nation-state actors pursuing strategic intelligence objectives — develop increasingly sophisticated attack capabilities that exploit the complexity and interconnectedness of modern mobile network architectures. The most significant emerging threats to India's mobile networks include: SS7 (Signalling System 7) attacks, which exploit vulnerabilities in the legacy signalling protocols used for roaming and inter-operator communications to track subscriber locations, intercept SMS messages, and redirect calls; Diameter protocol attacks, which use similar techniques against the 4G successor to SS7 to attack subscribers on LTE networks; supply chain attacks targeting the software update mechanisms of network equipment, which can enable attackers to install malicious firmware on deployed equipment; and application layer attacks targeting the web-based management interfaces of network elements, which can enable remote access to network configuration and monitoring systems. India's telecommunications security framework must address each of these threat categories through specific technical standards, monitoring requirements, and incident response procedures.

The SS7 vulnerability — which has been publicly known since 2014 and has been demonstrated to enable real-world subscriber location tracking, call interception, and SMS fraud by both criminal actors and nation-state intelligence services — represents a systemic vulnerability in the global mobile telecommunications infrastructure that cannot be fully remediated without fundamental changes to the international telecommunications signalling

architecture. India's response to the SS7 vulnerability — through CERT-In advisories, DoT security condition amendments, and industry coordination — has focused on deploying SS7 firewalls that filter potentially malicious signalling traffic at operators' network boundaries, limiting the attack surface available to external adversaries. However, SS7 firewalls provide incomplete protection: they can block known attack patterns but cannot detect novel attack techniques, and they cannot protect against attacks originating from within a trusted operator's network (such as attacks by a rogue operator or a compromised operator that has been accessed by a hostile state actor). The longer-term solution — the complete migration from SS7 to more secure signalling protocols — requires international coordination that is progressing slowly given the global installed base of SS7-dependent infrastructure.

I.2 CERT-In and International Cooperation

CERT-In's international cooperation activities — through its participation in FIRST (Forum of Incident Response and Security Teams), bilateral CERT partnerships, and multilateral cybersecurity governance forums — are an essential component of India's cybersecurity governance framework that directly benefits the telecommunications sector. FIRST membership provides CERT-In with access to real-time threat intelligence shared by over 500 incident response teams globally, enabling early warning of global cyber attack campaigns before they reach Indian telecommunications infrastructure. CERT-In's bilateral information sharing arrangements with partner CERTs in the US (CISA), UK (NCSC), Australia (ACSC), Japan (NPA), and other strategic partners provide access to classified or sensitive threat intelligence that is not shared through multilateral channels, enabling more specific and actionable warning of targeted attacks against Indian critical infrastructure. CERT-In's contribution to these partnerships — through sharing India-specific threat intelligence and hosting bilateral exercises — maintains the reciprocal character of the relationships that makes them valuable for Indian cybersecurity.

The development of India's international cybersecurity legal framework — specifically the bilateral legal agreements that govern the sharing of cybercrime-related data, the extradition of cybercrime perpetrators, and the mutual recognition of cybersecurity incident determinations — is an important complement to the technical cooperation provided through CERT partnerships. The Budapest Convention on Cybercrime — the primary international legal framework for cybercrime cooperation — has been signed by over 60 countries but not by India, which has historically been reluctant to accede to treaties that it regards as having been negotiated without adequate developing-country participation. India's development of bilateral cybercrime cooperation agreements that achieve the practical objectives of the Budapest Convention

(mutual legal assistance, preservation of evidence, extradition for specified cybercrimes) without accepting the convention's specific legal framework would enable India to participate fully in the international cybercrime cooperation ecosystem while maintaining its principled position on the need for more inclusive international cybercrime governance processes.

I.3 DPDPA Implementation for Telecom: Practical Guidance

The practical implementation of DPDPA compliance for telecommunications operators — covering the full lifecycle of subscriber personal data from collection through processing to deletion — requires a systematic data governance programme that integrates legal requirements, technical controls, and operational procedures. A comprehensive DPDPA implementation programme for a major telecom operator should address: data mapping (identifying all categories of personal data collected, the purposes for which it is processed, the systems in which it is stored, and the third parties with whom it is shared); legal basis assessment (determining the appropriate lawful basis for each category of data processing, including consent requirements for non-essential processing and legitimate use assessments for operational data processing); consent management (implementing the DPDPA-compliant consent mechanisms required for processing that is not covered by the necessity bases, including granular consent options, withdrawal mechanisms, and consent record-keeping); data subject rights processes (establishing operational procedures for handling data principal requests for access, correction, erasure, and portability within the statutory timelines); data security measures (implementing the technical and organisational measures required to protect personal data against unauthorised access, disclosure, and loss); and data breach response (developing and testing breach detection, notification, and remediation procedures that comply with the CERT-In and Data Protection Board notification requirements).

The governance structure for DPDPA compliance in a major telecommunications operator — including the roles and responsibilities of the Data Protection Officer (DPO), the IT security team, the legal team, and business units — must be clearly defined and embedded in the operator's corporate governance framework. The DPO's role under the DPDPA is to: monitor compliance with the Act and with the operator's internal data protection policies; advise on data protection impact assessments for high-risk data processing activities; cooperate with the Data Protection Board in the event of investigations; and act as the point of contact for data subjects exercising their rights. The DPO must have sufficient authority and independence to discharge these functions effectively — reporting to senior management or the board, rather than being embedded in a business unit that might face commercial pressure to de-prioritise data protection compliance. The development of a clear governance framework for DPDPA compliance — with

defined accountabilities, escalation paths, and reporting mechanisms — is as important as the technical and legal implementation work for ensuring that DPDPA compliance is genuinely embedded in the operator's operations.

SUPPLEMENTARY NOTE J

Security: Concluding Analysis

J.1 National Security Architecture for Telecom

The national security architecture for India's telecommunications sector — the institutional and legal framework through which the government identifies and manages national security risks in the sector — involves multiple agencies with distinct but overlapping mandates. The Intelligence Bureau (IB) and the Research and Analysis Wing (RAW), as India's primary domestic and foreign intelligence agencies, assess threats to national security infrastructure including telecommunications. The Ministry of Home Affairs (MHA) coordinates the government's response to internal security threats and oversees the implementation of security conditions in telecommunications licences. The Ministry of Defence ensures that military communications remain secure and that telecommunications infrastructure does not create vulnerabilities to India's defence posture. And DoT, as the licensor of telecommunications services, translates national security requirements into licence conditions and evaluates vendors against security standards through the TTP framework. The coordination between these agencies — and the integration of their distinct intelligence and security perspectives into coherent, actionable regulatory requirements — is the central institutional challenge of national security-oriented telecommunications regulation.

The legal framework through which national security considerations are translated into telecommunications regulatory requirements involves several distinct legal instruments: the Telecommunications Act, 2023's security provisions (which provide the statutory basis for security conditions in authorisations, the TTP framework, and the government's power to issue national security directions); the Unified Licence security conditions (which have been the primary vehicle for implementing national security requirements for licensed operators in the pre-2023 Act period); CERT-In's cybersecurity directions (which implement cybersecurity requirements under the IT Act framework that complement the telecommunications licensing conditions); and the Trusted Telecom Portal guidelines (which implement the supply chain security requirements for telecommunications equipment through the vendor evaluation framework). The coherence and consistency of the obligations imposed through these multiple

legal instruments — and their alignment with India's national security assessment of the specific threats faced by the telecommunications sector — is an ongoing regulatory management challenge that requires close coordination between the security agencies, DoT, and CERT-In.

The transparency of India's telecommunications national security framework — specifically the extent to which the basis for national security requirements in licence conditions and TTP decisions is published and accessible to operators and their advisers — is an area where India's practice differs significantly from that of some comparable democracies. In the UK, Ofcom and the NCSC publish detailed guidance on the security requirements for telecommunications networks, including the specific technical standards that operators must meet and the reasoning for those requirements. In India, the security conditions of the Unified Licence are published, but the specific implementation guidance for many of the most important security requirements — including the TTP evaluation criteria, the LI capability specifications, and the network architecture security requirements — is not publicly available, creating compliance uncertainty for operators and advisers who must meet requirements that are incompletely specified in public documents. The development of more comprehensive, publicly available guidance on telecommunications security requirements — while maintaining appropriate confidentiality for the most sensitive security specifications — would improve the quality and consistency of compliance with national security requirements across the sector.

J.2 Closing Perspectives on Cybersecurity Regulation

India's cybersecurity regulatory framework for the telecommunications sector — encompassing the TTP vendor evaluation framework, CERT-In's incident reporting and response framework, the DPDPA's data security requirements, and the evolving national security conditions — represents a comprehensive but still maturing governance architecture for the security challenges of the digital telecommunications era. The framework's strengths include its broad legal basis (drawing on both the Telecommunications Act and the IT Act), its institutional diversity (multiple agencies with complementary capabilities working in coordination), and its progressive development through successive refinements that have incorporated lessons from global cybersecurity experience. The framework's weaknesses include regulatory fragmentation (multiple overlapping obligations from different regulatory instruments), insufficient transparency (limited public guidance on specific compliance requirements), inadequate enforcement resources (CERT-In and DoT face significant capacity constraints in monitoring and enforcing complex security requirements across hundreds of operators and thousands of vendors), and the persistent challenge of keeping the framework current with a threat landscape that evolves faster than regulatory processes can respond. The Telecommunications Act, 2023's implementation

provides an opportunity to address these weaknesses — through clearer, more consolidated security obligations, more transparent and published compliance guidance, better-resourced enforcement, and faster regulatory adaptation mechanisms — that should be explicitly prioritised in the implementation agenda.

SUPPLEMENTARY NOTE K

Security Regulation: Closing Notes

K.1 Cybersecurity Standards Development

The development of India-specific cybersecurity standards for the telecommunications sector — calibrated to the specific threat landscape, technology deployment patterns, and regulatory context of Indian telecommunications networks — is an important complement to the international standards frameworks (3GPP security specifications, ETSI security standards, ISO 27001) that provide the baseline for global telecommunications security. While international standards provide valuable frameworks developed through global expert consensus, they are necessarily generic and may not address the specific characteristics of India's telecommunications environment: the particular threat actors that target Indian telecommunications infrastructure, the specific technology configurations deployed in India's networks, and the specific regulatory and institutional context in which security governance operates. TEC's telecommunications security standards development programme — working through its technical working groups with industry participation — should systematically review international standards for their applicability to India's context and develop India-specific additions or modifications where the generic standards are insufficient. The publication of these India-specific telecommunications security standards — through TEC's standards catalogue and through their incorporation into licence conditions and TTP evaluation criteria — would improve the specificity and effectiveness of India's telecommunications security regulatory framework.

The role of Indian industry in telecommunications security standards development — both domestically (through TEC working groups) and internationally (through 3GPP, ETSI, ITU-T, and O-RAN Alliance security working groups) — is an important aspect of India's influence on the global telecommunications security landscape. India's participation in international telecommunications security standards bodies has historically been limited by resource constraints and by the limited number of Indian organisations with the technical expertise to contribute meaningfully to highly technical security standards discussions. The government's investment in telecommunications R&D; through C-DoT, TEC, and the IIT system is creating a

growing base of technical expertise that should translate into more active Indian participation in international standards bodies. Building India's capacity for international telecommunications security standards engagement — through dedicated participation resources, training programmes for standards delegates, and strategic prioritisation of the standards bodies and working groups where India's influence is most commercially and strategically significant — is an important long-term investment in India's technological sovereignty and global influence.

The legal framework for cybersecurity insurance in the Indian telecommunications sector — still largely undeveloped but increasingly important as the financial consequences of cybersecurity incidents grow — requires coordinated development by IRDAI (which regulates insurance products), DoT (which could mandate minimum cyber insurance as an authorisation condition), and CERT-In (which could specify the security standards that must be met for cyber insurance eligibility). The key policy questions for a telecommunications cybersecurity insurance framework include: should cyber insurance be mandatory (as a condition of telecom authorisation) or voluntary (as a market-based risk management tool)? What should be the minimum coverage requirements for mandatory insurance (ensuring that coverage is sufficient to address the most significant cyber risk exposures)? How should the insurance premium be structured to create positive incentives for cybersecurity investment (rather than simply transferring risk without incentivising risk reduction)? And how should the proceeds of insurance claims be treated for regulatory purposes (specifically, whether insurance recoveries should offset regulatory penalties for cyber incidents)? The development of a consultative, cross-regulatory process for addressing these questions — involving DoT, CERT-In, IRDAI, and the industry — would produce a more coherent and effective cybersecurity insurance framework than piecemeal regulatory development by individual agencies.

K.2 Closing Thoughts on Cybersecurity Governance

The cybersecurity governance framework for India's telecommunications sector — as described and analysed throughout this booklet — is at a critical juncture. The technical threats facing the sector are growing in sophistication and scale; the commercial and social consequences of telecommunications cybersecurity failures are becoming more significant as the economy and society become more dependent on digital connectivity; and the regulatory and institutional frameworks for managing these threats are still developing. The Telecommunications Act, 2023 provides a significantly improved statutory foundation for telecommunications cybersecurity governance, and the implementing rules being developed under the Act offer an opportunity to substantially strengthen the practical effectiveness of the regulatory framework. Seizing this opportunity — by developing clear, comprehensive, and

well-resourced cybersecurity regulatory requirements; building the institutional capacity to enforce those requirements effectively; and fostering the industry culture of security investment and transparency that makes regulatory compliance a floor rather than a ceiling — is one of the most important governance tasks of the coming decade. The ultimate measure of success is not the sophistication of the regulatory framework but the actual security of the telecommunications infrastructure on which India's digital future depends.

FINAL NOTE: Cybersecurity — A Practitioner's Synthesis

The cybersecurity and data protection regulatory framework for India's telecommunications sector — as comprehensively analysed throughout this booklet — is one of the most demanding and rapidly evolving regulatory environments in Indian law. The intersection of telecommunications regulation (governed by the Telecommunications Act, 2023 and TRAI's regulatory framework), data protection law (governed by the DPDPA, 2023), cybersecurity law (governed by the IT Act and CERT-In's directions), national security law (governed by the Intelligence Bureau's oversight and the telecom licence security conditions), and constitutional law (governed by Puttaswamy's privacy framework and the proportionality doctrine) creates a multi-dimensional compliance challenge for telecommunications operators and a multi-disciplinary practice area for legal advisers. The practitioners who work in this space must maintain expertise across all these regulatory dimensions while also understanding the technical telecommunications and cybersecurity foundations that give the law its practical meaning. The development of integrated cybersecurity and data protection legal practice — combining technical knowledge, regulatory awareness, and constitutional literacy — is one of the most important professional development challenges for the next generation of Indian telecommunications lawyers.

The practical advice for telecommunications operators managing cybersecurity and data protection compliance can be distilled into several key principles. First, compliance is a process, not a destination: the threat landscape and regulatory framework evolve continuously, and compliance programmes must be designed to adapt rather than to achieve a static state of compliance with current requirements. Second, security and privacy are complementary, not competing: a telecommunications operator that protects its network from cybersecurity threats is also protecting the privacy of its subscribers, and an operator that respects data protection principles in its network operations is also improving its security posture. Third, regulators are partners as much as enforcers: in the cybersecurity context especially, operators and regulators share a common interest in improving the security of the telecommunications infrastructure, and transparent engagement with CERT-In and DoT — including proactive disclosure of security

vulnerabilities and incidents — builds regulatory relationships that are more valuable than the adversarial posture of minimising regulatory engagement. Fourth, the board must own cybersecurity and data protection: these are material business risks that require board-level oversight, adequate resource allocation, and the same management attention as financial and operational risks.

India's telecommunications sector is at the forefront of the global convergence between telecommunications technology and digital governance — experiencing the full range of cybersecurity, privacy, and regulatory challenges that other developing countries will face as their digital sectors mature, and developing regulatory responses that will inform global best practice. The practitioners who work in India's telecommunications cybersecurity and data protection space have an opportunity — and a responsibility — to contribute to this global learning by: developing robust, legally defensible compliance frameworks that serve as models for other markets; engaging constructively with regulatory development processes to ensure that India's regulations reflect both best practice and practical operability; contributing to international standards bodies and regulatory forums to ensure that India's experience shapes global frameworks; and communicating the insights of regulatory practice through publications, conferences, and professional development programmes that build the broader community's expertise.

The regulatory treatment of cybersecurity vulnerability disclosures — the process by which security researchers, operators, and vendors identify, report, and remediate security vulnerabilities in telecommunications infrastructure — is an important area of cybersecurity governance that India's regulatory framework must address more explicitly. The current framework — which relies primarily on CERT-In's vulnerability disclosure guidelines and on the security conditions of telecommunications licences — does not provide a comprehensive or well-coordinated process for managing the disclosure and remediation of vulnerabilities in telecommunications-specific equipment and systems. The development of a telecommunications-specific vulnerability disclosure policy — specifying: the process for security researchers to report vulnerabilities in telecommunications equipment to vendors; the timeline within which vendors must acknowledge, assess, and remediate disclosed vulnerabilities; the process for notifying affected operators of vulnerabilities and required mitigations; and the circumstances under which public disclosure of unpatched vulnerabilities is appropriate — would significantly improve the speed and effectiveness of vulnerability remediation in the sector. CERT-In and TEC should jointly develop this telecommunications vulnerability disclosure framework, in consultation with operators, equipment vendors, and the security research

community, ensuring that it reflects both the specific technical characteristics of telecommunications security vulnerabilities and the operational realities of patching and updating large, complex deployed networks.

The security implications of increasingly automated network operations — where AI systems make real-time decisions about traffic routing, resource allocation, and security response without human intervention — require proactive regulatory engagement. The risk of "automation surprise" — unexpected, emergent behaviours from AI network management systems that have not been foreseen in the system's design — is a significant safety and security concern for telecommunications networks. Unlike traditional network equipment (whose behaviour is fully determined by its software and configuration), AI-based network management systems exhibit behaviours that may not be predictable from their design specifications, particularly in rare or novel operational conditions that differ from their training data. The regulatory framework for AI in telecommunications network management must address: pre-deployment testing standards (requiring operators to test AI network management systems against a comprehensive range of scenarios before deployment, including adversarial scenarios designed to reveal unexpected behaviours); continuous monitoring requirements (requiring ongoing assessment of AI system behaviour in production to detect drift from expected behaviour); incident reporting requirements (requiring operators to report significant unexpected AI system behaviours to CERT-In and DoT); and human oversight requirements (specifying the conditions under which AI-driven network management decisions must be reviewed or overridden by human operators).

The international dimensions of India's telecommunications cybersecurity framework — specifically its alignment with and divergence from the cybersecurity frameworks of India's major trading and strategic partners — have significant implications for both the effectiveness of India's cybersecurity governance and its digital economy relationships. India's bilateral digital security arrangements with the United States, European Union, Japan, Australia, and the United Kingdom — which include information sharing, joint incident response exercises, and mutual recognition of security standards — provide a network of security cooperation that strengthens India's collective defence against sophisticated cyber threats. The divergence between India's cybersecurity requirements (particularly in areas such as data localisation and lawful interception) and those of its democratic partners creates friction in digital trade and investment that requires careful management. The development of a comprehensive digital security engagement strategy — aligning India's cybersecurity regulatory framework with international best practice where feasible, engaging constructively with partners on areas of divergence, and proactively contributing to the development of international cybersecurity norms that reflect

India's interests — is an important foreign policy and regulatory governance priority.

DISCLAIMER: This publication is prepared for general informational and educational purposes only. It does not constitute legal advice and does not create an attorney-client relationship. Readers are advised to seek professional legal counsel for specific legal matters. Bhatt & Joshi Associates does not make any representation as to the accuracy or completeness of information contained herein. This publication complies with the Bar Council of India Rules on Professional Standards and is not intended as solicitation.