

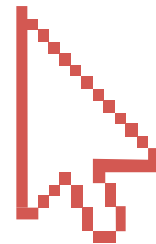


GLOBAL
NETWORK
INITIATIVE



THE SURVEILLANCE LAW LANDSCAPE IN INDIA AND THE IMPACT OF *Puttaswamy*

CENTRE FOR COMMUNICATION GOVERNANCE
at National Law University Delhi





Published by National Law University Delhi Press,

Sector 14, Dwarka, New Delhi 110 078

© National Law University Delhi 2023

All Rights Reserved

Authors: Jhalak M. Kakkar, Nehmat Kaur, Sharngan Aravindakshan, Shashank Mohan, Shubhi Agarwal, Sravya Movva, Vasudev Devadasan, and Vrinda Bhandari

Patrons: Professor (Dr.) G.S. Bajpai (Vice Chancellor, NLUD), Professor (Dr.) Harpreet Kaur (Registrar, NLUD)

Faculty Director, CCG: Dr. Daniel Mathew

Executive Director, CCG: Jhalak M. Kakkar

Supported by

Global Network Initiative



Acknowledgements: This report was made possible by the generous support we received from the National Law University Delhi (NLUD). The Centre for Communication Governance (CCG) would therefore like to thank our patrons, the Vice Chancellor Professor (Dr.) G.S. Bajpai and the Registrar Prof. (Dr.) Harpreet Kaur of NLUD for their guidance. CCG would also like to thank our Faculty Director Dr. Daniel Mathew for his continuous direction and mentorship. This report would not be possible without the support provided by the Global Network Initiative (GNI). We are grateful for comments received from GNI, the Data Governance Network and their reviewers and Srinivas Kodali. CCG would also like to thank Smitha Krishna Prasad for conceptualising the report. Special thanks to the ever-present and ever-patient Suman Negi and Preeti Bhandari for the unending support for all the work we do at CCG. Lastly, we would also like to thank all members of CCG for the many ways in which they supported the report.

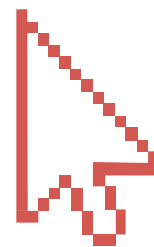


(CC-BY-NC-SA 4.0)

ISBN 978-93-84272-43-2

THE SURVEILLANCE LAW LANDSCAPE IN INDIA AND THE IMPACT OF *Puttaswamy*

**Jhalak M. Kakkar, Nehmat Kaur, Sharngan Aravindakshan,
Shashank Mohan, Shubhi Agarwal, Sravya Movva, Vasudev
Devadasan, and Vrinda Bhandari**



**An academic report by the National Law University
Delhi, Centre for Communication Governance**

→ ccgdelhi.org

→ **Twitter: @CCGNLUD**

Supported by the Global Network Initiative

→ GlobalNetworkInitiative.org

→ **Twitter: @theGNI**

**as part of the Sustaining Multi-stakeholder Networks
for Internet Freedom Project**

Disclaimer: The content, analysis, and recommendations of this report belong solely to the author and do not necessarily reflect the opinions of the Global Network Initiative.

ABOUT THE NATIONAL LAW UNIVERSITY DELHI (NLUD)

The National Law University Delhi is one of the leading law universities in the capital city of India. Established in 2008 by an Act of the Delhi legislature (Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold the constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law.

The University offers a five year integrated B.A., LL.B (Hons.), a one-year postgraduate masters in law (LL.M), and a Ph.D. program, along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research. Over the last decade, the University has established many specialised research centres and this includes the Centre for Communication Governance (CCG), Centre for Innovation, Intellectual Property and Competition, Centre for Corporate Law and Governance, Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

ABOUT THE CENTRE FOR COMMUNICATION GOVERNANCE

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research in India on information technology law and policy in India and in a short span of time has become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain. CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, Law Commission of India, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, and the Tech Policy Design Centre at the Australian National University.

The Centre has had multiple publications over the years including reports on Intermediary Liability in India, a report Mapping the Blockchain Ecosystem in India and Australia, a book on Privacy and the Indian Supreme Court, Hate Speech Report, and most recently two essay series, one on Democracy in the Shadow of Big and Emerging Tech, and a second on Emerging Trends in Data Governance. The Centre has launched freely accessible online databases - Privacy Law Library (PLL) and High Court Tracker (HCT) to track privacy jurisprudence across the country and more than sixteen jurisdictions across the globe in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. CCG also has an online 'Teaching and Learning Resource' database for sharing research-oriented reading references on information technology law and policy. In recent times, the Centre has also offered courses on AI Law and Policy, Technology and Policy, and first principles of cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and ensure their nuanced engagement with the dynamic space of existing and emerging technology and cyberspace, their implications for the society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the

University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy.

ccgdelhi.org | privacylibrary.ccgnlud.org | ccg@nludelhi.ac.in | Twitter: @CCGNLUD



FOREWORD

I was fascinated to read the draft of the National Law University, Delhi publication titled "The surveillance law landscape in India and the impact of *Puttaswamy*". The decision of the 9-Judge Bench of the Supreme Court of India in the case of *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1 was a landmark judgment holding that right to privacy is an integral part of the right to life guaranteed under Article 21 of the Constitution of India. Privacy of an individual is a very wide concept. There are various facets of privacy. In fact, the concept of privacy is ever evolving with the changing society. The transformative constitutionalism will result in expansion of the concept of privacy.

It can be always said that privacy has always been a natural right. It is an integral part of the fundamental right to live with dignity. In the 21st Century, the world has changed very fast and surveillance by the State and its agencies has become a very crucial issue. The reason is that by using modern technology, keeping surveillance on individuals has become very easy. Therefore, the instances of State-sponsored surveillance on individuals in breach of privacy rights are ever increasing.

The Publication of the University deals exhaustively with several aspects of surveillance in the context of privacy rights. It also deals with the absence of proper procedural safeguards for preventing illegal surveillance. It is rightly said that post-*Puttaswamy*, surveillance cannot be authorised purely on the ground of expediency. The surveillance on the ground of necessity should be authorised only when no other equally effective and restrictive measure is available. The State cannot authorise surveillance which will encroach upon the right to privacy only because it is desirable.

The issue of lack of transparency and accountability when it comes to the operation of surveillance systems is an area of great concern which is highlighted in the Report. In the coming years, dealing with issues of surveillance affecting the right to privacy is going to be a huge challenge for the Constitutional Courts. The work done by the University has to be applauded as this work should be the basis for discussion at the national level on all issues

concerning surveillance. In fact, these issues need a nationwide debate.

I appreciate and admire the work done by those who have contributed to this Publication. In fact, reading the draft Publication triggered my thought process. I have avoided the temptation to express my views on the subject as it will be inappropriate considering the constitutional post which I am holding at present.

This Publication will be useful not only for law students but to every citizen who is concerned about his right to privacy.

20.05.2023


(ABHAY S. OKA)

PREFACE

The right to privacy has been emphatically re-affirmed as having constitutional status by a nine-judge bench of the Supreme Court of India in the landmark decision of *K.S. Puttaswamy v Union of India*. The judgement represents a watershed moment, not just for the right to privacy in India, but also the broader rights landscape in the country. The right to privacy has important consequences for issues such as the freedom of expression and association, the right against self-incrimination, and the right to decisional autonomy. In *Puttaswamy*, the Supreme Court characterised the right to privacy as not just the “*freedom from unwarranted stimuli*”, but also the positive ability to pursue dissent and heterodoxy, to defy societal mores without fear, and live one’s life on one’s own terms without the trepidation of being monitored or subjected to reprisal. This conception of privacy has already revolutionised areas of Indian society, with the Supreme Court in 2019 de-criminalising homosexuality on the grounds of privacy and decisional autonomy. However, one of the key impacts of the judgment may be on how it has the potential to re-shape India’s surveillance law landscape.

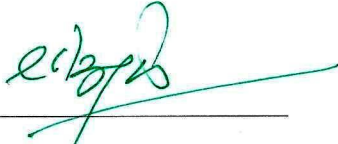
The question of State surveillance is at the heart of *Puttaswamy*’s conception of privacy. As former Chief Justice Subba Rao noted decades ago, a person under surveillance can move physically, but they cannot do so freely, for all their activities are watched and noted (*Kharak Singh v State of Uttar Pradesh* 1954). The spectre of surveillance may inhibit an individual’s ability to live a life of liberty, denying them the solitude to question society’s dominant practices and inhibiting their willingness to seek out new ideas. Ultimately this may constrain the diversity and pluralism that constitutional democracy seeks to protect. Thus, while surveillance is not *per se* unconstitutional, it must abide by constitutional restraints.

The Court in *Puttaswamy* established that privacy infringing measures such as government surveillance must be subject to constitutional protections and safeguards. It set out the test of proportionality, requiring privacy limiting measures to satisfy certain criteria such as legality, necessity, and procedural safeguards against potential abuse. While *Puttaswamy* represents a crucial moment for the reformation of the surveillance landscape in India, legal structures regulating surveillance in India pre-date *Puttaswamy*, and in some cases, even the adoption of the Constitution.

In this context, it is my pleasure to introduce the present report titled ‘*The surveillance law landscape in India and the impact of Puttaswamy*’. The report provides a detailed analysis of the constitutional and legal framework for surveillance in India, including the various laws and regulations that govern various surveillance measures. It also examines the safeguards and accountability mechanisms that are in place to protect individual privacy and prevent the abuse of surveillance powers. The report further explores the challenges and limitations of the current legal framework, including potential inconsistencies with the principles set out in *Puttaswamy*, and the need for greater transparency and accountability. The report also makes broad recommendations for decision makers to assess the realignment of surveillance law in India with constitutional principles in light of *Puttaswamy* and other global developments. As technology continues to evolve, the report also enumerates India’s modern surveillance systems and explains where they sit in the overall landscape.

As India seeks to reform its telecommunications and information technology legislation and adopt a first ever data protection law, this report makes an important contribution to the ongoing dialogue on how governmental surveillance can be consistent with the right to privacy. The

Centre for Communication Governance has conducted extensive research and analysis, drawing on a range of legal and policy documents. I commend the authors for their dedication and diligence in producing this report, and I hope that it will be a useful resource for judges, policymakers, legal professionals and students, and civil society organisations as they continue to engage in the important work of safeguarding privacy and facilitating governance that is in harmony with the Constitution.



Prof. (Dr.) G.S. Bajpai,

*Vice Chancellor,
National Law University Delhi*

CONTENTS

Executive Summary	14
1. Introduction	20
2. Indian Privacy Doctrine and Surveillance	25
(a) The Right to Privacy in <i>Puttaswamy</i>	25
(b) Surveillance as a restriction on constitutional rights	26
(c) Assessing the constitutionality of surveillance measures	28
3. India's Legislative Framework for Targeted Surveillance	32
(a) Interception under the Telegraph Act, 1885	32
(b) Duty of telecom service providers	40
(c) Surveillance under the Information Technology Act, 2000	44
(d) Interception and information gathering under criminal law	60
4. Impact of <i>Puttaswamy</i> on Statutory Surveillance Framework	65
(a) Surveillance law after PUCL: A time for reconsideration	67
(b) Independent oversight of surveillance action	69
(c) Illegally obtained evidence	74
(d) Post- <i>Puttaswamy</i> reforms to surveillance	78
5. Mapping India's Modern Surveillance Programs	82
(a) Centralised Monitoring System	84
(b) Network Traffic Analysis	88
6. Testing Modern Surveillance Programs against <i>Puttaswamy</i>	89
(a) Legality	89
(b) Legitimate aim	93
(c) Suitability	93
(d) Necessity and Proportionality	94
(e) Procedural Safeguards	96
7. Way Forward and Conclusion	99
Annexure: Data Collection and Sharing Programs	103

List of Abbreviations

Aadhaar Judgement	<i>K.S. Puttaswamy II vs. Union of India (2019) 1 SCC 1</i>
AFRS	Automated facial recognition systems
CBI	Central Bureau of Investigation
CCA	Controller of Certifying Authorities
CCTNS	Crime and Criminal Tracking Network and Systems
CDRs	Call Detail Records
CERT-In	Indian Computer Emergency Response Team
CMS	Central Monitoring System
CrPC	Code of Criminal Procedure, 1973
DPDP Bill	Digital Personal Data Protection Bill, 2022
ECtHR	European Court of Human Rights
Evidence Act	Indian Evidence Act, 1872
FIR	First Information Report
Intermediary Guidelines 2021	Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021
ISP	Internet Service Provider
IT Act	Information Technology Act, 2000
IT Interception Rules	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
IT Traffic Data Rules	Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009
MCOCA	Maharashtra Control of Terrorism and Organised Crime Act, 1999
MEITY	Ministry of Electronics and Information Technology
NATGRID	National Intelligence Grid
NCRB	National Crime Records Bureau
NETRA	Network Traffic Analysis
NHS	National Health Stack

RTI Act	Right to Information Act, 2005
SEBI	Securities and Exchange Board of India
Telegraph Act	Indian Telegraph Act, 1885
Telegraph Rules	Indian Telegraph Rules, 1951
TSP	Telecom Service Provider
UAPA	Unlawful Activities Prevention Act, 1967
UL	Unified License Agreements

Executive Summary

India, like countries across the world, has experienced a growth in the avenues of State surveillance, driven by an expansion in the technical capacity of the State to conduct surveillance and the increased use of electronic communications and information technology tools by individuals. Indian doctrine surrounding the right to privacy represented a patchwork of protections that did not confront this modern paradigm until the landmark judgement by a nine-judge bench of the Supreme Court in *K.S. Puttaswamy vs. Union of India*. The judgement re-affirmed the right to privacy as embedded in the Indian Constitution and provided an analytical framework to evaluate the constitutionality of privacy-infringing measures such as State surveillance, by adopting the proportionality test.

This report harnesses this new conceptualisation of the right to privacy and applies the analytical framework provided by the Supreme Court to assess India's framework for targeted and modern surveillance programs. Some of the key findings of the report are set out below.

1. Controlling precedent of *Puttaswamy*

Context: The Indian Constitution does not contain an explicit privacy guarantee or protection. Over the years courts have recognized that privacy protections are implicit in the constitutional guarantees of Fundamental Rights that the Constitution secures. However, the judgement in *Puttaswamy* settles any doubt that the right to privacy is constitutionally protected. Crucially, because the decision was taken by a nine-judge bench of the Supreme Court, it constitutes controlling precedent for courts across the country that are tasked with evaluating privacy infringing measures.

On the question of evaluation, the bench in *Puttaswamy* adopted the proportionality test to determine the constitutionality of privacy-infringing measures. The test laid down by the Court is rigorous in part due to its conjunctive structure. Where a State measure interferes with the right to privacy, it is only constitutional when it satisfies the requirements of: (i) legality, the measure is authorised by statute; (ii) legitimate goal, the measure pursues a proper purpose; (iii) suitability, the measure takes meaningful steps towards achieving the proper purpose; (iv) necessity, the measure is the least rights-restrictive measure amongst equally effective alternatives; (v) proportionality, the measure does not disproportionately impact individual rights; and (vi) procedural safeguards, the measure incorporates meaningful guardrails against possible abuse.

Insight: The application of the proportionality test by Indian courts post-*Puttaswamy* has been critiqued and the nature and scope of judicial review mitigates against the Court prescribing detailed instructions on how surveillance may be conducted. Nonetheless, the judgement in *Puttaswamy* constitutes a watershed moment as it represents an invitation to future courts to protect the privacy of individuals against instances of unconstitutional State surveillance and empowers them with the tools to do so. This is of particular relevance given that several aspects of India's surveillance framework are currently under legal challenge before courts.

2. IT Act lowers the threshold for targeted surveillance

Context: Under the Telegraph Act, there exists twin conditions to initiate interception: (i) there should be a “public emergency” or the interception is to ensure “public safety”; and (ii) the interception must be “necessary or expedient” for reasons concerning the security, sovereignty, integrity of India, its relations with foreign States, public order, or preventing the incitement of an offence. However, under the IT Act, the threshold for initiating electronic surveillance is merely that the government is satisfied that it is “necessary or expedient” to initiate surveillance in the interests of the sovereignty, integrity, defence, or security of India, its friendly relations with foreign States, public order, preventing the incitement to any cognizable offence, or for the investigation of an offence. Thus, under the IT Act, the pre-condition of “public emergency” or “public safety” is dispensed with, and surveillance may be initiated to investigate offences. This significantly lowers the substantive threshold for when targeted surveillance may be initiated.

Insight: Post-*Puttaswamy*, the question of whether surveillance can be authorised purely on the grounds of ‘expedience’ needs to be reassessed. An essential limb of the proportionality test is that of “necessity”, a measure should only be authorised when no equally effective, less rights-restrictive measure is available. Authorising surveillance merely because it is beneficial or desirable may fall foul of the necessity requirement set out in *Puttaswamy*. Further, the ground of “investigation of an offence” fails to distinguish what types of offences surveillance may be an appropriate response to. If surveillance (a rights-impinging measure) is adopted for minor offences, it would be disproportionate. Thus, without additional statutory guidance, the proportionality of the current thresholds for targeted surveillance under the IT Act remain in doubt.

3. Ineffective procedural safeguards and need for independent oversight

Context: Surveillance orders issued under the Telegraph Act and the IT Act

are reviewed by a committee of senior government officials under Rule 419A of the Telegraph Rules. Thus, orders issued and operationalised by the executive branch are also scrutinised by the executive branch through an in-house ‘Review Committee’. The Union Government has refused to disclose the total number of surveillance orders issued by it for given periods. Government disclosures under the Right to Information Act and the work done by a government appointed committee to create India’s data protection framework, suggests that the procedural safeguard of the Review Committee provides insufficient oversight over government surveillance.

Insight: Right to privacy doctrine post-*Puttaswamy* may necessitate additional protections in the form of independent authorisation and scrutiny for surveillance activities. In its 1997 decision in *PUCL vs. Union of India*, the Supreme Court declined to invalidate provisions of the Telegraph Act for failing to require judicial scrutiny of telephonic interceptions. However, since *PUCL* there has been a paradigm shift in the nature and volume of surveillance, as well as legal doctrine with the decision in *Puttaswamy*.

When evaluating the constitutionality of a surveillance measure, under the “necessity” limb of the proportionality test, a court must consider alternatives to the impugned measure that still achieve the government’s stated objective in ‘real and substantial manner’. It must then determine whether the impugned measure is the least-rights restrictive but equally effective measure that the government can adopt; if not, the measure fails the test of necessity. If the “measure” is considered as a whole (from authorisation to oversight), independent scrutiny by judges or another independent body would be more rights-protective than the status-quo of executive oversight. Further, the government has not demonstrated why judicial or independent scrutiny (either *ex-ante* or *ex-post*) of surveillance would hamper the government’s investigative aims. Thus, judicial or independent oversight represents a less-restrictive (more protective) measure that is likely equally effective. This should result in a reconsideration of the constitutionality of the current procedural safeguards for surveillance.

4. Issues with evidence gathered through unlawful surveillance

Context: Under Indian law, the primary rule for evaluating the admissibility of evidence is relevance. The Supreme Court in *Pooran Mal vs. Director of Inspection* has held that illegally obtained evidence is admissible absent a constitutional or statutory prohibition. Neither the Constitution nor the IT Act, Telegraph Act, or Evidence Act place a bar on the admissibility of evidence collected through unlawful surveillance. This poses a significant challenge to the accountability of surveillance programs in India. Given the secret nature of surveillance, the

affected individuals cannot meaningfully challenge the legality of the surveillance conducted against them until the contents of such surveillance are introduced at their trial. Admitting into evidence information that was gathered through unlawful surveillance creates a situation where law enforcement accrues significant prosecutorial benefits from conducting unlawful surveillance but risks no legal consequence. Thus, excluding evidence collected pursuant to unlawful surveillance may be an invaluable safeguard against investigatory transgressions and incentivise law enforcement to comply with procedures for lawful surveillance.

Insight: The Supreme Court's decision in *Pooran Mal* relied on an earlier decision of the Court in *M.P. Sharma vs. Satish Chandra*. The decision in *M.P. Sharma*, along with other decisions such as that in *Kharak Singh vs. State of Uttar Pradesh* opined that privacy was not a constitutionally protected right. Crucially, the decisions in *M.P. Sharma* and *Kharak Singh* led to a line of cases that failed to recognize the importance of privacy, including those concerning the admissibility of intercepted communications at trial. However, the decisions in *M.P. Sharma* and *Kharak Singh* were expressly overruled in *Puttaswamy*, substantially undermining the doctrinal foundations of latter cases admitting illegally obtained evidence. Thus, the issue of whether evidence gathered through unconstitutional, privacy-infringing surveillance is admissible at trial may also need to be revisited post-*Puttaswamy*.

5. Constitutionality of modern surveillance programs

Context: In the past few years, India has implemented newer surveillance programs such as the Central Monitoring System (CMS) and the Network Traffic Analysis program (NETRA). There is limited information regarding the exact nature and operation of these programs. However, unlike traditional interception measures under the Telegraph Act and IT Act which are reliant on telecom and internet companies and target specific individuals, these programs seek to automate the government's ability to intercept and monitor communications and may possess mass surveillance capabilities leading to the monitoring of large groups of individuals to identify and investigate potential illegality. For example, NETRA is a dragnet tool that intercepts and analyses internet traffic for specific keywords such as "bomb"..

Insight: As privacy limiting measures, the constitutionality of these programs is subject to their satisfying the proportionality standard set out in *Puttaswamy*. The first limb of the proportionality test is that of "legality", which requires all privacy infringing measures to be authorised by statute. While the Union Government has asserted that these programs are governed by the Telegraph Act and the IT Act;

- i. the CMS facilitates interception without assistance from telecom companies in a manner not contemplated by the Telegraph Act or the Telegraph Rules; while

- ii. limited publicly available information suggests that NETRA is envisaged as a potential mass, undirected surveillance system contrary to the two statutes' regime of specific and targeted authorisation for interception.

Thus, it remains questionable whether CMS or NETRA are specifically authorised by any statute. Both programs have been implemented pursuant to decisions by the executive, and the limited information available regarding them comes from government tenders, responses to parliamentary questions, and disclosures under the Right to Information Act. Thus, to the extent that such programs operate outside the ambit of the Telegraph Act and IT Act, their constitutionality remains open to question.

The test of proportionality set out in *Puttaswamy* is conjunctive, and a failure of the “legality” limb opens up such programs to being invalidated by courts. Further, because these programs are not authorised by statute, there is limited information regarding how they are intended to be operated, making an analysis of limbs such as legitimate aim, necessity, and proportionality hard to conduct. For example, both the Telegraph Act and IT Act clearly state the grounds on which interception may be initiated, requiring these grounds to be satisfied *in each instance* where surveillance is undertaken. However, a program such as NETRA contemplates the automatic, ongoing, and wholesale collection of information, making it impractical (if not meaningless) to evaluate whether the grounds for surveillance under the IT Act or Telegraph Act are satisfied.

Thus, given these programs operate beyond the four corners of the Telegraph Act and IT Act, and their lack of alternative statutory basis or any transparency surrounding the programs, the operation of these programs cannot be adequately tested against any standards provided for in legislation. It is unclear how and for what purposes they are being used, making a legal analysis of whether they pursue a ‘proper purpose’ or are ‘necessary’ challenging.

The Way Forward

Several provisions authorising targeted surveillance, as well as India’s modern surveillance programs, are currently under challenge before courts. India is also in the process of adopting a data protection framework and revamping its telecommunications and information technology legislation. Considering this context, we suggest that:

- i. The substantive threshold for authorising surveillance be that of “necessity”, where less intrusive methods of intelligence gathering have failed.
- ii. India adopts robust independent oversight of State surveillance activities. This includes requiring law enforcement to secure prior authorisation for

initiating surveillance from an independent or judicial authority. We also suggest independent ex-post oversight.

- iii. In addition to oversight, there should be increased transparency to the public and Parliament regarding the use of surveillance measures in a manner that does not interfere with active investigations. For example, regular reporting on the aggregate number of interception and monitoring actions will not hamper investigations.
- iv. Evidence gathered through measures that violate the constitutional right to privacy of individuals should not be admissible in court.
- v. India's modern surveillance programs which may have mass surveillance capabilities should first be authorised by statute.

1. Introduction

States have been carrying out surveillance for hundreds of years. However, in the past, limited technological capacity meant that State surveillance could not embody the ‘Panopticon’ or the ‘all-seeing State’.¹ Surveillance was restricted to informant networks, physical surveillance, postal mail tracking, and telegraph interception, that allowed governments to gather limited information about persons of interest.² As the U.S. Supreme Court’s Justice Sotomayor noted, “in the pre- computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.”³ However, the scope, extent, effectiveness, and very nature of surveillance has significantly changed over time.⁴

As technology has become more sophisticated and reliance on physical proximity has reduced, States can access a much larger set of data sources, such as call records, CCTV surveillance, and footprints left on the internet.⁵ Today, States can conduct surveillance across a wider swathe of the population, with CCTV cameras allowing for limitless real-time observation, not just of persons of interest, but practically all persons within the vicinity of these cameras.⁶ Surveillance over any given individual is now also deeper and more invasive, with voice, facial, and

¹ James Waldo, ‘A Short History of Surveillance and Privacy in the United States’, *Engaging Privacy and Information Technology in a Digital Age* (National Academies Press 2007); David Lyon, ‘Surveillance, Power and Everyday Life’ in Phillip Kalantzis-Cope and Karim Gherab-Martín (eds), *Emerging Digital Spaces in Contemporary Society: Properties of Technology* (Palgrave Macmillan UK 2010).

² Ben Underwood and Hossein Saiedian, ‘Mass Surveillance: A Study of Past Practices and Technologies to Predict Future Directions’ (2021) 4 *Security and Privacy*.

³ *United States v Jones* 565 US 400 (2012) (Sotomayor J. concurring) (U.S. Supreme Court).

⁴ Zachary W Smith, ‘Privacy and Security Post-Snowden: Surveillance Law and Policy in the United States and India’ (2014) 9 *Intercultural Human Rights Law Review* 137; Vrinda Bhandari and Karan Lahiri, ‘The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World’ (2020) 3 *University of Oxford Human Rights Hub Journal* 15.

⁵ Neil M Richards, ‘The Dangers of Surveillance’ (2013) 126 *Harvard Law Review* 1934; Thorin Klosowski, ‘Facial Recognition Is Everywhere. Here’s What We Can Do About It.’ (*Wirecutter: Reviews for the Real World*, 15 July 2020) <<https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>> accessed 16 February 2023; Steven Feldstein, ‘The Global Expansion of AI Surveillance’ (Carnegie Endowment for International Peace 2019) <https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf> accessed 16 February 2023.

⁶ Jeremy Schiff and others, ‘Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns’ in Andrew Senior (ed), *Protecting Privacy in Video Surveillance* (Springer 2009).

emotional recognition technology allowing for precise identification.⁷ Surveillance has thus become both wider and deeper.⁸ The increase of the State's surveillance capacity is also dialectically connected with the increased use of electronic networks, devices, and services by citizens.⁹ Today, more information about citizens is available on the internet than ever before, and governments have shown a willingness to capture and utilise this information for surveillance.¹⁰

The development and use of surveillance tools in India has followed a similar path, with an increase in the deployment of new age surveillance technology such as dragnet systems for electronic surveillance, facial recognition, and the use of data analytics and profiling on individuals.¹¹ India's modern surveillance programs such as the Central Monitoring System ("CMS"), the National Intelligence Grid ("NATGRID"), and Network Traffic Analysis ("NETRA") allow for the automation of interception, the facilitating of data sharing for the creation of an integrated intelligence database, and the wholesale (or dragnet) collection of electronic communications to identify threats.¹²

⁷ Deepayan Bhowmik and Mehryar Emambakhsh, 'Image Processing for Surveillance and Security', *Handbook of Research on Applied Cybernetics and Systems Science* (IGI Global 2017); KIKTOVA Eva and JUHAR Jozef, 'Speaker Recognition for Surveillance Application' (2015) 8 *Journal of Electrical and Electronics Engineering* 19; Article 19, 'Emotional Entanglement: China's Emotion Recognition Market and Its Implication for Human Rights' (Article 19 2021) <<https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>> accessed 26 May 2022.

⁸ Bhandari and Lahiri (n 4).

⁹ Arne Hintz, Lina Dencik and Karin Wahl-Jorgensen, 'Digital Citizenship and Surveillance Society' (2017) 11 *International Journal of Communication* 731.

¹⁰ Richards (n 5).

¹¹ Ministry of Home Affairs, 'Expression of Interest for Selection of Systems Integrators for Implementing Entity Extraction, Visualization & Analytics (EVA) System (29 October 2017) 14 <https://www.mha.gov.in/sites/default/files/EOIEVA_29092017.pdf> accessed 31 May 2022; Vrinda Bhandari, 'Facial Recognition: Why We Should Worry About the Use of Big Tech for Law Enforcement', *The Future of Democracy in the Shadow of Big and Emerging Tech* (Centre for Communication Governance, National Law University Delhi 2020) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/the-future-of-democracy-in-the-shadow-of-big-and-emerging-tech-ccg-248.pdf>> accessed 26 May 2022; Shefali Mehta and Kamlesh Shekar, 'The State of Surveillance in India: National Security at the Cost of Privacy?' (Observer Research Foundation, 17 February 2022) <<https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india/>> accessed 26 May 2022.

¹² Pranesh Prakash, 'How Surveillance Works in India' (*India Ink*, 10 July 2013) <<https://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/>> accessed 26 May 2022; 'Govt to Launch Internet Spy System "Netra" Soon' *The Times of India* (6 January 2014) <<https://timesofindia.indiatimes.com/tech-news/govt-to-launch-internet-spy-system-netra-soon/articleshow/28456222.cms>> accessed 27 March 2023. See also Minister of State in the Ministry of Home Affairs, Answer to Unstarred Question No 3493 (Lok Sabha, 11 August 2015) <<https://www.mha.gov.in/MHA1/Par2017/pdfs/par2015-pdfs/ls-110815/3493.pdf>> accessed 27 February 2023.

Although sophisticated surveillance architecture is in place and operating in India, there had been limited doctrinal engagement with these developments in the Indian context until the judgment delivered by the nine-judge bench of the Supreme Court of India in *K.S. Puttaswamy vs. Union of India*.¹³ While the case did not pertain to surveillance specifically, the Court in *Puttaswamy* unanimously reaffirmed, that the Constitution of India guarantees a fundamental right to privacy to Indian citizens.¹⁴ The Court provided a new vocabulary for thinking about the importance of privacy and the dangers presented by unchecked surveillance mechanisms.¹⁵ The Court also set out an analytical framework to evaluate the constitutionality of privacy-infringing measures by adopting the proportionality test.¹⁶

This report harnesses this new conceptualisation of the right to privacy and the analytical framework provided in *Puttaswamy* for evaluating the constitutionality of surveillance measures, and applies it to India's targeted and modern surveillance frameworks. While literature on surveillance makes a distinction between 'targeted' and 'mass' surveillance programs, given the limited information on how India's newer programs operate, this report instead characterises them as 'modern' surveillance programs. The distinction may be described as follows.

- Targeted surveillance typically begins with a reasonable suspicion regarding an identified individual(s) and involves intercepting and monitoring their (and only their) communications.
- India's modern surveillance programs on the other hand are not limited to an identified individual(s), instead they both automate interception and proactively monitor large swathes of people to identify unlawful activity and have potential mass surveillance capabilities.

Given the structural difference between the two types of surveillance programs, and the fact that India's targeted surveillance programs have a statutory basis, while its modern surveillance programs do not, this report separates its analysis of targeted and modern surveillance programs. Additionally, the statutory provisions authorising India's targeted surveillance programs have been subject to constitutional scrutiny in the past (albeit, pre-*Puttaswamy*), while modern surveillance programs represent uncharted doctrinal territory. However, there are several ongoing cases examining these programs.

¹³ (2017) 10 SCC 1.

¹⁴ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [652].

¹⁵ Bhandari and Lahiri (n 4).

¹⁶ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [325].

In the context of targeted surveillance, the present report maps out the statutory framework governing government interceptions, monitoring, and decryption, along with key judicial developments in the area. Based on the impact *Puttaswamy* has had on India's privacy doctrine, the report then examines whether past judicial findings on surveillance need to be revisited considering the decision in *Puttaswamy*. Given that there exist no judicial findings on modern surveillance programs in India, these chapters of the report directly apply the proportionality test set out in *Puttaswamy* to the limited information available regarding India's modern surveillance programs.

Finally, India has also adopted several welfare schemes and e-governance programs that involve the aggregation and analysis of individuals' data from both governmental agencies and private companies. These programs raise considerable indirect surveillance risks, as they allow for the profiling and tracking of individuals across various areas of their public and private lives. However, given that these programs do not involve primary data collection from communications, but rather raise concerns of consent and purpose limitation, the legal analysis of such schemes is better approached from the perspective of data protection and not that of surveillance. Nonetheless, given the surveillance risks these schemes raise, a summary of relevant schemes is set out as an annexure to this report.

Outline of the report

- Chapter 2 of this report traces the evolving understanding of the right to privacy and the constitutionally permissible restrictions on the right in the Indian context.
- Chapter 3 maps India's legislative framework for targeted surveillance, covering the Telegraph Act, 1885 ("**Telegraph Act**") and the telecom and internet licenses issued under the Act; the Information Technology Act, 2000 ("**IT Act**"); and surveillance under criminal laws.
- Chapter 4 analyses the potential impact of *Puttaswamy* on the constitutionality of India's statutory framework for targeted surveillance including: (i) whether the safeguards for intercepting communications set out by the Supreme Court in *PUCL vs. Union of India*¹⁷ require reconsideration in light of *Puttaswamy*; (ii) whether independent authorisation and oversight of government surveillance is now required by the proportionality standard; (iii) whether evidence obtained through unlawful or unconstitutional surveillance can be admissible in court; and (iv) whether the grounds for surveillance in the Telegraph Act and IT Act

¹⁷ (1997) 1 SCC 301.

are constitutionally compliant.

- Chapter 5 sets out India's modern surveillance programs, specifically examining the capabilities of the Central Monitoring System and the Networking Traffic Analysis software.
- Chapter 6 evaluates India's modern surveillance programs against the standards of proportionality set out in *Puttaswamy*.
- Chapter 7 concludes with some recommendations.
- The Annexure sets out India's data collection and sharing programs that are not grounded in interception and monitoring but raise surveillance risks including: (i) the National Intelligence Grid; (ii) the Crime and Criminal Tracking Network; (iii) Aadhaar; (iv) National Health Stack; (v) National E-Transport Project; (vi) Digi Yatra; and (vii) the Criminal Procedure (Identification) Act, 2022.

2. Indian privacy doctrine and surveillance

The Indian Constitution does not contain a specific or explicit provision protecting the right to privacy. Since the adoption of the constitution, the Supreme Court has vacillated on whether the Constitution includes a right to privacy, with the Court even expressly rejecting the notion of the right's constitutional status in *M.P. Sharma vs. Satish Chandra*¹⁸ and *Kharak Singh vs. State of Uttar Pradesh*.¹⁹ However, in 2017 a nine-judge bench of the Supreme Court in *Puttaswamy* reaffirmed that the right to privacy is a fundamental right guaranteed to all persons and expressly overruled *M.P. Sharma* and *Kharak Singh*.²⁰

Building on a number of national and international judgments and academic commentary on different aspects of the right to privacy, the nine-judge bench of the Court held that privacy is an inherent, inalienable natural right, grounded in the dignity, liberty, and autonomy of an individual.²¹ The Court declared the right to privacy an “intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III [fundamental rights] of the Constitution.”²²

(a) The right to privacy in *Puttaswamy*

The judgement in *Puttaswamy* consists of several concurring opinions reflecting the approach of each judge towards the right to privacy and the threats faced by it. There was consensus on the transformation of the right to privacy from a ‘property right’ to one rooted in the security of personhood, spatial control, decisional autonomy, and informational control.²³ The Court observed that privacy had transformed from merely protecting individuals against physical interference with their property (primarily covering the right against trespass) to now guarantee the

¹⁸ (1954) SCR 1077.

¹⁹ (1964) 1 SCR 332.

²⁰ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [652].

²¹ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [102]–[118], [320] (Chandrachud J).

²² *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [652].

²³ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [652]. See also Gautam Bhatia, ‘The Supreme Court’s Right to Privacy Judgment – I: Foundations’ (*Indian Constitutional Law and Philosophy*, 27 August 2017) <<https://indconlawphil.wordpress.com/2017/08/27/the-supreme-courts-right-to-privacy-judgment-i-foundations/>> accessed 27 May 2022.

“physical and psychological integrity” of a person (e.g. safety from illegal search and seizure)²⁴, and their decisional, informational, and behavioural autonomy.²⁵

The Court in *Puttaswamy* acknowledged that informational privacy included an “interest in preventing information about the self from being disseminated and controlling the extent of access to information”, while noting that privacy enabled an individual to “restrict access to communications or control the use of information which is communicated to third parties.”²⁶ This rich conceptualisation of privacy in *Puttaswamy* also laid the groundwork for a new understanding of the harms of surveillance, particularly in the digital era.

Justice Kaul’s concurring opinion from *Puttaswamy* is notable for its elaborate discussion on the impact of technology on modern State surveillance, the deep digital footprints left by citizens online, and how ‘profiling’ can invade individual privacy.²⁷ Justice Kaul noted that while profiling can be used to further public interest and enhance national security, it can also result in discrimination based on religion, gender or caste.²⁸ Justice Kaul also raised concerns about how State possession and control over personal data can enable the creation of a ‘Big Brother’ State, that exercises excessive control over its citizens, which can in turn affect other rights such as freedom of expression.²⁹ Thus, he urged the State to ensure that surveillance technologies are balanced against the right to privacy.³⁰

(b) Surveillance as a restriction on constitutional rights

Surveillance, *per se*, infringes fundamental rights, including the right to privacy, guaranteed under the Constitution. The right to privacy has two kinds of interest inscribed in it: (i) an interest in avoiding disclosure of personal matters (e.g., disclosure of personal data about their health), and (ii), an interest in the independence to make certain kinds of important decisions (e.g. engaging in lawful but unpopular behaviour).³¹ Surveillance threatens both of these interests.

²⁴ Roger JR Levesque, ‘Spatial Privacy’, *Adolescence, Privacy, and the Law* (Oxford University Press 2016).

²⁵ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [248]–[250]. See also Bhairav Acharya, ‘The Four Parts of Privacy in India’ (2015) 50 *Economic and Political Weekly* 7.

²⁶ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [250] (Chandrachud J).

²⁷ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [585]–[586] (Kaul J).

²⁸ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [585] (Kaul J).

²⁹ *K S Puttaswamy v Union of India* (2017) (2017) 10 SCC 1 [585]–[586] (Kaul J).

³⁰ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [585]–[586] (Kaul J).

³¹ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [518] (Nariman J) citing *Whalen v Roe* 429 US 589 (1977) (U.S. Supreme Court).

Even the mere apprehension of surveillance may interfere with the second interest (decisional autonomy) by inhibiting individuals from taking decisions they might otherwise take. Given that surveillance is usually carried out in secret, the apprehension of surveillance has a chilling effect on an individual's ability to speak and move freely, to meet others, her intellectual privacy, and may cause a stifling of dissent and self-censorship.³² As free speech protects the right of the individual to speak freely without fear, secret or unforeseeable State surveillance constitutes an interference not only with the right to privacy, but also the right to free speech and free association.³³

The chilling effect of surveillance is well-recognised. In *NAACP vs. Alabama*,³⁴ the U.S. Supreme Court struck down the compelled disclosure of the membership lists of a civil rights organisation (the National Association for the Advancement of Colored People), noting that the mere knowledge of surveillance would force politically unpopular or dissident individuals and groups into self-censorship. This reasoning has also been recognised by Indian courts. As Subba Rao J. noted in his dissent in *Kharak Singh* – which is now good law after being approved in *Puttaswamy* – surveillance places ‘psychological restraints’ that condition our minds and introduce inhibitions that are akin to physical restraints.³⁵

Surveillance, when viewed as control over the body of an individual, can also be experienced as a violation of their bodily integrity and mental privacy, that hinders the autonomous management of their bodies and their selves.³⁶ Feminists have long argued that data must be seen as being inextricably linked to our bodies, and not as something external to ourselves.³⁷ Control over one's body, especially for women, is essential to retaining their autonomy, their decision-making ability, and

³² Richards (n 5); Jillian York, ‘The Harms of Surveillance to Privacy, Expression and Association’ (Electronic Frontier Foundation 2014) <<https://giswatch.org/thematic-report/internet-rights/harms-surveillance-privacy-expression-and-association>> accessed 26 May 2022.

³³ *Weber and Saravia v Germany* App No 54934/00 (ECtHR, 29 June 2006); Gautam Bhatia, ‘Free Speech and Surveillance’ (Centre for Internet and Society, 7 July 2014) <<https://cis-india.org/internet-governance/blog/free-speech-and-surveillance>> accessed 31 January 2023.

³⁴ 357 US 449 (1958) (U.S. Supreme Court).

³⁵ *Kharak Singh v State of Uttar Pradesh* (1964) 1 SCR 332.

³⁶ Sukanya Shantha, ‘Presence of Over 60 Women in Leaked List Highlights “Bodily Violation” Posed by Spyware’ *The Wire* (24 July 2021) <<https://thewire.in/women/pegasus-project-women-surveillance>> accessed 26 May 2022.

³⁷ Anja Kovacs, ‘When Our Bodies Become Data, Where Does That Leave Us?’ (*Deep Dives*, 8 June 2020) <<https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969>> accessed 26 May 2022.

hence, their privacy.³⁸

(c) Assessing the constitutionality of surveillance measures

Fundamental rights in India, including the right to privacy, are not absolute and can be restricted if such restrictions are just, fair, and reasonable.³⁹ As we noted in the previous section, surveillance *per se* impinges on the fundamental rights of citizens and thus must be operationalised and implemented subject to constitutional constraints. Therefore, the central legal question is how to assess when such restrictions are unconstitutional? In addition to its articulation of the right to privacy, *Puttaswamy* also crystallised the proportionality test, to evaluate the constitutionality of a particular State measure that restricts fundamental rights.⁴⁰

The plurality opinion in *Puttaswamy*, authored by Chandrachud J., clarified that all actions which interfere with the right to privacy have to meet the criteria of legality, legitimacy of objectives, and proportionality.⁴¹ In his concurring opinion, Kaul J. fleshed out this test further, setting out a four-part test to determine when a measure is constitutional: (i) the measure must be sanctioned by law; (ii) the measure must be necessary in a democratic society for a legitimate aim; (iii) the extent of interference with a right must be proportionate to the need for such interference; and (iv) there must be procedural guarantees against abuse of interference.⁴²

The following criteria thus emerge to evaluate the constitutionality of a surveillance measure:⁴³

- i. *Legality*: there must be a law authorising the interference with an individual's right. Thus, all surveillance measures and systems must be

³⁸ Ramya Chandrasekhar, 'Here Are the Consequences of Linking Women's Medical Records to Their Aadhaar' (*The Indian Express*, 24 April 2018) <<https://indianexpress.com/article/gender/here-are-the-consequences-of-linking-womens-medical-records-to-their-aadhaar-5139360/>> accessed 26 May 2022.

³⁹ *K S Puttaswamy v Union of India* (2017) 10 SCC 1; *Maneka Gandhi v Union of India*, AIR 1978 SC 597.

⁴⁰ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [325] (Chandrachud J), [638] (Kaul J).

⁴¹ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [325] (Chandrachud J).

⁴² *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [638] (Kaul J).

⁴³ Bhandari and Lahiri (n 4).

backed by law.⁴⁴

Legitimacy, suitability, and necessity: the measure must pursue a legitimate State aim and be necessary in a democratic society.⁴⁵ This latter limb involves evaluating whether: (a) the measure has a rational nexus with the State's legitimate aim (i.e., to what extent does the measure advance the State's intended aim); and (b) the measure has the minimal possible impact on rights.⁴⁶

- ii. *Proportionate*: the extent of interference with the fundamental right must be proportionate to the need for such interference.
- iii. *Procedural safeguards*: the law must contain procedural guarantees to prevent abuse.⁴⁷

In 2019, a Constitution Bench of the Supreme Court (5 judges) evaluated the constitutionality of the Indian Government's Aadhaar welfare scheme in *K.S. Puttaswamy II vs. Union of India* ("**Aadhaar Judgement**").⁴⁸ The scheme involved the creation of a centralised database consisting of sensitive biometric data of every resident, paired with an Aadhaar number.⁴⁹ While the Court upheld the State's measure, the resulting judgement provided additional specificity on the analysis required to be conducted under *Puttaswamy*'s proportionality standard; requiring every rights-infringing measure to satisfy the following test:⁵⁰

- i. *Legality*: the measure must be sanctioned by statute.
- ii. *Legitimate goal*: the measure must have a legitimate aim or proper purpose.

⁴⁴ *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [109]-[121]; *Bachan Singh v State of Punjab* (1980) 2 SCC 684. In the Indian context, "law" under Art. 21 has been interpreted to mean a "valid" law, that is, more than just the procedure laid down by the law. It also needs to be "fair, just and reasonable." International human rights jurisprudence incorporates further requirements within 'legality'; such as the law also needing to be fair, accessible, clear, and having independent oversight mechanisms.

⁴⁵ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [325] (Chandrachud J), [638] (Kaul J).

⁴⁶ Bhandari and Lahiri (n 4).

⁴⁷ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [638] (Kaul J).

⁴⁸ 2019 1 SCC 1.

⁴⁹ Planning Commission, 'UIDAI Strategy Overview: Creating a Unique Identity Number for Every Resident in India' (2010) <https://prsindia.org/files/bills_acts/bills_parliament/2010/UIDAI_STRATEGY_OVERVIEW.pdf> accessed 26 May 2022; Jean Dreze, 'All That Data That Aadhaar Captures' *The Hindu* (8 September 2017) <<https://www.thehindu.com/opinion/lead/all-that-data-that-aadhaar-captures/article19646150.ece>> accessed 26 May 2022.

⁵⁰ *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [148], [157]-[158].

- iii. *Suitability*: the measure must be a suitable means of achieving the legitimate aim (i.e., the State's measure must bear a rational connection to the legitimate aim sought to be achieved).
- iv. *Necessity*: the measure must be the least rights-restrictive option amongst equally effective alternatives. The majority adopted David Bilchitz's⁵¹ formulation for applying this standard, requiring the court to:
 - a) identify the range of possible alternative measures that the government could adopt;
 - b) determine the effectiveness of each alternative measures to evaluate if they achieve the stated aim in a 'real and substantial manner';
 - c) determine the impact of the measures on the concerned right; and
 - d) make an overall judgement on whether the rights are adequately balanced, and if there is a preferable alternative to the government's choice.
- v. *Balancing*: the measure must not have a disproportionate impact on the rights holders.

Thus, Indian Supreme Court doctrine provides clear legal standards that every rights-infringing surveillance measure must satisfy. However, the application of these standards is often not rigorous in practice.⁵² For example, in the *Aadhaar Judgment* itself, the majority and minority subjected the facts of the case to the same proportionality test and arrived at contrasting outcomes on the constitutionality of the measure.⁵³

Through a study of cases between 2004 to 2016, Aparna Chandra found that the Supreme Court rarely, if ever, engaged in the 'necessity' analysis or considered

⁵¹ David Bilchitz, 'Necessity and Proportionality: Towards a Balanced Approach?' in Liora Lazarus, Christopher McCrudden and Nigel Bowles (eds), *Reasoning Rights: Comparative Judicial Engagement* (Hart Publishing 2014).

⁵² Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere?' (2020) 3 *University of Oxford Human Rights Hub Journal* 55.

⁵³ *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [1343]-[1367], [1382]-[1383], [1539]. Chandrachud J wrote a dissenting opinion which agreed that proportionality was the appropriate standard of review but differed from the majority in his application of the test. Unlike the majority, Chandrachud J. found that data collected under Aadhaar could in fact be used to profile and surveil individuals, and that there did exist less intrusive alternative means to achieve the aim of delivering state benefits.

alternative, less rights-infringing measure the government could have pursued.⁵⁴ It broadly adopted an approach deferential to the State, both on the substantive thresholds and the evidentiary burdens to be satisfied, in assessing the rights-infringing measures.⁵⁵ Nevertheless, these judgments are significant as they provide a concrete analytical framework to evaluate India's existing surveillance architecture.

⁵⁴ Aparna Chandra, 'Limitation Analysis by the Indian Supreme Court' in Andrej Lang, Mordechai Kremnitzer and Talya Steiner (eds), *Proportionality in Action: Comparative and Empirical Perspectives on the Judicial Practice* (Cambridge University Press 2020).

⁵⁵ *ibid*; Chandra (n 52).

3. India's legislative framework for targeted surveillance

Before we can evaluate India's surveillance frameworks against the legal standards set out in *Puttaswamy*, it is necessary to map India's legislative and executive framework that governs targeted surveillance. The legislative framework governing targeted surveillance in India consists primarily of the Telegraph Act and IT Act, and their accompanying Rules.

Telecom service providers (“**TSPs**”) and internet service providers (“**ISPs**”) require a license issued by the Union Government to operate in India.⁵⁶ As discussed below, these licenses require TSPs and ISPs to cooperate with law enforcement agencies to operationalise surveillance. Thus, in addition to the statutory frameworks of the Telegraph and IT Acts, the licenses issued to TSPs and ISPs form essential elements of the surveillance architecture in the country.

Finally, Indian criminal law, including the Code of Criminal Procedure, 1973, the Indian Evidence Act, 1872 and specific organised crime and anti-terror statutes also authorise surveillance, and govern the conduct of investigative agencies during criminal investigations to varying degrees, including the crucial issue of admissibility of intercepted communications as evidence at trial.

(a) Interception under the Telegraph Act, 1885

The Telegraph Act is a colonial law that deals with the establishment, conduct, and licensing of telegraphs, and authorises the government to set up telegraph lines.⁵⁷ The definition of ‘telegraph’ is extremely broad, covering both wired and wireless communication, and bringing in virtually any kind of communication device within its ambit.⁵⁸ Due to its broad definition, the word ‘telegraph’ has the ability to include newer forms of technology and communication devices, such as telephones

⁵⁶ The Indian Telegraph Act, 1885, s. 4

⁵⁷ The Indian Telegraph Act, 1885, s. 4

⁵⁸ Indian Telegraph Act, 1885 s. 3(1AA). “telegraph” means any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means. Explanation. “Radio waves” or “Hertzian waves” means electro-magnetic waves of frequencies lower than 3,000 giga-cycles per second propagated in space without artificial guide.

and wireless mobile phones.⁵⁹

In 2022, the Union Government released draft legislation intended to eventually replace the Telegraph Act. The draft, titled the “Indian Communication Bill, 2022” defined “telecommunication services” as services which are made available to users by telecommunication, including “*broadcasting services, electronic mail, voice mail, voice, video and data communication services ... fixed and mobile services, internet and broadband services, satellite based communication services, internet based communication services ... interpersonal communication services, machine to machine communication services, over-the-top (OTT) communication services*.”⁶⁰

Given this broad definition, and the fact that the Bill also authorises interception on “telecommunication services”,⁶¹ the Bill may have substantial implications for the types of information that could be collected under the new legislation. However, at the time of writing this report, the Union Government is still soliciting feedback on the draft legislation. It is also relevant to note that the *standards* for interception (i.e., when interception is permitted) in the new Bill are analogous to the standards provided in the Telegraph Act, making an analysis of the Telegraph Act of continued relevance.

(i) Substantive standard for interception

Section 5(1) of the Telegraph Act empowers the Union and state governments to take temporary possession of licensed telegraphs. Section 5(2) empowers the Union and state governments to order the interception or detention of messages, to direct that the messages shall not be transmitted, or that messages shall be disclosed to the government. However, the exercise of this power is subject to two substantive conditions:

(1) the occurrence of a “public emergency” OR the interception is “in the interest of public safety”;

AND

(2) the interception is “necessary or expedient” in the interests of the “sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence”

⁵⁹ *Senior Electric Inspector v Laxminarayan Chopra* (1962) 3 SCR 146 [7].

⁶⁰ ‘Draft Indian Telecommunications Bill’ (Department of Telecommunications 2022) <<https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf>>. See Clause 2(1)(21).

⁶¹ *ibid.*

An interception order under Section 5(2) of the Telegraph Act should be in writing with reasons.⁶² However, once an interception order is passed, the power under the provision is wide; any message or class of messages to or from any person or class of persons, or relating to any particular subject can be intercepted and disclosed to the concerned authorities.⁶³ These messages may have been scheduled to be transmitted, being transmitted, or already received.⁶⁴ Thus, understanding the substantive standard for when interception powers may be invoked is crucial.

Public emergency and public safety

The Supreme Court of India has interpreted the terms “public emergency” and “in the interest of public safety” to mean situations that are not secretive but are apparent to a reasonable person; and that raise problems concerning the sovereignty, security, or integrity of India, its friendly relations with foreign States, public order, or the prevention of incitement of an offence.⁶⁵ In 1997, when the constitutionality of Section 5(2) of the Telegraph Act was challenged in *PUCL vs. Union of India*, the Supreme Court expressly observed:

*Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression ‘public safety’ means the state or condition of freedom from danger or risk for the people at large... Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a reasonable person.*⁶⁶

Thus, interception powers under Section 5(2) of the Telegraph Act are not meant to be exercised routinely, simply for the investigation or prevention of a crime. Governments should satisfy themselves about the existence of danger or risk to the public, or a situation where imminent action is necessary. The pre-condition of ‘public emergency’ and ‘public safety’ creates a high threshold for the government to satisfy before it may consider curtailing fundamental rights by intercepting communications.

⁶² The Indian Telegraph Act, 1885, s. 5(2).

⁶³ The Indian Telegraph Act, 1885, s. 5(2). The proviso to s. 5(2) provides that messages of accredited government press correspondents intended to be published in India shall not be intercepted or detained unless their transmission has been prohibited under the section.

⁶⁴ The Indian Telegraph Act, 1885, s. 5(2).

⁶⁵ *Hukam Chand v Union of India* AIR 1976 SC 789 [13].

⁶⁶ *PUCL v Union of India* (1997) 1 SCC 301 [28].

How this high threshold may apply in practice was demonstrated by the High Court of Bombay in *Vinit Kumar vs. Central Bureau of Investigation*. In this case, the Central Bureau of Investigation (“CBI”) intercepted conversations from the petitioner’s phone as part of an investigation regarding the bribing of a public servant. The orders of interception were issued on the grounds of ‘public safety’.

Applying the Supreme Court’s ruling in *PUCL*, the High Court observed that an order based on the ground of ‘public safety’ would have to relate to “*danger or risk for the people at large.*”⁶⁷ The High Court ruled that the charge-sheet submitted by the CBI failed to demonstrate any threat to public safety.⁶⁸ Given that the grounds of public emergency or public safety are essential pre-conditions for the invocation of interception powers under Section 5(2) of the Telegraph Act, and these pre-condition had not been fulfilled, the Court quashed the interception order and directed the destruction of the intercepted messages.⁶⁹

Necessary and expedient

Section 5(2) additionally requires that the interception be “necessary or expedient” in the interests of the sovereignty, security, or integrity of India, its friendly relations with foreign States, public order, or the prevention of incitement of an offence.⁷⁰ The Supreme Court has provided valuable clarity on how the terms security of the State, public order, and incitement are to be interpreted. The Court has clarified that public order does not mean a simple law and order situation.⁷¹ In *Ramlila Maidan vs. Secretary*, the Court held that ‘public order’ was “*an aggravated form of disturbance of public peace which affects the general course of public life*” as distinguished from ‘law and order’ which may include “*any act which merely affects the security of others.*”⁷²

The Court further contrasted the term ‘public order’ with the terms ‘law and order’ and ‘security of the state’. It held that while all three terms fall within the ambit of ‘social order’, the interests of the ‘security of the State’, ‘public order’, and ‘law and order’ form three concentric circles with ‘law and order’ being the outermost and most inclusive circle.⁷³ Thus, “*an activity which could affect ‘law and order’ may not*

⁶⁷ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [17].

⁶⁸ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [19].

⁶⁹ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [19].

⁷⁰ The Indian Telegraph Act, 1885, s. 5(2).

⁷¹ See *Ram Manohar Lohia v State of Bihar* (1966) 1 SCR 709; *Ramlila Maidan v Secretary* (2012) 5 SCC 1.

⁷² *Ramlila Maidan v Secretary* (2012) 5 SCC 1.

⁷³ See *Ram Manohar Lohia v State of Bihar* (1966) 1 SCR 709; *Ramlila Maidan v Secretary* (2012) 5 SCC 1.

*necessarily affect public order and an activity which might be prejudicial to public order, may not necessarily affect the security of the State.*⁷⁴

Lastly, it is relevant to note that when interpreting the term “incitement” in the context of rights-restricting measures, the Supreme Court has repeatedly read in a requirement of imminence and proximity, requiring a strong and close connection between the individual’s conduct and the risk of the offence in question.⁷⁵

(ii) Procedural framework for interception

As noted above, the constitutionality of Section 5(2) of the Telegraph Act was challenged in *PUCL* as violating the fundamental rights to free speech, privacy, and personal liberty under Articles 19(1)(a) and 21.⁷⁶ The petition was filed in light of a report documenting the tapping of politicians’ phones, which highlighted concerns about phone tapping on the basis of oral requests, tapping for beyond 180 days without any permission, the failure of TSPs to maintain proper records for the authorisation of interception, and the non-disclosure of telephone numbers that were under interception. At the time, no rules had been framed on the procedure for the interception of messages.

The petitioners argued that Section 5(2) facilitated telephonic interception without any due process guarantees, and thus the power to intercept communications was unbridled and unconstitutional. The petitioners sought to have Section 5(2) declared unconstitutional or ‘read down’ to include mandatory procedural safeguards to regulate the exercise of interception.

In *PUCL* the Supreme Court acknowledged that telephone tapping was a serious invasion of the right to privacy and that privacy was a fundamental right under Article 21 of the Constitution. However, rather than strike down Section 5(2), the Court laid down guidelines that formed procedural safeguards to adequately balance the State’s intelligence gathering with the invasion of privacy caused by telephone tapping.⁷⁷ These guidelines were largely codified in 1999 by the Union Government when it added Rule 419A to the Indian Telegraph Rules (“**Telegraph Rules**”).⁷⁸ (Rule 419A was subsequently amended in 2007 and 2014.) Rule 419A

⁷⁴ *Ramlila Maidan v Secretary* (2012) 5 SCC 1.

⁷⁵ *The Superintendent, Central Prison, Fatehgarh v Dr. Ram Manohar Lohia*, 1960 (2) SCR 821; *Arup Bhuyan v State of Assam* 2011 (3) SCC 377; *Shreya Singhal v Union of India* 2015 (5) SCC 1.

⁷⁶ *PUCL v Union of India* (1997) 1 SCC 301 [2].

⁷⁷ *PUCL v Union of India* (1997) 1 SCC 301 [34].

⁷⁸ Indian Telegraph Act, 1885, s. 7 pertains to rule-making powers of the Union Government. s. 7(2) (b) empowers the Government to make rules on the precautions to be taken for preventing improper interception or disclosure of messages.

prescribes the procedure for interception and is discussed below.

It is important to note, however, that although the petitioners argued that prior judicial scrutiny or a judicial warrant should be required before passing an interception order under Section 5(2), the Court rejected this argument. It agreed with the amicus and the government's contention that since prior judicial oversight of surveillance action was not envisaged in the Telegraph Act, it could not read in such a requirement. It also drew support from the fact that the then equivalent legislation in the United Kingdom, the Interception of Communications Act, 1985, also did not require a judicial warrant to carry out interception. However, courts can still exercise their power of judicial review *post facto*, to determine whether the procedure for interception was just, fair, and reasonable; and complied with Section 5(2) of the Telegraph Act and Rule 419A of the Telegraph Rules.⁷⁹

Procedure for interception under the Telegraph Act

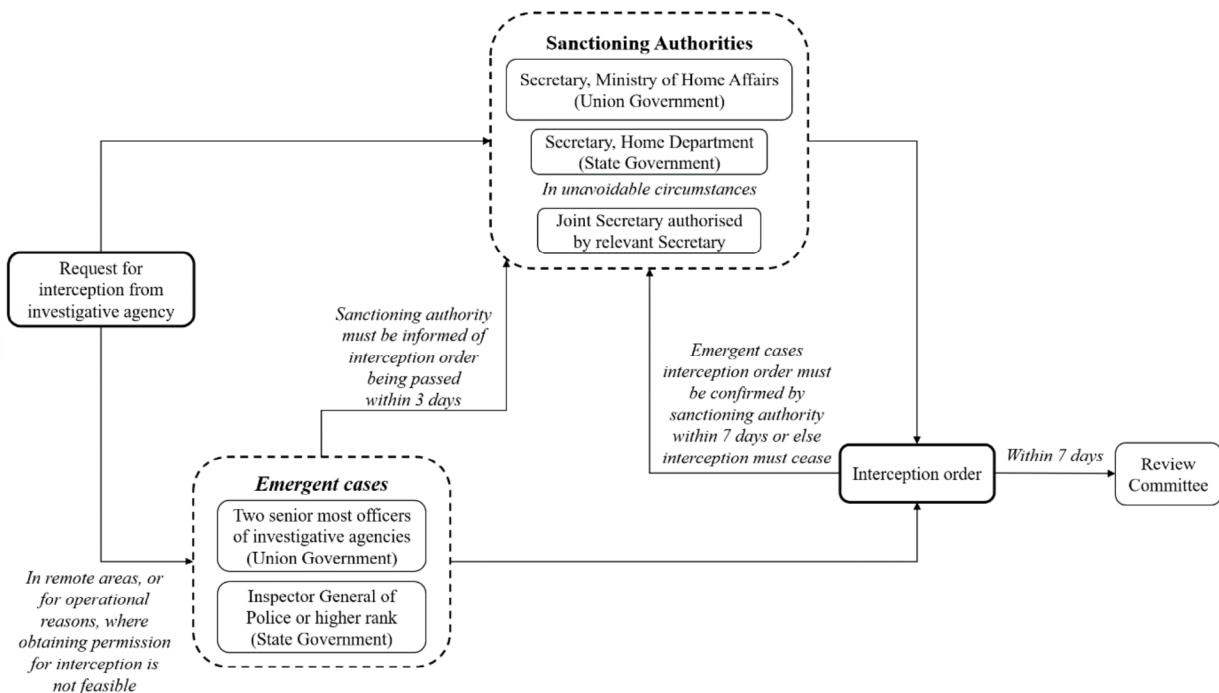
Rule 419A provides that the order for interception shall, in the ordinary course, only be issued by the 'competent authority'. This is the Secretary to the Ministry of Home Affairs at the Union level, and the Secretary to the Home Department in cases of the state government.⁸⁰ In unavoidable circumstances or emergent cases, these powers can be exercised by more junior level officers, or the heads of the concerned investigative agencies or police, subject to certain conditions.⁸¹ Where an interception order is passed by a member of the police or investigative agency, the Secretary, Ministry of Home Affairs (for the Union Government) or the Secretary, Home Department (for the State Government), as competent authorities, must be informed of the interception within three days and must confirm the interception order within seven days.⁸² If the interception order is not confirmed, Rule 419A(1) stipulates that the interception shall cease, but does not state that the interception order is *void ab-initio* or that the intercepted material must be destroyed. The flow chart below depicts the procedure to procure a lawful interception order.

⁷⁹ *State of Maharashtra v Bharat Shanti Lal Shah* (2008) 13 SCC 5 [60]; *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [20].

⁸⁰ Indian Telegraph Rules, 1951, r. 419A(1).

⁸¹ Indian Telegraph Rules, 1951, r. 419A(1).

⁸² Indian Telegraph Rules, 1951, r. 419A(1).



The interception order issued under Section 5(2) must be in writing, and must document the reasons for interception.⁸³ While issuing an interception order, the officer has to consider the possibility of acquiring the information through other means, and an order should only be passed when it is not possible to acquire the information through any other reasonable means.⁸⁴ The order must specify that the use of the intercepted messages is subject to Section 5(2) of the Telegraph Act.⁸⁵ Once issued, an order will remain valid for a period of 60 days unless revoked earlier, and can be renewed for a maximum period of 180 days.⁸⁶

Notably, records of the interception directions and the intercepted messages have to be destroyed by the competent authority and the investigative agencies every six months, unless retained for ‘functional requirements’.⁸⁷ Similarly, service providers are also obligated to maintain ‘extreme secrecy’ and destroy records pertaining to the direction for interception within two months of the stoppage of the same.⁸⁸ These confidentiality requirements ensure that the nature of

⁸³ Indian Telegraph Act, 1885, s. 5(2); Indian Telegraph Rules, 1951, r. 419A(2).

⁸⁴ Indian Telegraph Rules, 1951, r. 419A(3).

⁸⁵ Indian Telegraph Rules, 1951, r. 419A(5).

⁸⁶ Indian Telegraph Rules, 1951, r. 419A(6).

⁸⁷ Indian Telegraph Rules, 1951, r. 419A(18).

⁸⁸ Indian Telegraph Rules, 1951, r. 419A(19).

surveillance remains secret, even after the fact.

Interception orders must also be forwarded to the three-member Review Committee (consisting entirely of senior government officials from the executive) within seven working days.⁸⁹ At the Union level, the Review Committee comprises the Cabinet Secretary (as the Chairperson), the Law Secretary, and the Secretary to the Department of Telecommunications. The Review Committee at the state level is comprised of equivalent officers.⁹⁰

The Committee must meet at least once in two months and record its findings on the validity of interception orders and compliance with the parameters of Section 5(2) of the Telegraph Act. If it finds that the interception directions are not in consonance with the requirements of Section 5(2), it may set aside the orders or order the destruction of the data already intercepted.⁹¹

Call data not interception

Authorities, government agencies, or statutory regulators not mentioned in Rule 419A *cannot* be authorised by the Union Government under Section 5(2) to intercept or prohibit the sending of calls or messages. State police also cannot exercise interception powers under the Telegraph Act. However, the provision does not prevent regulators such as the Securities and Exchange Board of India (“SEBI”) from requisitioning static information such as call detail records (“CDRs”) and other details such as tower location from TSPs – since they do not relate to the *interception* of messages.

In *Indian Council of Investors vs. Union of India*, the Bombay High Court clarified that apart from its powers under the SEBI Act and Securities Law (Amendment) Ordinances (issued in 2013 and 2014) that permitted SEBI to call for CDRs, “*the calling of static information like CDRs from a TSP does not in any manner violate Section 5(2) of the Indian Telegraph Act, 1885.*”⁹² To prevent the abuse of this power, the Bombay High Court laid down safeguards to regulate the exercise of such powers by SEBI, such as requiring the requisitioning of CDRs and tower location information be done in accordance with law, as such requests constituted

⁸⁹ Indian Telegraph Rules, 1951, r. 419A(2).

⁹⁰ Indian Telegraph Rules, 1951, r. 419A(16).

⁹¹ Indian Telegraph Rules, 1951, r. 419A(17).

⁹² *Indian Council of Investors v Union of India* (2014) SCC Online Bom 4767 [23].

infringements on a subscriber's right to privacy.⁹³

While this decision applies to SEBI, it is important to note that state police can still request CDRs of investigative targets under Section 91 of the Code of Criminal Procedure, 1973 whenever it is “necessary or desirable”.⁹⁴ Section 91 gives the police wide powers, and is examined in detail below.

(b) Duty of telecom service providers

As discussed above, to operate in India, a TSP or ISP must obtain a license from the Union Government.⁹⁵ The Department of Telecommunications, India's government department for telecom regulation, enters into license agreements with service providers to enable them to operate in India. These Unified License Agreements (“UL”) impose obligations on the service providers, including enabling State surveillance of communication by disclosing content and metadata of communication, providing access to CDRs, and the location of target subscribers.⁹⁶

Thus, while the Telegraph Act and IT Act set out how and when surveillance can take place, the licensing regime under the Telegraph Act dictates how surveillance is *operationalised*, by setting out the obligations on service providers to create and operate the techno-legal infrastructure for surveillance.

(i) Unified License framework

Authorisation under the UL can be for any one of several services, including Unified License (all services); Access Service (including specific service areas); Internet Service (divided further into Category A, with all India jurisdiction, and Categories B and C in service areas and secondary switching areas); and National and International Long-Distance Service.⁹⁷

The licensor is the President of India acting through the Department of

⁹³ *Indian Council of Investors v Union of India* (2014) SCC Online Bom 4767 [24].

⁹⁴ Arnabjit Sur, ‘Using Call Detail Records to Track down Criminals’ *The Hindu* (3 July 2022) <<https://www.thehindu.com/news/cities/Delhi/how-police-are-using-cdr-to-track-down-criminals/article65596488.ece>> accessed 5 February 2023. s. 91 CrPC empowers any officer in charge of a police station to compel the production of “any document or other thing” when “necessary or desirable” for the purposes of an investigation.

⁹⁵ Indian Telegraph Act, 1885, s. 4(2).

⁹⁶ Vipul Kharbanda, ‘Policy Paper on Surveillance in India’ (*The Centre for Internet and Society*, 3 August 2015) <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india#_ftnref121> accessed 26 May 2022.

⁹⁷ ‘Unified License’ (Department of Telecommunications | Ministry of Communication | Government of India) <<https://dot.gov.in/unified-license>> accessed 31 May 2022.

Telecommunication, and the licensee is the service provider (e.g. an ISP or a TSP). The license is valid for a period of twenty years, and is governed by the Telegraph Act, Wireless Telegraphy Act, Telecom Regulatory Authority of India Act, and the IT Act.

The UL facilitates State surveillance through various contractual obligations imposed on ISPs and TSPs. First, service providers have to set up requisite monitoring and interception facilities and equipment, at their own cost, for each type of service.⁹⁸ In the same vein, licensees must ensure that the necessary hardware and software is available in their equipment to undertake lawful interception and monitoring from a centralised location.⁹⁹ For monitoring traffic, the licensees must also provide the security agencies access to their network and other facilities as well as to books of accounts.¹⁰⁰

Once operational, service providers must provide the necessary facilities to enable interception under Section 5(2) of the Telegraph Act.¹⁰¹ Service providers must also be able to trace “*nuisance, obnoxious or malicious calls, messages or communications*” on its network at the behest of the State, for the investigation or detection of crime or in the interest of national security.¹⁰²

All service providers must provide traceable identity information of their subscribers.¹⁰³ However, in case of providing service to roaming subscribers of foreign companies, the Indian company shall endeavour to obtain traceable identity of roaming subscribers from the foreign company as a part of its roaming agreement.¹⁰⁴ In the same vein, all service providers must be able to provide geographical location of any subscriber (base station location and location details including latitude & longitude details) at a given point of time.¹⁰⁵

Service providers are also required to provide the necessary facilities to the government to counteract espionage, subversive acts, sabotage, or any other unlawful activity.¹⁰⁶ Service providers are prohibited from employing bulk

⁹⁸ Department of Telecommunications, “License Agreement for Unified License” <https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf> accessed on 30 May 2022 [“**Unified License Agreement**”], Clause 23.2.

⁹⁹ Unified License Agreement, Clause 39.23 (xvi).

¹⁰⁰ Unified License Agreement, 39.23(xx).

¹⁰¹ Unified License Agreement, Clause 40.2.

¹⁰² Unified License Agreement, Clause 38.2.

¹⁰³ Unified License Agreement, Clause 39.23 (ix).

¹⁰⁴ Unified License Agreement, Clause 39.23 (ix).

¹⁰⁵ Unified License Agreement, Clause 39.23 (x).

¹⁰⁶ Unified License Agreement, Clause 39.1.

encryption equipment on their network, and the government may evaluate any encryption equipment connected to the network.¹⁰⁷ However, the service providers must also ensure the privacy of communications, and ensure unauthorised interception of messages does not take place.¹⁰⁸

ISP licenses

ISP licenses are granted as a subset of the broader ULs. In addition to the general obligations specified above, ISPs must maintain lawful interception and monitoring systems for internet traffic through their Internet gateways or Internet nodes, based on the requirements of investigative agencies, including Internet telephony traffic.¹⁰⁹ These systems can be set up at a central location at the ISP's premises, or at specific nodes or points of presence.¹¹⁰ Further, all licensees also have to maintain copies of all the packets originating from or terminating into 'Customer Premises Equipment' (instruments such as modems located on the customer's property) for the purpose of interception and monitoring of traffic, and these packets must be made available to the government and investigative agencies.¹¹¹

Access service licenses

Access licenses are also granted as a subset of the broader UL for providing access services, covering the transmission of voice and non-voice messages over the licensee's designated network. In addition to the general obligations of the UL mentioned above, licensees providing access services have to maintain and furnish all call-related information, including mobile numbers (even when a subscriber is roaming); time, date and duration of interception; location of target subscribers; telephone numbers (if call forwarding features have been invoked); data records for failed call attempts; and CDRs of a roaming subscriber, along with the monitored call, as and when required.¹¹²

Moreover, since the State has the right to monitor the telecommunications traffic at any point in the network of the TSP where it is technically feasible, the provider must undertake the installation, use, and maintenance of the monitoring equipment, often at its own cost. The service provider must ensure suitable redundancy facilities in the complete chain of monitoring equipment for trouble-

¹⁰⁷ Unified License Agreement, Clause 37.1.

¹⁰⁸ Unified License Agreement, Clause 37.1-37.2.

¹⁰⁹ Unified License Agreement, Clause 8.1.1, Chapter IX (ISP License).

¹¹⁰ Unified License Agreement, Clause 8.4, Chapter IX (ISP License).

¹¹¹ Unified License Agreement, Clause 7.3, Chapter IX.

¹¹² Unified License Agreement, Clause 8.3, Chapter VIII (Access Services).

free operations of monitoring of at least 480 simultaneous calls, with at least thirty simultaneous calls for any authorised law enforcement agency.¹¹³

(ii) Prevention of unauthorised surveillance

When an interception order is issued, the order is communicated to the relevant service provider who has been granted a license under the Telegraph Act. The Telegraph Rules require licensed service providers to put in place ‘adequate and effective internal checks’ to ensure unauthorised interception does not take place and protect the privacy of the persons whose messages are intercepted.¹¹⁴ Service providers must designate two nodal officers in every area, state, and union territory to handle requests for interception.¹¹⁵

In 2011, the Supreme Court in *Amar Singh vs. Union of India* faced a dispute where the interception orders received by the TSPs were later found to be falsified and not from the government authorities. The Court ruled that service providers should immediately act on interception order, but to prevent unauthorised interception must also “*simultaneously verify the authenticity of the same from the author of the document.*”¹¹⁶

The Court opined that TSPs and ISPs provided functions of a ‘public nature’ and thus, it was “*inherent in its duty to act carefully and with a sense of responsibility.*”¹¹⁷ The Court found that the communication sent to the TSP had many errors and mistakes and could not have seemed like a genuine official communication to any reasonable person. Thus, it held that the service provider failed in its duty to verify the authenticity of such communication.

The Court in *Amar Singh* also directed the Union Government to frame statutory guidelines to prevent unauthorised interception.¹¹⁸ In 2014, the government amended Rule 419A of the Telegraph Rules to include some safeguards against unauthorised interception.¹¹⁹ The amended Rule 419A requires an officer to deliver a written requisition to the service providers ‘by secure electronic communication’¹²⁰ and every fifteen days, the service providers must forward a list of authorisation orders received to the issuing authorities to confirm their

¹¹³ Unified License Agreement, Clause 8.2, Chapter VIII (Access Services).

¹¹⁴ Indian Telegraph Rules, 1951, r. 419A(14).

¹¹⁵ Indian Telegraph Rules, 1951, r. 419A(10).

¹¹⁶ *Amar Singh v Union of India* (2011) 7 SCC 69 [39]-[42].

¹¹⁷ *Amar Singh v Union of India* (2011) 7 SCC 69 [42].

¹¹⁸ *Amar Singh v Union of India* (2011) 7 SCC 69 [43].

¹¹⁹ G.S.R. 18, Indian Telegraph (1st Amendment of 2014) Rules, 2014, (28 January 2014).

¹²⁰ Indian Telegraph Rules, 1951, r. 419A(7).

authenticity.¹²¹

(c) Surveillance under the Information Technology Act, 2000

The IT Act was passed with the objective of facilitating economic growth by giving legal recognition to e-commerce and electronic transactions. It provides a legal framework to regulate India's digital ecosystem, electronic communication, cyber-crimes, and security practices.

The law was significantly amended in February 2009, when Parliament passed the Information Technology (Amendment) Act, 2008. The amendment was introduced in the aftermath of the terror attacks in Mumbai, and added new provisions for the interception, monitoring, and decryption of communications, and for the monitoring of internet traffic data. The amendment also provided safeguards to protect personal data, and delineated responsibilities for service providers and intermediaries.¹²²

As we discuss below, the IT Act permits direct surveillance through Section 69 and Section 69B of the IT Act, and indirect surveillance and monitoring through intermediary liability provisions and the regulation of cyber cafes.¹²³

In general, the powers vested in the State under the IT Act to intercept and monitor electronic communication and online activity are wider than the Telegraph Act. This is primarily because the IT Act authorises interception and monitoring on a "computer resource" as opposed to a "telegraph". The Telegraph Act defines "telegraph" as 'any appliance, instrument, material or apparatus used for transmission or reception of signs, signals, images, sounds, or intelligence by wire, visual, or electro-magnetic emissions.'¹²⁴ However, the IT Act authorises interception and monitoring of a "computer resource" which is defined to include

¹²¹ See Indian Telegraph Rules, 1951, r. 419A(13).

¹²² The Information Technology (Amendment) Act, 2008, ss. 22, 40.

¹²³ Software Freedom Law Centre, 'India's Surveillance State' (Software Freedom Law Centre 2014) <<https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf>> accessed 26 May 2022.

¹²⁴ Indian Telegraph Act 1885, s. 3(1AA).

a “computer”¹²⁵ and a “computer system”.¹²⁶ Thus, while the Telegraph Act’s interception provisions are primarily directed at TSPs and ISPs responsible for the transmission of communications, the IT Act permits surveillance through TSPs and ISPs but also on any computer system that not only transmits but also hosts or stores information, including individual devices (e.g., a laptop or a server).¹²⁷

There is some overlap in the operation of interception regimes of the Telegraph Act and the IT Act with respect to communications through mobile phones. This is because telephones (including mobile phones) are classified both as a “telegraph” under the Telegraph Act and a “communication device” within the meaning of ‘computer resource’ under the IT Act.¹²⁸ Thus interception on mobile phones may take place on either statute.

In January 2019, various civil society organisations and human rights activists challenged the constitutionality of the surveillance powers under Section 69 of the IT Act, including the procedures and safeguards for surveillance set out in delegated legislation, in multiple petitions before the Supreme Court.¹²⁹ The challenge was predicated on the changing standards of the right to privacy and proportionality elaborated by the Supreme Court in *Puttaswamy* and the *Aadhaar Judgment*. The petitions are currently pending before the Court.¹³⁰

(i) Interception, monitoring, and decryption under Section 69 of the IT Act

Section 69 of the IT Act lays down the power of the Union and state governments to issue directions to monitor, intercept, or decrypt (collectively ‘electronic

125 Information Technology Act, 2000, s. 2(1)(i). “Computer” means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

126 Information Technology Act, 2000, s. 2(1)(l). “Computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

127 Indian Telegraph Act 1885, s. 5(2); Information Technology Act, 2000, s. 69(1). The Telegraph Act specifically uses the phrase “brought for transmission by or transmitted or received by any telegraph”, while the IT Act uses the phrase “information generated, transmitted, received or stored in any computer resource”.

128 Kharbanda (n 96). Overlap with the IT Act.

129 *Internet Freedom Foundation v Union of India* WP (C) 44 of 2019; *PUCL v Union of India* WP (C) 61 of 2019.

130 *M L Sharma v Union of India* WP (Criminal) 1 of 2019 (see also cases tagged with this petition).

surveillance’)¹³¹ any information generated, transmitted, received, or stored on a computer resource. Thus, Section 69 authorises State surveillance of the *content* of electronic communication both in real time and after the fact.

Electronic surveillance orders must be in writing and contain the reasons for surveillance.¹³² Just as under the Telegraph Act, service providers are tasked with operationalising surveillance. However, in the case of the IT Act, such service providers may include TSPs, ISPs, or even online intermediaries.¹³³

Substantive standard for interception

Under Section 69 of the IT Act, the State may authorise electronic surveillance if it is satisfied that it is “necessary or expedient” to do so in the interests of the sovereignty, integrity, defence, or security of India, its friendly relations with foreign States, public order, preventing the incitement to any cognizable offence, or for the investigation of an offence. Although Section 69 has evidently been modelled after Section 5(2) of the Telegraph Act, there are two key differences that result in Section 69 expanding the surveillance power of the State.¹³⁴

1. The pre-conditions of “public emergency” or in the “interest of public safety” for invoking surveillance powers under Section 5(2) of the Telegraph Act have been removed. Thus, key threshold requirements that form constraints on when the State may exercise its surveillance powers have been removed. This substantially expands when the State may conduct surveillance, consequently heightening the risk to the right to privacy of citizens.¹³⁵ This approach also deviates from the surveillance framework considered (and modified) by the Supreme Court in *PUCL*. The Court upheld the constitutionality of the Telegraph Act’s interception regime *inter alia* because it included a high substantive threshold for the initiation of surveillance (public emergency and the interests of public safety)¹³⁶ that is absent in the IT Act and may alter an analysis of the latter statute’s constitutionality.

¹³¹ See Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 G.S.R. 780(E) dated 27 October 2009 [“**IT Interception Rules**”], r. 2(g), 2(l), 2(o).

¹³² Information Technology Act, 2000, s. 69(1).

¹³³ Information Technology Act, 2000, s. 2(1)(w).

¹³⁴ Vrinda Bhandari and Renuka Sane, ‘Towards a Privacy Framework for India in the Age of the Internet’ (National Institution of Public Finance and Policy 2016) <https://macrofinance.nipfp.org.in/PDF/ILEPCPr_BhandariSane20160926.pdf> accessed 26 May 2022.

¹³⁵ Software Freedom Law Centre, ‘India’s Surveillance State’ (n 123) 16.

¹³⁶ *PUCL v Union of India* (1997) 1 SCC 301 [28]-[30].

2. Section 69(1) of the IT Act *expands* the reasons for which electronic surveillance may be conducted. In addition to the grounds such as the sovereignty of India and public order listed in the Telegraph Act, the IT Act authorises electronic surveillance for reasons of ‘investigating an offence’ or the “defence of India”.¹³⁷

In the context of the Telegraph Act, the Supreme Court had interpreted the terms “public emergency” and “in the interests of public safety” fairly strictly, requiring the State to demonstrate how ‘the interests of the people at large’ were impacted for surveillance to be justified. The absence of these pre-conditions coupled with the authorisation of surveillance for ‘investigating an offence’ allows the surveillance powers of the IT Act to be utilized for ordinary law enforcement investigations, even to target a single individual. This may be contrasted to the Telegraph Act, which only permits interception in situations where the welfare of a large number of people may be at stake (in public emergencies or situations impacting public safety). Thus, the substantive threshold for the IT Act is significantly lower than that of the Telegraph Act. As discussed later in this report, this has significant implications when assessing the constitutionality of the surveillance provisions under the IT Act.

Procedural framework for interception under the IT Act

The procedure and safeguards for electronic surveillance under Section 69 are set out in delegated legislation,¹³⁸ specifically the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (“**IT Interception Rules**”). As noted above, an order for electronic surveillance under the IT Act must be in writing,¹³⁹ contain the reasons for issuing such a direction, and specify the name and designation of officer to whom the information is to be disclosed.¹⁴⁰

Under the IT Interception Rules, the “competent authority” to issue electronic surveillance orders is the Secretary to the Ministry of Home Affairs where the Union Government is concerned, and the Secretary to the Home Department, in cases of a State Government.¹⁴¹ In unavoidable circumstances or emergent cases, these powers can be exercised by more junior level officers, subject to certain

¹³⁷ Information Technology Act, 2000, s. 69.

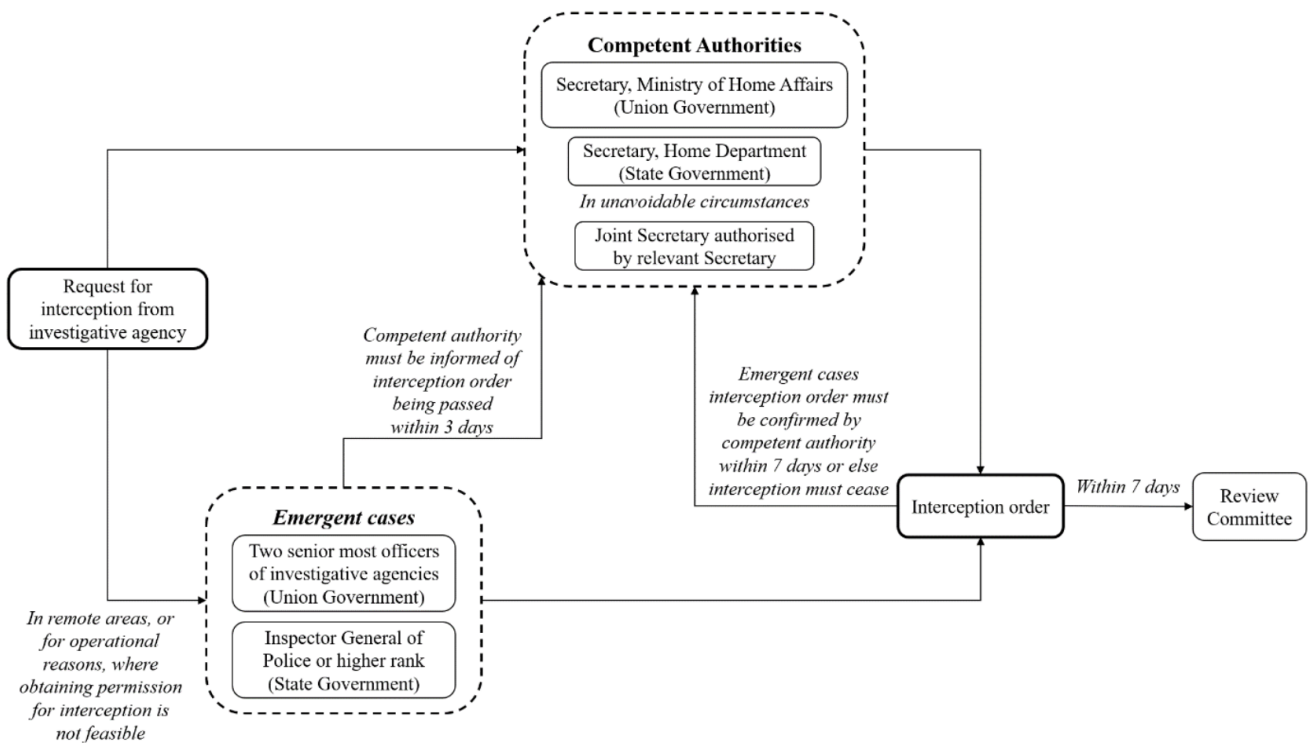
¹³⁸ Information Technology Act, 2000, s. 69(2).

¹³⁹ Information Technology Act, 2000, s. 69(1).

¹⁴⁰ IT Interception Rules, r. 7, 10.

¹⁴¹ IT Interception Rules, r. 2(d) read with r. 3.

conditions including *ex-post* approval by the above-mentioned senior officers.¹⁴² State level police officers, such as the Station House Officer of a police station, cannot directly authorise electronic surveillance.¹⁴³ Like Rule 419A of the Telegraph Rules, where interception orders are issued by members of investigative agencies or the police, the competent authority must be informed within three days and the interception order must be confirmed within seven days.¹⁴⁴ If an order is not confirmed, the IT Interception Rules state that the interception shall cease,¹⁴⁵ but do not state that the interception order is *void ab initio* or that the intelligence gathered during the seven days shall be destroyed. A flow chart depicting the procedure to procure a lawful interception order is provided below:



The competent authority may also empower an ‘authorised agency’ to conduct electronic surveillance on a computer resource for the purposes specified in Section 69(1).¹⁴⁶ In December 2018, the Ministry of Home Affairs issued a

¹⁴² IT Interception Rules, r. 3.

¹⁴³ IT Interception Rules, r. 3 (proviso).

¹⁴⁴ IT Interception Rules, r. 3.

¹⁴⁵ IT Interception Rules, r. 3.

¹⁴⁶ Information Technology Act, s. 69(1); IT Interception Rules, r. 4.

notification authorising ten Union Government agencies including the CBI, Intelligence Bureau, Research & Analysis Wing, and Enforcement Directorate to conduct electronic surveillance under the IT Act.¹⁴⁷ These are thus the ‘authorised agencies’ under Section 69 of the IT Act.

This notification has also been challenged as part of the larger constitutional challenge to electronic surveillance under the IT Act.¹⁴⁸ The petitioners in this case *inter alia* argue that the notification, and the scheme of surveillance under Section 69(1) of the IT Act contravenes the *Aadhaar Judgement*, which struck down a provision permitting officers holding the rank of Joint Secretary to disclose citizen’s information in the interest of national security.¹⁴⁹

As under the Telegraph Rules, the IT Interception Rules requires the competent authority (or authorised agency) to consider alternative means to acquire the information prior to issuing a surveillance order.¹⁵⁰ The electronic surveillance order will remain valid for a period of 60 days unless revoked earlier, and can be renewed for a maximum of 180 days.¹⁵¹

Rule 22 of the IT Interception Rules requires the agency implementing surveillance to destroy all records, including those pertaining to directions for electronic surveillance, every six months, unless needed for “functional requirements.”¹⁵² Intermediaries also must destroy records pertaining to the surveillance directions within two months from the discontinuance of electronic surveillance, and in doing so, they must maintain extreme secrecy.¹⁵³

In an appeal against the non-disclosure of information under the Right to Information Act, 2005 before the High Court of Delhi, when asked about the *total*

147 Ministry of Home Ministry (Cyber and Information Security Division) S.O. 6227(E) dated 20 December 2018. The notified agencies are: (i) Intelligence Bureau; (ii) Narcotics Control Bureau; (iii) Enforcement Directorate; (iv) Central Board of Direct Taxes; (v) Directorate of Revenue Intelligence; (vi) Central Bureau of Investigation; (vii) National Investigation Agency; (viii) Cabinet Secretariat (Research & Analysis Wing); (ix) Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only); (x) Commissioner of Police, Delhi.

148 *Internet Freedom Foundation v Union of India* WP (C) 44 of 2019; *PUCL v Union of India* WP (C) 61 of 2019.

149 Mehal Jain, ‘Challenge Against 69 IT Act And MHA Notification On Monitoring Computers: SC Issues Notice To Centre’ (*Live Law*, 14 January 2019) 69 <<https://www.livelaw.in/top-stories/challenge-against-69-it-act-and-mha-notification-on-monitoring-computers-sc-issues-notice-to-centre-142098>> accessed 28 March 2023.

150 IT Interception Rules, r. 8.

151 IT Interception Rules, r. 11.

152 IT Interception Rules, r. 23(1).

153 IT Interception Rules, r. 23(2).

number of electronic surveillance orders passed under the IT Act, the Ministry of Home Affairs of the Union Government cited Rule 22 as a reason for destroying even information regarding the total number of surveillance orders passed over a two-year period.¹⁵⁴ The High Court directed the Central Information Commission to decide on the validity of the Union Government's justification for not disclosing the total number of electronic surveillance orders.¹⁵⁵

As discussed at the start of this section, orders for electronic surveillance under Section 69 may be issued to TSPs, ISPs, or online intermediaries.¹⁵⁶ Under sections 69(3) and 69(4) of the IT Act, all 'intermediaries' or 'persons in charge of a computer resource' must "extend all facilities and technical assistance" to provide access to the specified computer resource, secure it, intercept, monitor or decrypt the information on the resource, or provide the information stored in the computer resource.

This includes providing technical assistance and equipment (or access to equipment) including hardware, software, firmware, storage, and relevant interfaces to facilitate surveillance.¹⁵⁷ Such technical assistance could be for: (i) the installation of equipment of the authorised agency; (ii) the maintenance, testing or use of such equipment; (iii) the removal of such equipment; or (iv) the performance of any action required for accessing stored information.¹⁵⁸

This extends to authorising intermediaries to install computer equipment, install any communication link software at the subscriber's end, and access stored information from a computer resource.¹⁵⁹ Failure to provide technical assistance is punishable with imprisonment up to seven years and a fine.¹⁶⁰

To guard against unauthorised surveillance, intermediaries must send a list of electronic surveillance orders received by them every fifteen days to the

¹⁵⁴ Internet Freedom Foundation, 'Delhi HC Directs MHA to Clarify Its Position on Maintenance of E-Surveillance Data' (*Internet Freedom Foundation*, 8 April 2022) <<https://internetfreedom.in/delhi-hc-directs-mha-to-clarify-its-position-on-maintenance-of-e-surveillance-data/>> accessed 30 May 2022.

¹⁵⁵ Internet Freedom Foundation, 'DHC Directs CIC to Decide IFF's Appeals within 8 Weeks' (*Internet Freedom Foundation*, 2 December 2021) <<https://internetfreedom.in/dhc-directs-cic-to-decide-iffs-appeals-within-8-weeks/>> accessed 26 May 2022; Internet Freedom Foundation, 'Top Secret MHA Refuses to Reveal Total Number of Snooping Requests' (*Internet Freedom Foundation*, 6 February 2019) <<https://internetfreedom.in/top-secret-government-refuses-to-reveal-total-number-of-snooping-requests/>> accessed 26 May 2022.

¹⁵⁶ Information Technology Act, 2000, s. 2(1)(w).

¹⁵⁷ IT Interception Rules, r. 19.

¹⁵⁸ IT Interception Rules, r. 19.

¹⁵⁹ IT Interception Rules, r. 24.

¹⁶⁰ Information Technology Act, 2000, s. 69(4).

issuing authorities and agencies, to confirm the authenticity of the orders.¹⁶¹ Intermediaries must also ensure that the contents of intercepted, monitored, or decrypted information are not used or disclosed to any person other than the intended recipient of the information.¹⁶²

Similar purpose limitation obligations are placed on the agencies authorised to carry out surveillance; they cannot disclose the contents of information gathered except when sharing intelligence with other agencies for investigatory purposes, or in judicial proceedings.¹⁶³ The contents of collected information cannot be disclosed or reported in public by any means without a prior court order.¹⁶⁴

A copy of every electronic surveillance direction shall be sent to the Review Committee that reviews telephonic interception under the Telegraph Act (constituted under Rule 419A of the Telegraph Rules) within seven working days.¹⁶⁵ The Review Committee must meet at least once in two months and record its findings on whether the directions for electronic surveillance comply with the IT Interception Rules.¹⁶⁶ In case the Committee is of the opinion that the directions are not in accordance with the Rules, it may set aside the directions and issue orders for destruction of the electronic records collected.¹⁶⁷

(ii) Monitoring and collecting traffic data or metadata under Section 69B, IT Act

Section 69B of the IT Act empowers the Union Government to authorise any government agency to monitor and collect: (i) “traffic data” or (ii) information generated, transmitted, received or stored in any computer resource. The information may be collected for cyber security purposes or to prevent the intrusion or spread of a computer contaminant in the country.¹⁶⁸

Traffic data has been defined in a manner that includes metadata¹⁶⁹ (i.e., data about

¹⁶¹ IT Interception Rules, r. 18(2).

¹⁶² IT Interception Rules, r. 25(1).

¹⁶³ IT Interception Rules, r. 25(2).

¹⁶⁴ IT Interception Rules, r. 25(2).

¹⁶⁵ IT Interception Rules, r. 2(q) read with r. 7.

¹⁶⁶ IT Interception Rules, r. 22.

¹⁶⁷ IT Interception Rules, r. 22.

¹⁶⁸ Information Technology Act, 2000, s. 69B.

¹⁶⁹ Information Technology Act, 2000, s. 69B(4)(ii). “Traffic data” is “any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service or any other information.”

data). Thus, Section 69B enables the government to engage in the surveillance of internet metadata. The collection of metadata does raise certain risks to the right to privacy. As explained by the Necessary & Proportionate Principles launched at the UN Human Rights Council in Geneva (cited by Nariman J. in *Puttaswamy*), “communications metadata may create a profile of an individual’s life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.”¹⁷⁰

Permitting the collection of ‘information generated, transmitted, received or stored in any computer service,’ would seemingly allow broad and deep surveillance. However, recognised practice under this provision is yet to emerge, and courts are yet to meaningfully interpret this provision. Unlike electronic surveillance powers under Section 69, the power to monitor and collect ‘traffic data’ and other information is limited to the Union Government. State governments cannot exercise any surveillance powers under Section 69B of the IT Act.

Substantive and procedural contours of Section 69B

The powers under Section 69B can only be exercised for two purposes: (i) to enhance “cyber security”; and (ii) for identification, analysis and prevention of intrusion or spread of a “computer contaminant” in the country. Both the terms “cyber security” and “computer contaminant” have been broadly defined in the IT Act,¹⁷¹ and vest substantial discretion with the government in determining when to exercise these powers.¹⁷² For example, under the head of “cyber security” a monitoring order can be issued for the forecasting of imminent cyber incidents, detection of viruses or computer contaminant, and tracking cyber security breaches.¹⁷³

¹⁷⁰ Electronic Frontier Foundation, ‘Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance’ (*Necessary & Proportionate*, May 2014) <<https://necessaryandproportionate.org/images/np-logo-og.png>> accessed 26 May 2022.

¹⁷¹ Information Technology Act, 2000, s. 2(1)(ns); Information Technology (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 G.S.R. 782(E) dated 27 October 2009 [“**IT Traffic Data Rules**”], r. 3(2). Cyber security is defined as “protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction”; Information Technology Act, 2000, s. 43, Explanation (i). Computer contaminant has been defined as: “any set of computer instructions that are designed – (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network.”

¹⁷² Software Freedom Law Centre, ‘India’s Surveillance State’ (n 123) 18.

¹⁷³ Information Technology Act, 2000, ss. 69B(2), 69B(4); IT Traffic Data Rules, r. 3(2).

Like Section 69, the Union Government has the power to specify the procedure for carrying out surveillance under Section 69B through delegated legislation. In this regard, the Union Government notified the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (“**IT Traffic Data Rules**”) in 2009. Any action under Section 69B must be carried out according to the procedure and safeguards laid down in these Rules.

The competent authority to authorise surveillance under Section 69B is the Secretary to the Ministry of Electronics and Information Technology (“**MEITY**”); who can further authorise any agency to undertake such monitoring and collection.¹⁷⁴ Orders for monitoring must be in writing and contain reasons.¹⁷⁵ As under Section 69, the intermediary is bound to provide technical assistance and extend all facilities.¹⁷⁶

The Review Committee constituted under Rule 419A of the Telegraph Rules, that reviews interception orders under Section 5 of the Telegraph Act and electronic surveillance orders under Section 69 of the IT Act, also reviews the orders passed under Section 69B, to ensure compliance with Section 69B and the IT Traffic Data Rules.¹⁷⁷ The Review Committee can order the destruction of data collected in case of non-compliance.¹⁷⁸ Further, strict confidentiality is to be maintained with respect to the orders issued under Section 69B for monitoring and collection of traffic data and information.¹⁷⁹

(iii) Duty of intermediaries

Under Section 67C of the IT Act, intermediaries have a duty to preserve and retain information specified by the Union Government. They must do so for a duration, and in a manner, prescribed by the Government. Knowingly or intentionally failing to comply with this provision is punishable with imprisonment for up to three years and a fine.¹⁸⁰

Decryption

The IT Interception Rules also stipulate that where an intermediary holds a

¹⁷⁴ Information Technology Act, 2000, s. 69B(1); IT Traffic Data Rules, r. 4(1).

¹⁷⁵ IT Traffic Data Rules, r. 3(3).

¹⁷⁶ Information Technology Act, 2000, s. 69B(2); IT Traffic Data Rules, r. 4(4) - 4(10).

¹⁷⁷ IT Traffic Data Rules, r. 3(3).

¹⁷⁸ IT Traffic Data Rules, r. 3(3).

¹⁷⁹ IT Traffic Data Rules, r. 9(3).

¹⁸⁰ Information Technology Act, 2000, s. 67C(2).

decryption key, the intermediary must disclose the key or provide decryption assistance as may be specified in the electronic surveillance order issued under Section 69 of the IT Act.¹⁸¹ However, the IT Interception Rules clarify that the decryption direction “shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key.”¹⁸² Thus, under the IT Interception Rules, the duty of “technical assistance” would appear not to require an intermediary to implement changes in its platform architecture to create a backdoor, or weaken end-to-end encryption,¹⁸³ but merely assist with decryption in situations where it possesses the decryption key.

The issue of decryption was briefly argued before Indian courts in the context of the default end-to-end encryption provided by WhatsApp.¹⁸⁴ Subsequently, the adoption of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021 (“**Intermediary Guidelines 2021**”) introduced a requirement that a “social media intermediary” having more than five million users and “providing services primarily in the nature of messaging” shall “enable the identification of the first originator” of a particular message on its platform;¹⁸⁵ this requirement has also been challenged.¹⁸⁶ No judgement has been delivered in any of these cases at the time of this report.

Intermediary liability

¹⁸¹ IT Interception Rules, r. 5.

¹⁸² IT Interception Rules, r. 13.

¹⁸³ Vrinda Bhandari, Rishab Bailey and Faiza Rahman, ‘Backdoors to Encryption: Analysing an Intermediary’s Duty to Provide “Technical Assistance” [2021] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3805980>> accessed 1 May 2021.

¹⁸⁴ *Facebook v Union of India* TP (C) 1943-46 of 2019 (Supreme Court of India); *Antony Clement Rubin v Union of India*, WP (C) 20774 of 2018 (High Court of Madras). Internet Freedom Foundation, ‘Facebook’s Transfer Petition in Madras HC Case Involving Encryption and Traceability Allowed after Tamil Nadu Government Withdraws Objections’ (*Internet Freedom Foundation*, 22 October 2019) <<https://internetfreedom.in/facebooks-transfer-petition-in-madras-hc-case-involving-encryption-and-traceability-allowed-after-tamil-nadu-government-withdraws-objections/>> accessed 26 May 2022.

¹⁸⁵ Intermediary Guidelines 2021, r. 4(2). See also Intermediary Guidelines 2021, r. 2(1)(w) defining “social media intermediary” as an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services; Ministry of Electronics and Information Technology, Notification S.O. 942(E) dated 25 February 2021 stipulating that every “social media intermediary” having more than five million users shall qualify as a “significant social media intermediary” bound by Rule 4 of the Intermediary Guidelines 2021.

¹⁸⁶ *Facebook Inc v Union of India* WP (C) 7281 of 2021 (High Court of Delhi); *WhatsApp LLC v Union of India* WP (C) 7284 of 2021 (High Court of Delhi).

The Indian model of intermediary liability differs from the absolute model of safe harbour exemption under Section 230 of the Communications Decency Act of the United States.¹⁸⁷ In order to qualify for safe harbour in India, intermediaries must comply with various conditions set out under Section 79 of the IT Act and rules prescribed by the Union Government – the Intermediary Guidelines 2021.¹⁸⁸

Intermediaries must comply with these Guidelines to retain their safe harbour protection and avoid prosecution under criminal law for any unlawful content they host. Non-compliance with the Intermediary Guidelines 2021 may have other adverse consequences for ‘significant social media intermediaries’ (social media intermediaries with more than five million users in India).¹⁸⁹ Such entities are required to appoint local officers who reside in India, who are in turn responsible for coordination with investigative agencies and ensuring compliance with the Intermediary Guidelines 2021 more generally.¹⁹⁰ A breach of the Guidelines could result in the local officers being held personally liable.¹⁹¹

Challenges to the constitutionality of the Intermediary Guidelines 2021 are currently pending before multiple High Courts and the Supreme Court in India.¹⁹² On 9 May 2022, the Supreme Court stayed all proceedings in the High Courts until it decides whether these cases should be transferred to the Supreme Court and heard together.¹⁹³

¹⁸⁷ Vasudev Devadasan, ‘Report on Intermediary Liability in India’ (Centre for Communication Governance 2022) <<https://papers.ssrn.com/abstract=4343781>>.

¹⁸⁸ Information Technology Act, 2000, s. 79.

¹⁸⁹ Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) dated 25 February 2021 [“**Intermediary Guidelines 2021**”], r. 2(1)(w), 2(1)(v). A “significant social media intermediary” is an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services and has more registered users than a threshold specified by the Union Government. By Notification S.O. 942(E) dated 25 February 2021, the Ministry of Electronics and Information Technology specified the threshold as 5 million.

¹⁹⁰ Intermediary Guidelines 2021, r. 4(1). See also Devadasan (n 187).

¹⁹¹ Intermediary Guidelines 2021, r. 4(1)(a).

¹⁹² *LiveLaw Media Pvt Ltd v Union of India* WP (C) 6272 of 2021 (High Court of Kerala); *Sanjay Kumar Singh v Union of India* WP (C) 3483 of 2021 (High Court of Delhi); *Uday Bedi v Union of India* WP (C) 6844 of 2021 (High Court of Delhi); *Praveen Arimbrathodiyil v Union of India* WP (C) 9647 of 2021 (High Court of Kerala); *TM Krishna v Union of India* WP (C) 12515 of 2021 (High Court of Madras); *Sayanti Sengupta v Union of India* WPA (P) 153 of 2021 (High Court of Calcutta); *Nikhil Wagle v Union of India* PIL (L) 14204 of 2021 (High Court of Bombay); *Facebook Inc v Union of India* WP (C) 7281 of 2021 (High Court of Delhi); *WhatsApp LLC v Union of India* WP (C) 7284 of 2021 (High Court of Delhi).

¹⁹³ *Skand Bajpai v Union of India* WP (C) 799 of 2020 (Supreme Court of India) order dated 9 May 2022.

From the perspective of surveillance, two provisions are relevant. First, under Rule 3(1)(j) of the Intermediary Guidelines 2021, any intermediary (whether TSP, ISP, or online intermediary), must provide authorised investigative agencies with ‘information under its control or possession, or assistance’ within 72 hours of receipt of a written order. Such orders may be issued to intermediaries for the purposes of verifying the identity of an internet user or for the prevention, investigation, or prosecution of an offence under any law. It is unclear how the scope of ‘information or assistance’ is to be interpreted, or how it relates to their duty to provide ‘technical assistance’ under Section 69 of the IT Act and the IT Interception Rules.

Second, Rule 4(2) requires significant social media intermediaries that provide “messaging services” to identify the “first originator” of content pursuant to an order by a court or an authorised investigative agency under Section 69 of the IT Act. Although the term “first originator” is not defined in the IT Act or the Intermediary Guidelines 2021, the IT Act does define the term ‘originator’ to mean a person who generates, stores, or transmits an electronic message or by their actions, causes a message to be generated, stored, or transmitted. Thus, the term “first originator” may be construed to mean the first person to generate, store, or transmit a specific piece of content on a messaging network. Rule 4(2) also states that where content originates from outside India, the “first originator” of the content shall be deemed to be the first person to have *received* the content in India.¹⁹⁴

An order to trace the “first originator” under Rule 4(2) shall only be passed for the purposes of preventing, detecting, investigating, prosecuting, or punishing an offence related to the sovereignty, integrity, or security of India, its friendly relations with foreign States; public order; the incitement to such offences; or offences relating to rape, sexually explicit material, or child sexual abuse material.¹⁹⁵ No order can be passed under Rule 4(2) if alternative, less intrusive means of identifying the originator are possible.¹⁹⁶ The Rule states that in complying with an order under Rule 4(2), a significant social media intermediary such as WhatsApp will not have to disclose the *content* of the message, or any other information relating to the first originator or its other users.¹⁹⁷

WhatsApp has specifically challenged the constitutionality of Rule 4(2) before the Delhi High Court for violating the fundamental rights of free speech and

¹⁹⁴ Intermediary Guidelines 2021, r. 4(2) (fourth proviso).

¹⁹⁵ Intermediary Guidelines 2021, r. 4(2) (first proviso).

¹⁹⁶ Intermediary Guidelines 2021, r. 4(2) (second proviso).

¹⁹⁷ Intermediary Guidelines 2021, r. 4(2) (third proviso).

privacy of its users.¹⁹⁸ A WhatsApp spokesperson said that, “Requiring messaging apps to “trace” chats is the equivalent of asking us to keep a fingerprint of every single message sent on WhatsApp, which would break end-to-end encryption and fundamentally undermines people’s right to privacy.”¹⁹⁹ Other petitions by Indian companies and citizens have challenged Rule 4(2) as being disproportionate and presuming criminality on an entire population, in violation of the *Aadhaar Judgment*.²⁰⁰ Various experts have argued that Rule 4(2) is disproportionate, as it infringes on the privacy of all users of messaging services to catch a few allegedly unlawful actors.²⁰¹

(iv) Cyber Café Rules

Cybercafés are facilities from where internet access is offered to members of the general public in the ordinary course of business.²⁰² Cybercafés are under a legal obligation to share information with the government, including logs reporting internet usage and the personal details of all visitors.²⁰³ The monthly reports thus allow the government to monitor the cybercafé usage of *all* citizens.

Authorised government officers are empowered to check a cybercafé at any time to assess compliance with the Information Technology (Guidelines for Cyber Café) Rules, 2011.²⁰⁴ During such an inspection, the cybercafé must share ‘every related document, register, or any necessary information’ with the inspecting officer.²⁰⁵

Notably, the inspecting authorities are not required to satisfy any preconditions to access such materials, or even have a reasonable suspicion of illegality before conducting such a search. Thus, the 2011 Rules raise concerns that these provisions will enable State surveillance by allowing the indirect monitoring of citizens’

198 *WhatsApp LLC v Union of India* WP (C) 7284 of 2021 (High Court of Delhi).

199 Deeksha Bhardwaj and Richa Banka, ‘WhatsApp Moves High Court against New IT Rules’ (*Hindustan Times*, 27 May 2021) <<https://www.hindustantimes.com/india-news/whatsapp-moves-high-court-against-new-it-rules-101622073962404.html>> accessed 26 May 2022.

200 *LiveLaw Media Pvt Ltd v Union of India* WP (C) 6272 of 2021 (High Court of Kerala); *TM Krishna v Union of India* WP (C) 12515 of 2021 (High Court of Madras).

201 Greg Nojeim and Namrata Maheshwari, ‘Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth’ (2021) 17 *Indian Journal of Law and Technology* 1; Gurshabad Grover, Tanaya Rajwade and Divyank Katira, ‘The Ministry and the Trace: Subverting End-To-End Encryption’ (2021) 14 *NUJS Law Review*; Devadasan (n 187).

202 Information Technology Act, 2000, s. 2(1)(na).

203 Information Technology (Guidelines for Cyber Café) Rules, 2011 G.S.R. 315(E) dated 11 April 2011 [“**Cyber Café Rules**”], r. 5(3).

204 Cyber Café Rules, r. 7.

205 Cyber Café Rules, r. 7.

internet usage and activities. However, it must be noted that with the increase of mobile internet subscribers in India,²⁰⁶ reliance on cybercafés to access the internet has reduced.

(v) Other powers under the IT Act

Apart from the surveillance powers described above, the IT Act also confers the power to call for information (and thus conduct indirect surveillance) on authorities such as the Controller of Certifying authorities (“**CCA**”), and the Indian Computer Emergency Response Team (“**CERT-In**”).

The CCA is a public authority set up by the IT Act to licence and regulate the functioning of Certifying Authorities (the entities granted a license to issue electronic signature certificates).²⁰⁷ To carry out its functions, the CCA has been granted a wide range of powers that raise surveillance-related concerns. The CCA, or an officer authorised by it, can investigate the contravention of any provision or rule under the IT Act, and its investigative powers are akin to those granted to income tax authorities under the Income Tax Act, 1961.²⁰⁸ Thus, the CCA can call for electronically stored information and conduct searches.²⁰⁹

This power extends to information from intermediaries.²¹⁰ For example, disclosures under the Right to Information Act, 2005 (“**RTI Act**”) revealed that in 2011, the CCA made 73 requests for user data and information to Yahoo, Google, Facebook, AOL, Orkut, Hotmail, and other intermediaries.²¹¹

CERT-In, established under Sec. 70B(1) of the IT Act, is under the administrative control of MEITY. CERT-In is tasked with ensuring cybersecurity and responding to cybersecurity incidents by collecting and analysing information, undertaking emergency measures, issuing alerts, and coordinating cyber incident response

²⁰⁶ Telecom Regulatory Authority of India, ‘The Indian Telecom Services Performance Indicators: January - March, 2022’ (Telecom Regulatory Authority of India 2022) <https://www.trai.gov.in/sites/default/files/QPIR_26072022_0.pdf>.

²⁰⁷ Information Technology Act, 2000, s. 2(1)(g). Certifying Authority is defined as a person who has been granted a license to issue a electronic signature certificate under s. 24

²⁰⁸ Information Technology Act, 2000, s. 28; Income Tax Act, 1961, Chapter XIII.

²⁰⁹ Information Technology Act, 2000, s. 29. Software Freedom Law Centre, ‘India’s Surveillance State’ (n 123) 19.

²¹⁰ *Yahoo India v Union of India* WP (C) 6654 of 2011 (High Court of Delhi). The CCA sought included the email addresses of certain individuals from Yahoo.

²¹¹ ‘Information on India’s Surveillance Practices Received under the Right to Information Act, 2005’ (Software Freedom Law Centre, 9 April 2014) <<https://sflc.in/information-received-under-rti-for-surveillance>> accessed 16 February 2023.

activities.²¹² To carry out these functions, CERT-In can call for information or issue directions to intermediaries, service providers, data centres, and companies.²¹³ Failure to provide information to CERT-In is punishable with imprisonment up to one year and/or a fine up to Rs. 1,00,000.²¹⁴

On 28th April 2022, MEITY and CERT-In released directions which require, *inter alia*, providers of virtual private networks and virtual private servers to maintain records of:

- the names, addresses, and contact numbers of their subscribers;
- IP addresses allotted to subscribers;
- IP addresses and email addresses used by subscribers at the time of onboarding;
- the period and purpose for which the virtual private network service was utilised; and;
- records of financial transactions.²¹⁵

CERT-In also requires all intermediaries and data centres to “mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days” within India.²¹⁶ The directions also state that CERT-In could requisition such information and that non-compliance with the directions “may invite punitive action” under the IT Act or other laws.²¹⁷ The directions have been challenged in the High Court of Delhi as being beyond the rule-making powers of CERT-In under the IT Act, and as harming free expression on the internet.²¹⁸

The IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 authorise government agencies to request any company for sensitive personal data about their users for the purpose of identity verification

²¹² Information Technology Act, 2000, s. 70B(4).

²¹³ Information Technology Act, 2000, s. 70B(6).

²¹⁴ Information Technology Act, 2000, s. 70B(7).

²¹⁵ Ministry of Electronics and Information Technology (Indian Computer Emergency Response Team (CERT-In), ‘Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.’ No. 20(3) of 2022 dated 28 April 2022 <https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf> accessed 11 May 2022 [“CERT-In Rules”], para (v).

²¹⁶ CERT-In Rules, para (iv).

²¹⁷ CERT-In Rules, para (iii), closing recital.

²¹⁸ *SNTHostings v Union of India* WP 13997 of 2022 (High Court of Delhi, 28 September 2022).

or for the prevention, detection, investigation, prosecution, or the punishment of offences.²¹⁹

(d) Interception and information gathering under criminal law

In addition to the Telegraph Act and IT Act, the Indian Code of Criminal Procedure (“CrPC”) and specialised state criminal laws such as the Maharashtra Control of Terrorism and Organised Crime Act, 1999 (“MCOCA”) also authorise the collection of information and surveillance.

(i) Interception under state criminal laws

In 1999, the government of Maharashtra enacted the MCOCA. In 2002 it was also extended by the Union Government to the National Capital Territory of Delhi.²²⁰ The MCOCA specifically authorises the interception of wire, electronic, and oral communications to both prevent, and aid investigations into organised crime.²²¹ The statute provides a *sui generis* procedural framework for such interceptions that is independent of the IT and Telegraph Acts.²²²

Under the MCOCA, a police officer of the rank of Superintendent of Police who is supervising an investigation under the Act can write to the “competent authority” (Secretary, Home Department of the State government) to authorise interceptions.²²³ The application is allowed if the competent authority has: (i) a ‘probable cause of belief’ that an individual has committed or is about to commit an offence under the MCOCA; (ii) that the particular communication can only be obtained through interception; and (iii) normal (less restrictive) modes of intelligence gathering have failed, are likely to fail, or are too dangerous to attempt.²²⁴

²¹⁹ Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 G.S.R. 131(E) dated 11 April 2011 [“**Reasonable Security Practices Rules**”], r. 6.

²²⁰ Ministry of Home Affairs, G.S.R. 6(E) dated 2 January 2002 <https://www.mha.gov.in/sites/default/files/video_59.PDF> accessed on 30 May 2022.

²²¹ Maharashtra Control of Organised Crime Act, 1999 [“**MCOCA**”], statement of objects and reasons.

²²² MCOCA, s. 14-16. See also Srijoni Sen and others, ‘Anti-Terror Law in India: A Study of Statutes and Judgements, 2001-2014’ (Vidhi Centre for Legal Policy 2015) 80 <https://vidhilegalpolicy.in/wp-content/uploads/2020/06/150531_VidhiTerrorismReport_Final.pdf> accessed 26 May 2022.

²²³ MCOCA, s. 13, 14(1).

²²⁴ MCOCA, s. 14(4).

Like the Telegraph Act and the IT Act, the MCOCA sets up a three-member executive Review Committee that reviews all interception orders passed under the Act, and can order the destruction of the intercepted communication if it disagrees with the competent authority's order.²²⁵ Unauthorised interception under the MCOCA is penalised.²²⁶ Other states have also passed similar laws. For example, the Karnataka Control of Organised Crime Act, 2000 also authorises interception through an identical set of provisions.²²⁷

The constitutional validity of the MCOCA, including the aforementioned interception provisions, was upheld by the Supreme Court in *State of Maharashtra vs. Bharat Shantilal Shah*.²²⁸ The Supreme Court held that the right to privacy was not an absolute right under Article 21 and could be curtailed in accordance with a just, fair, and reasonable procedure.²²⁹ The Court found that the law provided for sufficient safeguards against the misuse of interception powers, and thus upheld its validity.²³⁰

However, an analysis of the constitutionality of the MCOCA may be different post-*Puttaswamy*, where the Supreme Court adopted the proportionality test as the new standard that rights-infringing measures must satisfy. Given that *Bharat Shantilal Shah* was decided in 2008, the Court at the time did not undertake a structured proportionality analysis of the MCOCA's interception regime.

(ii) Information collection under the CrPC

Section 91 of the CrPC allows a court or an officer in charge of a police station (the 'Station House Officer') to issue a written summons to a person to produce a 'document or a thing' that is "necessary or desirable" for the purpose of any investigation, inquiry, trial, or other proceeding. Orders under Section 91, CrPC can be issued to intermediaries.²³¹

The broad wording of this provision allows its extension to electronic data, stored data, metadata, communication data, and details of emails sent and received,

²²⁵ MCOCA, s. 15.

²²⁶ MCOCA, s. 16.

²²⁷ Karnataka Control of Organised Crime Act, 2000, s. 14.

²²⁸ (2008) 13 SCC 5.

²²⁹ (2008) 13 SCC 5 [60].

²³⁰ (2008) 13 SCC 5 [61].

²³¹ *Antony Clement Rubin v State of Tamil Nadu* (2021) SCC Online Mad 2196.

thereby facilitating targeted surveillance.²³² In fact, in arguments before the Madras High Court and Delhi High Court, WhatsApp clarified that it complied with Section 91 requests by providing basic Subscriber Information (BSI) which “includes phone number, name, device info, App version, Start date/time, connection status, last connection date/time/[last known] IP, E-mail address, Web client data.”²³³

Thus, notices under Section 91, CrPC can reveal a significant amount of information about an individual, with relatively little oversight or accountability, even when compared to the IT Act.²³⁴ Commentators believe that investigative agencies prefer to use the broad authority under Section 91, CrPC compared to the stricter and more regulated powers under the IT Act.²³⁵

In general, courts and the police have a wide latitude when exercising powers under Section 91. However, there are certain limitations to the provision built in based on the nature and stage of the criminal proceedings.²³⁶ The powers under Section 91, CrPC cannot be used to conduct a ‘roving or fishing inquiry.’²³⁷ Some High Courts have opined that a request under Section 91 can only be made after a *prima facie* opinion has been formed that the ‘document or thing’ sought is necessary or desirable for an investigation or other proceeding under the CrPC.²³⁸

An order under Section 91 of the CrPC is mandatory and failure to produce a document or thing pursuant to a Section 91 request will amount to an offence under Section 175 of the IPC (‘omission to produce document to a public servant by

²³² Tarun Krishnakumar, ‘Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973’ (2019) 15 *Indian Journal of Law and Technology* 67; Sunil Abraham and Elonnai Hickok, ‘Government Access to Private-Sector Data in India’ (2012) 2 *International Data Privacy Law* 302.

²³³ *Ameet Parmeswaran v Commissioner of Police, Delhi* (2020) SCC Online Del 155; *Antony Clement Rubin v State of Tamil Nadu* (2021) SCC Online Mad 2196.

²³⁴ Kharbanda (n 96); Software Freedom Law Centre, ‘India’s Surveillance State: Other Provisions of Law That Enable Collection of User Information’ (SFLC.in, 2 December 2015) <<https://sflc.in/indias-surveillance-state-other-provisions-of-law-that-enable-collection-of-user-information>> accessed 26 May 2022.

²³⁵ Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, ‘How Stricter Procedures in Existing Law May Provide a Useful Path for Cloud Act Executive Agreements’ (*Cross-Border Data Forum*, 16 November 2018) <<https://www.crossborderdataforum.org/how-stricter-procedures-in-existing-law-may-provide-a-useful-path-for-cloud-act-executive-agreements/>> accessed 26 May 2022.

²³⁶ See *Om Prakash Sharma v Union of India* (2000) 5 SCC 679. The limitations depend on the stage or point of time of the power’s exercise in an investigation and must be commensurate with the nature of proceedings and the necessity and desirability of the information in question.

²³⁷ *State of Orissa v Debendra Nath Padi* (2005) 1 SCC 568.

²³⁸ *Subhasini Jena v Commandant of 6th Battalion* (1988) Cri LJ 1570 (Ori); *Hussenbhoy Abdoolabhoy Lalji v Rashid B Vershi* (1941) 43 Bom LR 523.

a person legally bound to produce'). Violations of Section 175, IPC are punishable with jail for up to 6 months and/or a fine of Rs. 1,000.

Section 92 of the CrPC empowers courts and either the Commissioner of Police or the District Superintendent of Police to demand and access any “document, parcel or thing” in the custody of the postal or telegraph authority. Under Section 92(1) District Magistrates, Chief Judicial Magistrates, Session Courts, or High Courts can direct the delivery of such a document, parcel, or thing to them. Other judges and the Commissioner of Police or the District Superintendent of Police can only call for such items to be searched and detailed pending an order by the above-mentioned judges under Section 92(1).²³⁹

(iii) Pegasus controversy and report

In July 2021, several news organisations reported that the Indian government had purchased and utilised the ‘Pegasus’ spyware on Indian citizens, including ministers in the Union Government, Members of Parliament, journalists, and members of civil society.²⁴⁰ Once a phone is infected with the spyware, Pegasus allows the individual supervising the spyware to copy messages and photos from the infected phone, record calls, and even record film through the infected phone’s camera or microphone.²⁴¹

In October 2021, the Supreme Court set up a committee to investigate the allegations of unauthorised surveillance using the Pegasus spyware, and appointed a retired Supreme Court judge to head the committee.²⁴² The committee also included computer security and forensic experts.²⁴³ In August 2022, the committee submitted its report to the Supreme Court but the Court did not release the

²³⁹ Code of Criminal Procedure, 1973, s. 92.

²⁴⁰ ‘Explained: The Findings of the Pegasus Committee, and What We Know about the Use of the Israeli Malware’ (*The Indian Express*, 25 August 2022) <<https://indianexpress.com/article/explained/explained-sci-tech/supreme-court-verdict-pegasus-spyware-case-explained-8110710/>> accessed 15 February 2023; Bilal Kuchay, ‘Pegasus Project: Is India “at Mercy of a Shady, Private Company”?’ *Al Jazeera* (20 July 2021) <<https://www.aljazeera.com/news/2021/7/20/pegasus-project-india-modi-treason-spyware-snooping-scandal>> accessed 28 March 2023; ‘India: Spyware Use Violates Supreme Court Privacy Ruling’ (*Human Rights Watch*, 26 August 2021) <<https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling>> accessed 28 March 2023.

²⁴¹ David Pegg and Sam Cutler, ‘What Is Pegasus Spyware and How Does It Hack Phones?’ *The Guardian* (18 July 2021) <<https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>> accessed 15 February 2023.

²⁴² *M L Sharma v Union of India* WP (Cri) 314 of 2021 (Supreme Court of India, 27 October 2021).

²⁴³ ‘Explained: The Findings of the Pegasus Committee, and What We Know about the Use of the Israeli Malware’ (n 240).

report to the public.²⁴⁴ According to media reports, the Union Government did not cooperate with the committee and insisted that all surveillance by Indian authorities complies with existing statutes such as the IT Act and Telegraph Act; however, the Government did not expressly deny the use of Pegasus.²⁴⁵

²⁴⁴ *ibid.*

²⁴⁵ *ibid.*

4. Impact of *Puttaswamy* on statutory surveillance framework

As set out above, India's statutory framework for surveillance facilitates interception through the Telegraph Act, the IT Act, and state criminal law statutes; it also facilitates information collection through the CrPC. Additionally, the license agreements executed between the government and TSPs and ISPs contractually obligate the latter to put in place the requisite infrastructure to conduct surveillance. However, with the advent of the Court's judgment in *Puttaswamy*, the constitutionality of some of these provisions may need to be re-considered.

With respect to some of these provisions, such as Section 5 of the Telegraph Act and Section 14 of the MCOCA, the Supreme Court has previously declared them to be constitutionally permissible interferences on privacy.²⁴⁶ However, with the decision of the nine-judge bench in *Puttaswamy*, two key changes have occurred. First, privacy has been categorically re-affirmed as fundamental right under the Constitution by a nine-judge bench of the Supreme Court, constituting controlling precedent. Second, the proportionality test discussed in Chapter 2 of this report is now the standard to evaluate the constitutionality of privacy infringing measures.

Thus, irrespective of whether a surveillance measure was upheld in the past, it remains an open question of law whether the measure continues to constitute a constitutionally permissible interference with privacy under current Supreme Court doctrine embodied by *Puttaswamy* and the *Aadhaar Judgement*. Additionally, any subsequent challenges to surveillance provisions must be examined through the lens of proportionality and *Puttaswamy* to arrive at a final determination of constitutionality.

This highlights the impact of *Puttaswamy* and the *Aadhaar Judgement*. For example, when the Union Government issued a notification authorising ten investigative agencies to conduct surveillance under Section 69 of the IT Act, multiple petitions were filed in the Supreme Court challenging the notification, Section 69 of the IT Act, and its corresponding IT Interception Rules.²⁴⁷ A petition was also filed challenging the surveillance framework for interception under Rule 419A of the Telegraph Rules.²⁴⁸ Key contentions in these petitions were that the statutory

²⁴⁶ *PUCL v Union of India* (1997) 1 SCC 301; *State of Maharashtra vs. Bharat Shantilal Shah* (2008) 13 SCC 5.

²⁴⁷ *Internet Freedom Foundation v Union of India* WP (C) 44 of 19; *M L Sharma v Union of India* WP (Cri) 1 of 2019.

²⁴⁸ *PUCL v Union of India* WP (C) 61 of 2019.

frameworks were now unconstitutional, and that the Court's judgment in PUCL affirming executive review of surveillance required reconsideration given the rulings in *Puttaswamy* and the *Aadhaar Judgment*.²⁴⁹ These petitions illustrate the importance of *Puttaswamy* and the *Aadhaar Judgment* in reshaping the conversation around privacy and surveillance.

It is worth noting that in its reply filed in these constitutional challenges, the Union Government filed a confidential standard operating procedure (SOP) that laid out the internal safeguards promulgated by the Union Home Ministry to be followed by investigative agencies when conducting surveillance.²⁵⁰ A response to a question in Parliament also indicated that the Department of Telecom has issued a SOP for TSPs.²⁵¹ However, reliance on such an SOP seems misconceived, given that it fails the legality test (which requires a publicly accessible law) and has no statutory basis under the Telegraph Act or the IT Act.²⁵²

In fact, it is a well settled principle of comparative law, including in judgments passed by the European Court of Human Rights (“**ECtHR**”) that laws must be clear, accessible, and foreseeable.²⁵³ The SOPs for surveillance are not publicly available and a Right to Information request for their disclosure was rejected on the ground that it would prejudicially affect the sovereignty and integrity of India and the security interests of the State.²⁵⁴

In this Chapter, we discuss the potential impact of *Puttaswamy* and the *Aadhaar Judgment* in reforming surveillance law. In particular, we examine whether: (i) current Supreme Court privacy doctrine necessitates a reconsideration of PUCL and the principles that should govern targeted interception; (ii) whether current Supreme Court privacy doctrine requires independent oversight of surveillance

²⁴⁹ Bhandari and Lahiri (n 4).

²⁵⁰ ‘Centre Defends Snooping Notification in the Supreme Court’ (*The Leaflet*, 11 March 2019) <<https://theleaflet.in/centre-defends-snooping-notification-in-the-supreme-court/>> accessed 14 February 2023.

²⁵¹ Minister of State in the Ministry of Home Affairs, Answer to Unstarred Question No 2593 (Rajya Sabha, 12 August 2015) <<https://www.mha.gov.in/MHA1/Par2017/pdfs/par2015-pdfs/rs-120815/2593.pdf>> accessed 31 May 2022.

²⁵² Internet Freedom Foundation, ‘IFF Files Rejoinder in PIL Seeking Surveillance Reform’ (*Internet Freedom Foundation*, 23 April 2019) <<https://internetfreedom.in/iff-files-rejoinder-in-pil-seeking-surveillance-reform/>> accessed 26 May 2022.

²⁵³ *Handyside v United Kingdom* App no 5493/72 (ECtHR, 7 December 1976) Office of the High Commissioner of Human Rights, ‘The right to privacy in the digital age’ A/HRC/27/37 (30 June 2014) [28]; Human Rights Commission, ‘Report of the Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism’ A/HRC/14/46 (17 May 2010) annex, [23].

²⁵⁴ *Virender Singh v CPIO, Ministry of Home Affairs* (2019) SCC Online CIC 8306.

action; and (iii) whether evidence obtained in violation of the law, or the Constitution, should be admissible in court following the decisions in *Puttaswamy* and the *Aadhaar Judgement*.

(a) Surveillance law after *PUCL*: A time for reconsideration

In its 1997 judgement in *PUCL*, the Supreme Court upheld the surveillance provisions under Section 5(2) of the Telegraph Act for two key reasons. First, the Court ruled that the guidelines provided by the Court would provide the necessary procedural safeguards for the exercise of interception powers under Section 5(2).²⁵⁵ These guidelines were subsequently given statutory force through amendments to the Telegraph Rules, specifically Rule 419A. Second, relying on the statutory text and the position in England at that time (under the Interception of Communications Act, 1985), the Court held that executive oversight of surveillance action satisfied the constitutional standard of ‘fair, just, and reasonable’ under Article 21 of the Indian Constitution.²⁵⁶

At the outset, the ‘just, fair and reasonable’ standard applied by the Supreme Court to interpret Section 5(2) of the Telegraph Act in *PUCL*²⁵⁷ is no longer the applicable constitutional standard to judge privacy infringements, with the Court in *Puttaswamy* categorially stating that infringements of privacy must satisfy the more rigorous test of proportionality.²⁵⁸ A key consequence of this is that the doctrine and guidelines set out by the Supreme Court in *PUCL* only satisfied the ‘just, fair and reasonable’ standard, but not necessarily the modern day proportionality standard. Thus, the principles regarding interception and surveillance set out in *PUCL* ought to be reconsidered, and the surveillance framework in the IT Act and the Telegraph Act needs to be tested against the four-part test laid out in *Puttaswamy* and the *Aadhaar Judgement*.²⁵⁹

The need to reconsider *PUCL* is further accentuated by how the understanding of the harms caused by surveillance in the digital age, and how this interacts with legal standards, has significantly evolved since 1997. For example, in *PUCL*, the Union Government contended that executive oversight over interception actions was sufficient by relying on the U.K.’s interception framework under the Interception of the Communications Act 1985.²⁶⁰ However, since *PUCL*, the U.K.

²⁵⁵ *PUCL v Union of India* (1997) 1 SCC 301 [34]-[35].

²⁵⁶ *PUCL v Union of India* (1997) 1 SCC 301 [33]-[34].

²⁵⁷ *PUCL v Union of India* (1997) 1 SCC 301 [30]-[34].

²⁵⁸ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [325].

²⁵⁹ *Bhandari and Lahiri* (n 4).

²⁶⁰ *PUCL v Union of India* (1997) 1 SCC 301 [33].

legislation has been held to be in violation of the European Convention of Human Rights,²⁶¹ and has also subsequently been replaced by the U.K. Parliament through the Regulation of Investigatory Powers Act 2000. The current position of law in the U.K. requires prior judicial scrutiny of interception warrants.²⁶²

Experience of the PUCL guidelines (subsequently incorporated within Rule 419A of the Telegraph Rules) has proven that at least some aspects of the Guidelines fail to meaningfully protect privacy. Namely, the three-member executive Review Committee (comprising of government officials) has failed to provide meaningful oversight over government surveillance.

In response to queries under the RTI Act in 2011, the Union Government disclosed that it issued between 7,500 and 9,000 interception orders every month.²⁶³ Given that the Review Committee only meets once every two months,²⁶⁴ it is effectively tasked with reviewing between 15,000-18,000 interception orders per meeting. As noted by the Srikrishna Committee on Data Protection, the large volume surveillance directions makes it “unrealistic” that the Committee can scrutinise interception orders in a manner that ensures the accountability of State surveillance.²⁶⁵ The experience of the Review Committee demonstrates how safeguards adopted by the Supreme Court in PUCL in 1997 may fail to adequately protect privacy in the modern day. Thus, it is time to reconsider the legal standards for targeted surveillance set out in PUCL.

261 *Liberty v United Kingdom* (2009) 48 EHRR 1, paras 16, 35, 43, 69.

262 Investigatory Powers Act 2016, s. 23 (U.K.).

263 Ministry of Home Affairs, ‘Application of Ms Shagun Belwal seeking information under the Right to Information Act, 2005’ dated 12 May 2014 <https://www.mha.gov.in/sites/default/files/RTI_ISIDiv_270814_0027_2081.PDF> accessed 31 May 2022; Vishwa Mohan, ‘Government Informs Rajya Sabha That on an Average 7500 - 9000 Orders for Interception (Telephone) Are Issued by the Centre Every Month.’ *The Times of India* (16 March 2011) <<https://timesofindia.indiatimes.com/government-informs-rajya-sabha-that-on-an-average-7500-9000-orders-for-interception-telephone-are-issued-by-the-centre-every-month-/articleshow/7719103.cms>> accessed 26 May 2022; Shyamlal, ‘9,000 Orders for Phone Interception Every Month: Govt’ (*The Indian Express*, 22 January 2012) <<https://indianexpress.com/article/india/politics/9-000-orders-for-phone-interception-every-month-govt/>> accessed 26 May 2022.

264 Indian Telegraph Rules, 1951, Rule 419A(17).

265 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, ‘A Free and Fair Digital Economy. Protecting Privacy, Empowering Indians’ (2018) 125 <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>. The Committee of Experts on a Data Protection Framework for India (chaired by Justice B.N. Srikrishna) was formed in August 2017 to examine issues related to data protection and draft a data protection bill. The Committee submitted its report on July 27, 2018.

(b) Independent oversight of surveillance action

The Court in *PUCL* refused to require prior judicial authorisation as a safeguard to interception, *inter alia* because the Telegraph Act made no mention of judicial authorisation.²⁶⁶ Instead, the Court opined that it was for the Union Government to promulgate rules governing the safeguards for interception.²⁶⁷ However, to view the Court's decision as an indication that the right to privacy does not require prior judicial authorisation for interceptions, or that a court cannot require prior judicial authorisations would be incorrect.²⁶⁸

Firstly, as noted in the previous section, the legal standard for evaluating the constitutionality of privacy-infringing measures has changed since *PUCL*, and it could be argued that the proportionality standard set out by *Puttaswamy* requires prior judicial authorisation (discussed below).

Second, the Court's reasoning against prior judicial authorisations in *PUCL* is contradictory, as none of the other procedural safeguards it set out (which were subsequently incorporated in Rule 419A of the Telegraph Rules) had any statutory basis either. Thus, the absence of a statutory provision envisaging prior judicial authorisation in the Telegraph Act need not have limited the Court in *PUCL* from requiring prior judicial authorisation.

Third, from a separation of powers perspective, it may not be appropriate for the Supreme Court to direct the Union Government to frame legislation that incorporates prior judicial authorisation for interceptions. However, if the Court finds that an interception regime only satisfies the proportionality test if it incorporates prior judicial authorisation, it is perfectly within the Court's power to invalidate provisions authorising interception that do not require prior judicial authorisation.

(i) Proportionality and judicial oversight

As discussed in Chapter 2, the test of proportionality is a conjunctive legal standard that requires the State to demonstrate that its privacy infringing measures satisfies the requirements of: (i) legality; (ii) a legitimate goal; (iii) suitability; (iv) necessity; (v) balancing; and (vi) procedural safeguards. Crucially, to satisfy the 'necessity' limb, there must not exist an alternative measure that while achieving the government's stated aim in a 'real and substantial manner', is less restrictive of individuals' rights. The existence of a lesser restrictive measure would lead to the impugned measure

²⁶⁶ *PUCL v Union of India* (1997) 1 SCC 301 [34].

²⁶⁷ *PUCL v Union of India* (1997) 1 SCC 301 [34].

²⁶⁸ Bhandari and Lahiri (n 4) 28.

failing the ‘necessity’ limb.

A ‘less rights-restrictive measure’ may be understood as an alternative to the *measure of interception*. Under this reading, the issue of necessity may centre on whether interception is only authorised when less restrictive measures are not available to investigators. However, one may also look at the issue of necessity more broadly, to scrutinise whether the impugned interception *process* (from authorisation to oversight) has failed to consider alternative measures that would be less rights restrictive, but equally effective. Such an approach neatly folds into the analysis of whether there exist sufficient procedural safeguards for rights-infringing measures.

Judicial authorisation for interception, either *ex-ante* or *ex-post*, represent an alternative measure that the government could adopt instead of executive oversight over interception. Given that judges independent of the executive are likely to provide greater scrutiny to interception orders than members of the executive itself, a judicial authorisation regime will likely result in fewer interceptions.

As noted by the ECtHR in *Klass vs. Germany*, judicial control offers the ‘best guarantees of independence, impartiality and a proper procedure’.²⁶⁹ This presumption is buttressed by the experience of the limited oversight provided by the existing Review Committee under the Telegraph Rules staffed solely by government officials. A parallel may also be drawn to the executive Review Committee that scrutinises government blocking orders against online content; disclosures under the RTI Act revealed that the Committee did not invalidate a single government blocking order between 2009 and 2022,²⁷⁰ suggesting executive oversight in India provided negligible protections for users’ rights.

Thus, even if judicial authorisation for interceptions results in a marginal increase in scrutiny, it represents a less rights-restrictive alternative measure to an interception regime operationalised entirely by the executive.²⁷¹ Finally, there is nothing to suggest that judicial authorisation would diminish the State’s capacity to achieve its investigatory or national security aims. Given the existence of a less rights-restrictive alternative, provisions authorising interception without requiring judicial authorisation may violate the necessity limb of the proportionality test and be rendered unconstitutional. Judicial authorisation would also represent a

²⁶⁹ *Klass v Germany* (1979-80) 2 EHRR 214, [49], [55].

²⁷⁰ Aarathi Ganesan, ‘Does This RTI Point to MeitY’s “rubber Stamp” Review Committee?’ (*MediaNama*, 11 August 2022) <<https://www.medianama.com/2022/08/223-meity-review-committee-not-one-69a-blocking-order-revoked/>> accessed 4 November 2022.

²⁷¹ Bhandari and Lahiri (n 4) 29.

valuable procedural safeguard.

There is some evidence that the Indian Supreme Court recognises the importance of independent judicial oversight over executive action when analysing the proportionality of a privacy infringing measure. In the *Aadhaar Judgment*, the Court struck down Section 33(2) of the Aadhaar Act which authorised the disclosure of biometric information and Aadhaar authentication records, pursuant to a direction by a Joint Secretary, in the interest of national security.²⁷² The holding *vis-à-vis* Section 33(2) was predicated on the fact that the provision did not require any independent (judicial) oversight of the important privacy-infringing powers given to the Joint Secretary, thus inadequately protecting the rights of individuals. The Court noted:

*Insofar as Section 33(2) is concerned, it is held that disclosure of information in the interest of national security cannot be faulted with. However, for determination of such an eventuality, an officer higher than the rank of a Joint Secretary should be given such a power. Further, in order to avoid any possible misuse, a Judicial Officer (preferably a sitting High Court Judge) should also be associated with. We may point out that such provisions of application of judicial mind for arriving at the conclusion that disclosure of information is in the interest of national security, are prevalent in some jurisdictions. In view thereof, Section 33(2) of the Act in the present form is struck down with liberty to enact a suitable provision on the lines suggested above.*²⁷³

The Constitution Bench of the Supreme Court clearly highlighted the need for judicial oversight over the disclosure of sensitive personal (biometric) data. Incidentally, following the judgment, the government amended Section 33(2) of the Aadhaar Act in 2019. However, it only substituted the word ‘Joint Secretary’ with ‘Secretary’, without introducing any provision for judicial oversight.²⁷⁴ This has been further challenged before the Supreme Court for violating the Court’s *Aadhaar Judgment* and failing to provide for judicial oversight for actions under Section 33(2).²⁷⁵ The litigation is currently pending.

Concerns regarding the lack of legislative or statutory interbranch oversight of

²⁷² K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1.

²⁷³ K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1 [513.6]

²⁷⁴ The Aadhaar and Other Laws (Amendment) Act, 2019, s. 14.

²⁷⁵ ‘SC Issues Notice On Plea Against Amendment Allowing Use Of Aadhaar Data By Private Entities’ (Live Law, 22 November 2019) <<https://www.livelaw.in/top-stories/sc-issues-notice-on-plea-against-amendment-allowing-private-entities-to-use-aadhaar-data-of-citizens-150046>> accessed 27 February 2023.

surveillance action in India have also been noted by the Srikrishna Committee on Data Protection as “not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in *Puttaswamy*, potentially unconstitutional.”²⁷⁶ After examining comparative models in other countries, the Committee noted that executive review alone ‘is not in tandem’ with comparative models of democratic nations.²⁷⁷

For instance, The U.K.’s Investigatory Powers Act, 2016 requires authorities to obtain a warrant from a competent authority, which must then be approved by an independent judicial commissioner.²⁷⁸ The Canadian Security Intelligence Service Act, 1984 also requires the issuance of warrants by a special set of judges for collection of information or intelligence about foreign individuals.²⁷⁹ Similarly, the United States also has special Foreign Intelligence Surveillance Courts that authorise the collection of foreign intelligence.²⁸⁰ Sweden’s Foreign Intelligence Court, comprising of two permanent judges and other members with a four year term, received approval from the ECtHR for being empowered as a judicial body to authorise the collection of signals intelligence.²⁸¹

Hence, the Srikrishna Committee recommended that the Union Government bring in a law that would ‘provide for both parliamentary oversight as well as judicial approval of all requests for non-consensual access to personal data.’ However, no such law has been introduced.

(ii) The positive case for judicial oversight

Independent of doctrinal considerations, there exist an independent substantive reason to provide judicial oversight for government interception and surveillance. Namely, the secret nature of surveillance, which makes it virtually impossible for an individual to know if and when they are placed under surveillance. Without the knowledge of having been placed under surveillance, there is no opportunity for the aggrieved individual to challenge the legality of the surveillance order. As Bhandari and Lahiri note:

By acknowledging the psychological restraints flowing from surveillance (as in the dissenting opinion in Kharak Singh), Puttaswamy implicitly recognises the dangers posed by the secret nature of State surveillance,

²⁷⁶ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 265) 127.

²⁷⁷ *ibid* 125.

²⁷⁸ Investigatory Powers Act 2016, s. 23 (U.K.).

²⁷⁹ Canadian Security Intelligence Service Act, 1984, Part II.

²⁸⁰ Foreign Intelligence Service Act 1978, s. 103 (U.S.).

²⁸¹ *Centrum för Rättvisa v Sweden* App No 35252/08 (ECtHR, 25 July 2021).

*which ensures that individuals have no way of knowing that they have been placed under surveillance. The apprehension that the government may be watching is enough to alter individual behaviour and reduce the ability for 'critical subjectivity', which is an essential part of democracy.*²⁸²

The situation is further exacerbated because TSPs, ISPs, and intermediaries have to maintain secrecy and confidentiality regarding the surveillance process,²⁸³ which makes it even more difficult to become aware of, and to challenge these orders in court. Thus, a mechanism to ensure independent judicial oversight prior to the authorisation of electronic surveillance against an individual will serve as an effective safeguard against the misuse of these powers, ensuring that the State's surveillance actions are at least subjected to some scrutiny.

For example, in *Big Brother Watch vs. the United Kingdom*, the Grand Chamber of the ECtHR noted that individuals who suspect their communications have been intercepted should have a remedy before “*a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, in so far as possible, an adversarial process.*”²⁸⁴ In this regard, it is noted that the Indian regime relies on the Review Committee, which is not independent of the executive, and individuals are not provided a hearing before the committee. In the absence of such an independent body, the need for judicial oversight is particularly pressing.

If the right to privacy is inhibited through secret surveillance action that has no prior or post judicial oversight, not only are the rights of individuals being violated, their right to seek constitutional remedies for such rights violations under Articles 32 and 226 of the Constitution is also being restricted, rendering such secret surveillance provisions open to a constitutional challenge.²⁸⁵

Without judicial oversight, even constitutional functionaries may be subject to electronic surveillance, without any checks outside the executive. This disproportionate exercise of power by one wing of the government not only impacts the vertical relationship between the citizen and the State, but also impacts the horizontal separation of power between the executive, legislature and judiciary.

²⁸² Bhandari and Lahiri (n 4).

²⁸³ Indian Telegraph Rules, 1951, Rule 419A(15); IT Traffic Data Rules, Rule 6; IT Interception Rules, Rule 25.

²⁸⁴ *Big Brother Watch v United Kingdom* App No 58170/30 (ECtHR, 25 May 2021) [359].

²⁸⁵ *Minerva Mills v Union of India* (1980) 2 SCC 591; *S P Sampath Kumar v Union of India* (1987) 1 SCC 124; *Kihoto Hollohan v Zachillhur* (1992) Supp (2) SCC 651 [120].

For these reasons, independent judicial oversight over the authorisation of surveillance will introduce accountability and due process within the surveillance framework. Additionally, it will also improve trust in the surveillance system, since any concerns that may arise around conflict of interest or lack of independence of an executive-oriented review committee will be suitably addressed.

(c) Illegally obtained evidence

A key issue concerning surveillance is the *consequence* of unlawful surveillance. As discussed in Chapter 3, several statutes that authorise interception also empower the government officials overseeing the surveillance to invalidate an interception or surveillance order and direct the destruction of the records. However, as also noted above, the scrutiny provided by the Review Committees is questionable. Further, because of the secret nature of surveillance, the individual under surveillance has no opportunity to contest the legality of the surveillance until trial, where the contents of surveillance are introduced against them as evidence.

The admissibility at trial of information collected pursuant to surveillance is a key check on surveillance. If evidence gathered through illegal surveillance is not admissible at trial, individuals can hold government surveillance practices accountable on a case-by-case basis. Over the longer term, the inadmissibility of illegally obtained evidence should also incentivise investigators to pursue lawful surveillance, with the goal of convictions at trial. Conversely, admitting evidence pursuant to unlawful surveillance may *incentivise* unlawful surveillance, as there are no legal consequences for conducting unlawful surveillance, only investigatory upside.

The Supreme Court of India has ruled that intercepted communications are admissible in a court of law as *res gestae*,²⁸⁶ if the communication is relevant (to the issue at hand), the voice (in case of a telephone conversation) identifiable, and accuracy of the intercepted communication is verifiable.²⁸⁷

Under Indian law, the primary rule for evaluating the admissibility of evidence is relevance.²⁸⁸ Hence, since as early as 1910, courts in India have been admitting illegally obtained evidence (or illegally intercepted evidence) as long as it is *relevant*.²⁸⁹ The only caution introduced by the Supreme Court in *R.M. Malkani vs.*

²⁸⁶ The Indian Evidence Act, 1872, s. 6. Statements that have been made contemporaneously with, or immediately after, an act by a person who themselves do not have first-hand knowledge of the act are an exception to the rule that hearsay evidence is inadmissible.

²⁸⁷ *R M Malkani v State of Maharashtra*, (1973) 1 SCC 471 [23]. Sen and others (n 222).

²⁸⁸ Indian Evidence Act 1872, s. 5.

²⁸⁹ *Barindra Kumar Ghose v Emperor* (1910) 37 ILR 467 (Cal).

State of Maharashtra is that a judge has the discretion to disallow admissibility of such evidence in a criminal trial if it would unfairly impact the fair trial of the accused.²⁹⁰

A Constitution Bench of the Supreme Court took the same view in *Pooran Mal vs. Director of Inspection*, where a tape recording of a conversation was held to be a relevant fact and admissible as evidence, with the Court observing, “the test of admissibility of evidence lies in relevancy, unless there is an express or necessarily implied prohibition in the Constitution or other law, evidence obtained as a result of illegal search or seizure is not liable to be shut out.”²⁹¹

As has been argued in detail by Bhandari and Lahiri, the foundation of this body of law “has been hollowed out by *Puttaswamy*.”²⁹² They rely on the fact that *Puttaswamy* expressly overruled the Supreme Court’s earlier decision in *M.P. Sharma* (which held that privacy was not a fundamental right). *M.P. Sharma* had been relied upon by the Constitution Bench in *Pooran Mal* to hold that illegally obtained evidence was admissible. Hence, post-*Puttaswamy*, the foundational basis for the *Pooran Mal* ruling on admissibility of illegally obtained evidence had been substantially undermined.

Further, *Puttaswamy* recognises *R.M. Malkani* as following the same line of reasoning as *Kharak Singh*, and the latter judgment was also expressly set aside by the Court since it did not acknowledge privacy as a protected constitutional right.²⁹³ After analysing each of these judgments in detail, Bhandari and Lahiri further argue that evidence obtained from surveillance conducted in violation of the right to privacy would be evidence collected in contravention of a constitutional right and should be excluded.²⁹⁴

This rationale was adopted by the 2019 judgment of the Bombay High Court in *Vinit Kumar vs. Central Bureau of Investigation*,²⁹⁵ where the Court held that the interception directions issued by the CBI under Section 5(2) of the Telegraph Act did not satisfy the *Puttaswamy* test of proportionality or the PUCL standard of ‘public emergency’ or ‘public safety’.²⁹⁶ The Court thus quashed the interception orders and directed the destruction of the evidence.²⁹⁷

²⁹⁰ *R M Malkani v State of Maharashtra* (1973) 1 SCC 471.

²⁹¹ (1974) 1 SCC 345 [24].

²⁹² Bhandari and Lahiri (n 4) 34.

²⁹³ *ibid.*

²⁹⁴ *ibid.*

²⁹⁵ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [42].

²⁹⁶ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [19].

²⁹⁷ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [43].

While deciding the course of action regarding evidence collected pursuant to illegal interception orders, the High Court observed that allowing illegally intercepted messages to be admissible will have the deleterious effects of promoting contempt for the law if messages intercepted under an order that does not have the sanction of law are allowed to be admitted as evidence, including matters involving the right to privacy under Article 21.²⁹⁸

Further, an ‘ends justify the means’ approach in the procurement of evidence for the administration of criminal law would amount to declaring that the government may violate any directions of the Supreme Court or mandatory statutory rules to secure evidence against the citizen, which would lead to manifest arbitrariness and disregard for the rule of law.²⁹⁹ As noted at the start of the section, admitting unlawfully gathered evidence at trial creates a situation where unlawful surveillance has investigatory upside but no legal consequences, potentially incentivising investigators to violate individuals’ privacy.

In reaching these conclusions, the High Court relied on the fact that the Supreme Court in *Puttaswamy* noticed that *R.M. Malkani* followed the same line of reasoning as *Kharak Singh*, which it overruled.³⁰⁰ The High Court also opined that *Pooran Mal* had no relevance since it did not involve a case where the executive was in breach of a fundamental right, or had breached the Court’s directions in *PUCL*, as had happened in *Vinit Kumar*.³⁰¹

Since the Telegraph Rules and the IT Interception Rules clearly authorised the Review Committee to direct the destruction of illegally obtained evidence in case of non-compliance with statutory provisions, the Court ordered the destruction of the illegal intercepts, thereby ensuring that the fundamental rights of the individual under surveillance were safeguarded.³⁰² The CBI has challenged the Bombay High Court’s judgment before the Supreme Court, which has stayed the operation of the High Court’s judgment, pending the final outcome of the appeal.³⁰³

²⁹⁸ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [42].

²⁹⁹ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [42]; Vasanth Rajasekaran and Reshma Ravipati, ‘Supreme Court Of India Applies The Doctrine of “Manifest Arbitrariness” to Strike Down Section 87 of the Arbitration Act’ (*Mondaq*, 5 December 2019) <<https://www.mondaq.com/india/trials-appeals-compensation/871672/supreme-court-of-ind305a-applies-the-doctrine-of-manifest-arbitrariness-to-strike-down-section-87-of-the-arbitration-act>> accessed 26 May 2022.

³⁰⁰ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [11].

³⁰¹ *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [39].

³⁰² *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [22].

³⁰³ *Central Bureau of Investigation v Vinit Kumar* SLP 902 of 2020 (Order dated 10 February 2020).

Slightly different observations were made by the Delhi High Court in *Deepti Kapur vs. Kunal Julka*.³⁰⁴ The High Court opined that where evidence is collected in breach of the fundamental right to privacy, the breach of the right alone would not render it inadmissible.³⁰⁵ Thus, while every litigating party had a right to privacy, it must yield to the opposite side being given a fair chance to bring relevant evidence to court.³⁰⁶ In reaching its conclusion, the Court relied on *Pooran Mal* and held that evidence is admissible as long as it is relevant.³⁰⁷

This case, however, differs significantly from *Vinit Kumar* as it involved a marital dispute, where the husband had recorded a private conversation between his wife and her friend, where she was speaking in a derogatory manner about him and his family. Hence, both these judgments may be reconciled since *Deepti Kapur* concerned the *horizontal* application of privacy (between two individuals), whereas *Vinit Kumar* involved a more traditional vertical application of the privacy doctrine (concerning the illegal use of State power against its citizens).

There is thus a strong case to require that illegally obtained evidence should not be admitted as evidence during trial, and that the doctrinal basis for its admissibility has been substantially undermined after the judgment of the Supreme Court in *Puttaswamy*. Further, the exclusion of illegally obtained evidence may also help shape the conduct of investigative agencies, and ensure strict compliance with the letter and spirit of the legal processes governing surveillance.³⁰⁸

Admissibility of evidence under the UAPA and organised crime statutes

The Unlawful Activities Prevention Act, 1967 (“**UAPA**”) is a *sui-generis* anti-terror law that applies across India. Section 46 of the UAPA provides for the admissibility in court of any evidence procured through interception of communication under the Telegraph Act, IT Act, or any other law in force, notwithstanding any provisions contained in the Indian Evidence Act, 1872 (“**Evidence Act**”).

Under the Evidence Act, as discussed above, even illegally obtained evidence can be admitted in trial as long as it meets the Evidence Act’s standards of ‘relevance’. However, under the UAPA, even this minimal threshold of ‘relevance’ need not be satisfied when seeking to admit intercepted communications as evidence.

³⁰⁴ (2020) SCC Online Del 672.

³⁰⁵ *Deepti Kapur v Kunal Julka* (2020) SCC Online Del 672 [22].

³⁰⁶ *Deepti Kapur v Kunal Julka* (2020) SCC Online Del 672 [23].

³⁰⁷ *Deepti Kapur v Kunal Julka* (2020) SCC Online Del 672.

³⁰⁸ Rishab Bailey and others, ‘Use of Personal Data by Intelligence and Law Enforcement Agencies’ (National Institute of Public Finance and Policy 2018) <<https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf>>.

Section 46 of the UAPA allows the admissibility of intercepted communication in court as long as the order to conduct such interception is shared with the accused at least ten days before the hearing. The judge can waive even this period if they conclude that the accused would not be prejudiced by failing to receive notice of the order.

Section 46 of the UAPA thus makes a key departure from India's previous (since-repealed) terrorism legislation, the Prevention of Terrorism Act, 2002. Under the 2002 Act, the accused was provided with a copy of the competent authority's interception order as well as the investigating agency's application for such order.³⁰⁹ However, under the UAPA, the accused is not provided with a copy of the application accompanying the interception request. Thus, the rights of the accused may be (legally) curtailed during trial, as it is more difficult to challenge the legality of the interception request.³¹⁰ Although there has been a reported rise in the number of cases registered under the UAPA,³¹¹ there is no publicly available data on the use of Section 46 specifically.

Similarly, under the MCOCA, the Karnataka Control of Organised Crime Act, 2000, and the Gujarat Control of Terrorism and Organised Crime Act, 2015, the evidence gathered through interception is admissible at the time of trial, provided that the contents of the intercepted communication are given to the accused ten days before the relevant hearing.³¹² As in the UAPA, this time period can be waived by the judge if they conclude that the accused would not be prejudiced by failing to receive notice of the order.³¹³

(d) Post-*Puttaswamy* reforms to surveillance

As mentioned in Chapter 3, petitions challenging the constitutionality of Section 5(2) of the Telegraph Act and Section 69 of the IT Act are pending before the

³⁰⁹ Prevention of Terrorism Act, 2002, s. 45

³¹⁰ Sen and others (n 222) 80.

³¹¹ IndiaSpend, 'Story in Numbers: Pending Cases under UAPA on the Rise, Shows Data' *Business Standard India* (22 November 2021) <https://www.business-standard.com/article/current-affairs/story-in-numbers-pending-cases-under-uapa-on-the-rise-shows-data-121112200046_1.html> accessed 26 May 2022; 'Parliament Proceedings | Over 72% Rise in Number of UAPA Cases Registered in 2019' *The Hindu* (New Delhi, 9 March 2021) <<https://www.thehindu.com/news/national/parliament-proceedings-over-72-rise-in-number-of-uapa-cases-registered-in-2019/article34029252.ece>> accessed 26 May 2022.

³¹² MCOCA, s. 14(13); Karnataka Control of Organised Crime Act, 2000, s. 14(13); Gujarat Control of Terrorism and Organised Crime Act, 2015, s. 14.

³¹³ MCOCA, s. 14(13); Karnataka Control of Organised Crime Act, 2000, s. 14(13); Gujarat Control of Terrorism and Organised Crime Act, 2015, s. 14.

Supreme Court.³¹⁴ The decision of the Supreme Court in these surveillance challenges, and its treatment of the decisions in *Puttaswamy* and the *Aadhaar Judgment*, will have significant repercussions on the legal framework for surveillance currently in place in India.

The state of our surveillance framework was also under active consideration by a technical committee constituted by the Supreme Court to investigate allegations that the Indian Government utilised the ‘Pegasus’ spyware against Indian citizens.³¹⁵ Apart from being tasked with investigating and determining the use of the Pegasus spyware on the phones of Indian citizens, the committee’s terms of reference also include making recommendations “*regarding enactment or amendment to existing law and procedures surrounding surveillance and for securing improved right to privacy.*”³¹⁶ While the committee submitted its report to the Supreme Court in 2022, at the time of writing, the report has not been released to the public.³¹⁷

From the discussion in the previous section, it is clear that post-*Puttaswamy*, the statutory surveillance framework should be amended to introduce judicial oversight over the authorisation of surveillance action, and that the Evidence Act should be amended to bar the admissibility of evidence obtained through illegal surveillance. Similarly, certain measure such as the ‘traceability’ mandate in Rule 4(2) of the Intermediary Guidelines 2021, that likely violate the proportionality test, ought to be withdrawn or struck down by courts.³¹⁸

In addition to the above conclusions, we believe that certain other amendments should be made to the text of the Telegraph Act and the IT Act. These include:

1. Foregoing the ‘expediency’ test

Both the Telegraph Act and the IT Act state that surveillance can only be authorised when it is ‘necessary or expedient’ to do so for reasons such as national security, public order, friendly relations with foreign states, etc.³¹⁹ Similarly, Clause

³¹⁴ *Internet Freedom Foundation v Union of India* WP (C) 44 of 19; *PUCI v Union of India* WP (C) 61 of 2019; *M L Sharma v Union of India* WP (Cri) 1 of 2019

³¹⁵ *M L Sharma v Union of India* WP (Cri) 314 of 2021 (Order dated 27 October 2021).

³¹⁶ *M L Sharma v Union of India* WP (Cri) 314 of 2021 (Order dated 27 October 2021).

³¹⁷ ‘Pegasus Probe Committee Report To Remain Sealed In Supreme Court’ (*Live Law*, 25 August 2022) <<https://www.livelaw.in/top-stories/breaking-pegasus-probe-committee-report-to-remain-sealed-in-supreme-court-207519>> accessed 15 February 2023.

³¹⁸ *Nojeim and Maheshwari* (n 201); *Grover, Rajwade and Katira* (n 201); *Devadasan* (n 187).

³¹⁹ Indian Telegraph Act 1885 s. 5(2); Information Technology Act, 2000, s. 69(1).

18 of the Digital Personal Data Protection Bill 2022 (“**DPDP Bill**”) released by MEITY provides broad exemptions from the Bill’s rigours for the purposes of preventing, detecting, or investigating the “contravention of any law.”³²⁰

Further, under Clause 18(2) of the DPDP Bill, the Union Government may exempt any “instrumentality of the State” from complying with the entire data protection framework in the interests of the sovereignty, integrity, security of India, its relations with foreign State, the maintenance of public order, or the incitement of an offence in relation to these categories.

As per *Puttaswamy*, any restrictions on fundamental rights can be justified only if they are necessary, i.e., the least restrictive alternative among equally effective alternatives. The requirement for necessity is present in Section 5(2) of the Telegraph Act and Section 69(1) of the IT Act. However, in both provisions it is coupled with a much lower threshold, that of ‘expediency.’

The continuation of the ‘expedient’ test to authorise surveillance can be challenged. The expedience test can easily devolve into a simple convenience, test based on the needs and requirements of the State, rather than a comprehensive assessment of potential alternatives to surveillance.³²¹

Safeguards introduced in the Telegraph Rules and the IT Interception Rules, requiring that the competent authority consider alternative means in acquiring the information, can easily be sidestepped by citing the legislative requirement of ‘expediency.’ Further, as discussed above, there is little oversight as to whether investigators engage in considering alternatives in practice. Thus, the term ‘expedient’ should be removed, and surveillance should only be authorised when “necessary”.

2. Removing the additional grounds under the IT Act

Another recommendation to amend the statutory text relates to the substantive grounds on which electronic surveillance is authorised under Section 69 of the IT Act. The 2009 amendment to Section 69 of the IT Act introduced two additional grounds on which surveillance may be authorised, ‘defence of India’ and ‘investigation of any offence’, which were not present in the Telegraph Act.

³²⁰ Digital Personal Data Protection Bill, 2022 <<https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>>.

³²¹ Vrinda Bhandari, Smriti Parsheera and Faiza Rahman, ‘Comments on the Draft Personal Data Protection Bill, 2019’ (*The Leap Blog*, Winter 2020) <<https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data.html>> accessed 26 May 2022.

The latter ground empowers the government to conduct surveillance of a large swathe of the population under the pretext of ‘investigation of *any* offence’. It makes no distinction based on the nature or severity of the offence, theoretically permitting surveillance even for minor offences, where surveillance may not be necessary. This is in direct contradiction to the standard of proportionality set out in *Puttaswamy*. This also raises issues of legality, as citizens cannot reasonably discern what types of conduct may result in them being subjected to surveillance. Thus, this ground may also be subject to a constitutional challenge, and may be struck down.

3. Improving the transparency and reporting requirements for investigative agencies

Although not directly related to the statutory surveillance framework, any reforms to surveillance should include improving transparency and reporting requirements of investigative agencies. Based on information available in the public domain, these agencies currently function under minimal accountability or supervision.

Such requirements can range from requiring agencies to proactively disclose the extent of surveillance conducted during a calendar year to publishing annual reports about their activities (after redacting any sensitive material). Additionally, data protection norms such as fairness in processing and data retention, purpose limitation, security safeguards, and grievance redressal should also be built into the functioning of agencies conducting surveillance.³²²

If accepted, these recommendations will go a long way in modernising India’s targeted surveillance framework and improving the transparency and accountability in the functioning of investigative agencies.

³²² Bailey and others (n 308) 34.

5. Mapping India's modern surveillance programs

The advancement of technology has considerably expanded the modes and methods of surveillance, and enabled governments to shift from *targeted* surveillance to *mass* surveillance. Mass surveillance is commonly understood as 'passive' or 'undirected' surveillance.³²³ It is not targeted at any particular person, but rather it collects data for future use.³²⁴ Carrying out mass surveillance is justified by governments as necessary to empower them to combat the myriad threats posed by criminal and terrorist organizations, that have benefited from sophisticated technologies, and can cause harm to society in novel, unpredictable, and undetectable ways.³²⁵

Courts across the world are grappling with questions pertaining to the legality of mass surveillance, the modes and methods through which it is carried out, and its impact on human rights such as the rights to privacy, expression, speech, and association. The Grand Chamber of the ECtHR in *Big Brother* gave a significant decision ruling that bulk interception regimes are not illegal *per se* if:

1. they incorporate 'end-to-end' safeguards which assess the necessity and proportionality of the collection at each stage of the surveillance;
2. the object and scope of the surveillance are subject to independent authorisation; and
3. the surveillance operation is subject to independent ex-post scrutiny.³²⁶

Other aspects of mass surveillance that are highly relevant include whether they follow data retention policies that lay down how long the data is retained for, as held in *Digital Rights Ireland*,³²⁷ and whether there are adequate safeguards

³²³ House of Lords, 'Surveillance: Citizens and the State - Constitution Committee (Chapter 2)' (*Parliament.uk*) <<https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm>> accessed 26 May 2022.

³²⁴ *ibid.*

³²⁵ Kevin Macnish, 'Justifying Surveillance' (*E-International Relations*, 20 January 2015) <<https://www.e-ir.info/2015/01/20/justifying-surveillance/>> accessed 26 May 2022.

³²⁶ *Big Brother Watch v United Kingdom* App No 58170/30 (ECtHR, 25 May 2021) [350].

³²⁷ Case C-293/12 *Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources* [2014] ECR I-238, [63]. The Court of Justice for the European Union (CJEU) ruled that retention of data beyond six months would be considered disproportionate.

regarding its availability, integrity and confidentiality.

In India, the major surveillance programs include the Central Monitoring System (“**CMS**”) that automates interception;³²⁸ the National Intelligence Grid (“**NATGRID**”), which is an integrated intelligence grid; and Network Traffic Analysis (“**NETRA**”), a dragnet system that identifies and collects electronic communications.³²⁹

Reports also indicate that the police in several states have begun deploying facial recognition technologies³³⁰ and drones³³¹ as aids for law enforcement. None of these programs, which have come into force after the 26/11 Mumbai attacks, have been deployed based on any specific legislative authority. Post *Puttaswamy*, the legality of the CMS, NATGRID, and NETRA has been challenged before the Delhi High Court for infringing the rights of individuals without any statutory basis.³³² The case is currently pending before the High Court.

While the CMS and NETRA involve primary data collection, programs such as NATGRID, the Crime and Criminal Tracking Network System (“**CCTNS**”), and the use of facial recognition technology on CCTV feeds are aimed at centralising and streamlining existing databases of information on individuals. Similarly, we have seen the proliferation of digital IDs in India as well. From Aadhaar (a biometric and digital ID) to the National Health Stack, the National E-Transport Project, and DigiYatra, the government has been increasingly collecting sensitive personal data about its citizens and creating more detailed profiles. This highlights the need for effective data protection legislation.

While these programs are essentially welfare schemes aimed at improving electronic governance, insofar as they increase governmental access to personal data, they present surveillance risks. These schemes also raise data access and purpose limitation concerns vis-à-vis the personal data of individuals.

³²⁸ Prakash (n 12).

³²⁹ ‘Govt to Launch Internet Spy System “Netra” Soon’ (n 12).

³³⁰ Internet Freedom Foundation, ‘Panoptic Tracker’ (*Panoptic*) <<https://panoptic.in>> accessed 26 May 2022.

³³¹ Aihik Sur, ‘Telangana Police Using Drones, in Some Cases with Sirens, to Identify Lockdown Violators’ (*MediaNama*, 26 May 2021) <<https://www.medianama.com/2021/05/223-telangana-drones-lockdown/>> accessed 26 May 2022; Shilpa Nair Anand, ‘COVID-19: Kerala Police Uses Drones to Keep an Eye on Those Who Flout the Lockdown’ *The Hindu* (Kochi, 13 April 2020) <<https://www.thehindu.com/society/kerala-polices-project-eagle-eye-uses-close-to-350-drones-to-track-those-flouting-the-rules-of-lockdown/article31331170.ece>> accessed 26 May 2022.

³³² *CPIIL v Union of India* WP (C) 8998 of 20 (High Court of Delhi); Software Freedom Law Centre, ‘Legal Challenge by CPIIL and SFLC.IN to Surveillance Projects CMS, NATGRID and NETRA’ (*SFLC.in*, 24 March 2022) <<https://sflc.in/legal-challenge-cpil-and-sflcin-surveillance-projects-cms-natgrid-and-netra>> accessed 26 May 2022.

While data sharing programs raise significant privacy concerns, the scope of the present report is limited to surveillance systems that facilitate primary data collection through interception and monitoring of communications. Thus, the CMS and NETRA are analysed in this Chapter, and information regarding India's remaining programs is set out as an Annexure to the present report.

(a) Centralised Monitoring System

Surveillance under the Telegraph Act and IT Act is targeted, and requires specific written and reasoned orders authorising interception, that must be complied with by ISPs, TSPs, and intermediaries. Investigative agencies must approach individual TSPs for interception of communication. There are thus some, albeit limited, statutory safeguards to regulate the conduct of surveillance and safeguard privacy. Based on the limited information available regarding the CMS, it does not appear to constitute a dragnet program that intercepts all communications, but rather the CMS automates existing targeted interception.³³³ However, as discussed below, the manner of this automation risks circumventing the minimal safeguards provided in the Telegraph and IT Acts.

In 2009, the Government of India announced that it was establishing a centralised system to automate interceptions on mobile phones, landlines, and the internet (including social media engagement) in the country, called the Centralised Monitoring System.³³⁴ The CMS was developed by the Centre for Development of Telematics, the research and development wing of the Department of Telecommunication. Public documents reveal that the CMS was approved by the Cabinet Committee on Security in 2011, with estimated government funding of Rs. 4 billion.³³⁵

The CMS was planned to require minimum manual intervention, being capable of 'instantaneous' interception, with direct electronic provisioning of target

³³³ Press Information Bureau, 'Centralised System to Monitor Communications' (Press Information Bureau, 26 November 2009) <<https://pib.gov.in/newsite/PrintRelease.aspx?relid=54679>> accessed 26 May 2022; Anurag Kotoky, 'India Sets up Elaborate System to Tap Phone Calls, e-Mail' Reuters (20 June 2013) <<https://www.reuters.com/article/us-india-surveillance-idUKBRE95J05G20130620>> accessed 26 May 2022.

³³⁴ Press Information Bureau, 'Centralised System to Monitor Communications' (n 333); Kotoky (n 333).

³³⁵ Sounak Mitra, 'CCS Nod for Telecom Testing and Security Certification Centre' *Business Standard India* (11 February 2013) <https://www.business-standard.com/article/economy-policy/ccs-nod-for-telecom-testing-and-security-certification-centre-113021101330_1.html> accessed 26 May 2022. Minister of Communications and Information Technology, 'Answer to Unstarred Question No 595' (Lok Sabha, 2 December 2015) <<http://164.100.24.220/loksabhaquestions/annex/6/AU595.pdf>> .

numbers by authorised agencies, without requiring any manual intervention from TSPs.³³⁶ Thus, the investigators could monitor their target through a centralised system, without approaching the TSPs. It establishes a secure flow of intercepted communication on a ‘near real-time basis’ between investigative agencies and TSPs on a secured and dedicated CMS network.

Public documents state its features also included filters and alerts being created on target telephone numbers, and data mining of Call Data Records (“**CDRs**”) to identify call and location details of the target telephone numbers.³³⁷ The analysis of CDRs is to help establish the links between ‘anti-social’ or ‘anti-national’ elements.³³⁸ The CMS has regional and central hubs, established to help both Union and state investigative agencies intercept and monitor communications in ‘serious’ or ‘desirable’ cases of national security or connected matters.³³⁹ The data collected by the CMS includes mobile numbers, time, data, and duration of interception, location of target subscribers, data regarding failed call attempts.³⁴⁰ Media reports also state that the CMS will facilitate real-time access to SMS, fax, web-site visits, social media usage, internet search, and email of unencrypted communications of surveillance targets through direct access of TSP and ISP networks.³⁴¹ While details regarding the exact operation of the CMS are scarce, if it automatically collects data beyond individual interceptions, it may have mass surveillance capabilities.³⁴²

To operationalise the CMS, the government amended the Unified License for TSPs (“**UL**”) in 2013, requiring the licensees’ to collect and forward the data gathered through their ‘Lawful Interception Systems’ to the ‘Interception Store and Forward’

336 Press Information Bureau, ‘Centralised System to Monitor Communications’ (n 333).

337 *ibid.* Ministry of Communications and Information Technology, ‘Answer to Unstarred Question No 1714’ (Lok Sabha, 4 May 2016) <<http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=33952&lsno=16>> accessed 31 May 2022.

338 Ministry of Communications and Information Technology, ‘Answer to Unstarred Question No 629’ (Lok Sabha, 7 August 2013) <<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=143964&lsno=15>> accessed 31 May 2022.

339 Ministry of Communications and Information Technology, ‘Answer to Unstarred Question No 1714’ (Lok Sabha, 4 May 2016) <<http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=33952&lsno=16>> accessed 31 May 2022.

340 Ministry of Communications and Information Technology (Department of Telecommunications), ‘Amendment to Unified License agreement regarding Central Monitoring System’ dated 11 October 2013 <<https://dot.gov.in/sites/default/files/DOC231013.pdf?download=1>> accessed 31 May 2022.

341 Shalini Singh, ‘India’s Surveillance Project May Be as Lethal as PRISM’ *The Hindu* (20 June 2013) <<https://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece>> accessed 28 March 2023; Prakash (n 12).

342 ‘Watch the Watchmen Series Part 2 : The Centralised Monitoring System’ (Internet Freedom Foundation, 14 September 2020) <<https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/>> accessed 9 January 2021.

servers that would be installed in their premises.³⁴³ These servers are connected to the CMS at regional and central databases (Regional Monitoring Centres), allowing investigative agencies direct access to all data intercepted by TSPs' 'Lawful Interception Systems'.³⁴⁴

The following language was added to Chapter VIII (relating to Access Service) in the UL:³⁴⁵

But in the case of a centralised monitoring system (CMS), the licensee shall provide connectivity up to the nearest point-of-presence of the multi-protocol label switching (MPLS) network of the CMS, at its own cost, in the form of dark optical fibre with redundancy. [...] From the point of presence of the MPLS network of the CMS, onward traffic will be handled by the government at its own cost.

These changes, and the entire rationale behind CMS, was to “automate” the process of lawful interception and monitoring of communications.³⁴⁶ Thus, communications intercepted by TSPs will be automatically routed to the Regional Monitoring Centres and automatically transmitted to the CMS, where communications will be collected for real time access.³⁴⁷

343 Ministry of Communications and Information Technology (Department of Telecommunications), 'Amendment to Unified License agreement regarding Central Monitoring System' dated 11 October 2013 <<https://dot.gov.in/sites/default/files/DOC231013.pdf?download=1>> accessed 31 May 2022.

344 PTI, 'Govt Setting up Monitoring System to Intercept Data: Ravi Shankar Prasad' *mint* (4 May 2016) <<https://www.livemint.com/Politics/CdtkNPkBf5umcVrTOYZ4GP/Govt-setting-up-central-monitoring-system-to-intercept-data.html>> accessed 26 May 2022; PTI, 'Government Setting up Centralised Monitoring System for Lawful Interception: Ravi Shankar Prasad' *The Economic Times* (4 May 2016) <<https://economictimes.indiatimes.com/news/economy/policy/government-setting-up-centralised-monitoring-system-for-lawful-interception-ravi-shankar-prasad/articleshow/52111222.cms>> accessed 26 May 2022.

345 Ministry of Communications and Information Technology (Department of Telecommunications), 'Amendment to Unified License agreement regarding Central Monitoring System' dated 11 October 2013 <<https://cis-india.org/internet-governance/blog/uas-license-agreement-amendment>> accessed 28 March 2023.

346 Ministry of Communications and Information Technology (Department of Telecommunications), 'Central Monitoring System' dated 2 December 2015 <<http://164.100.24.220/loksabhaquestions/annex/6/AU595.pdf>> accessed 16 February 2023.

347 Maria Xynou, 'India's Central Monitoring System (CMS): Something to Worry About?' (*The Centre for Internet and Society*, 30 January 2014) <<https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about>> accessed 10 February 2021; Sharad Vyas, 'Police Lack Technology Tools to Connect the Call Dots' *The Hindu* (Mumbai, 24 January 2016) <<https://www.thehindu.com/news/national/Police-lack-technology-tools-to-connect-the-call-dots/article14016306.ece>> accessed 9 January 2021.

The technology development and pilot trials of CMS have been completed, and CMS is being operationalised in different parts of the country, with ‘most of the Union investigative agencies and some of the State police’ being onboarded to the CMS network.³⁴⁸

The automation of the existing interception process under the CMS, the centralised access to all intercepted data with the CMS Authority, and the removal of the manual intervention by TSPs and ISPs may all be causes for concern. As many researchers and activists have pointed out, CMS departs from the Telegraph Act, because it facilitates automatic transmission of data to its data centres, without the TSP’s designated officers necessarily being informed about the same.³⁴⁹ This means that the government can access intercepted communication at a given instance, even without the knowledge of the TSPs.³⁵⁰ This results in the omission of an important potential safeguard, where someone outside of the government has actual knowledge of the surveillance being conducted, potentially making interceptions less transparent.³⁵¹

The government has stated that a review committee, similar to the one constituted under Rule 419A of the Telegraph Rules, is ‘applicable to interception under the CMS project’, and there is a built-in mechanism for checks and balances since the investigatory agencies “cannot provision the target and the provisioning agency cannot see the content.”³⁵² In response to parliamentary questions, the Government has also stated that the CMS generates an audit trail of command logs that can be examined in case of misuse.³⁵³ However, in the absence of any statute providing such safeguards, it may be difficult to secure transparency and ensure accountability. The less transparent surveillance is, the harder it is to identify illegal surveillance.

³⁴⁸ Centre for Development of Telematics, ‘Annual Report 2019-2020’ 4 <https://www.cdote.in/cdotweb/assets/docs/annualReports/ANNUAL_REPORT_2019-20.pdf> accessed 26 May 2022.

³⁴⁹ Prakash (n 12); Singh (n 341).

³⁵⁰ Xynou (n 347); Addison Litton, ‘The State of Surveillance in India: The Central Monitoring System’s Chilling Effect on Self-Expression’ (2015) 14 *Global Perspectives on Colorism* (Symposium Edition) 799.

³⁵¹ Litton (n 350) 808; Chris Sheehy, ‘Defining Direct Access: GNI Calls for Greater Transparency and Dialogue around Mandatory, Unmediated Government Access to Data’ (*Global Network Initiative*, 3 June 2021) <<https://globalnetworkinitiative.org/defining-direct-access-2/>> accessed 15 February 2023.

³⁵² Ministry of Communications and Information Technology, ‘Answer to Unstarred Question No 629’ (Lok Sabha, 7 August 2013) <<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=143964&lsno=15>> accessed 31 May 2022.

³⁵³ Jaideep Reddy, ‘The Central Monitoring System and Privacy: Analysing What We Know So Far’ (2014) 10 *Indian Journal of Law and Technology* 13.

(b) Network Traffic Analysis

NETRA is an internet surveillance system prepared by the Centre for Artificial Intelligence and Robotics, a department under the Defence Research and Development Organization. It is designed to intercept, analyse, and detect pre-defined keywords in internet traffic in real time. Simply put, it filters internet content for specific words such as ‘bomb’, ‘kill’, ‘terrorist’ and ‘attack’, among others, and then alerts relevant agencies.³⁵⁴

NETRA’s sources of data can include content published on social media platforms such as Twitter and Facebook, as well as content transmitted through emails, blogs, and instant messaging services (although it is unlikely to be able to access end-to-end encrypted messaging services).³⁵⁵ It has reportedly been used by the Research & Analysis Wing to intercept and monitor global internet traffic to India.³⁵⁶ Besides this, very little information about NETRA is publicly available. However, to the extent it indiscriminately trawls internet traffic to pull up data, it is a dragnet mass surveillance system.

³⁵⁴ Bailey and others (n 308); Kalyan Parbat, ‘Government to Launch “Netra” for Internet Surveillance’ *The Economic Times* (16 December 2013) <<https://economictimes.indiatimes.com/tech/internet/government-to-launch-netra-for-internet-surveillance/articleshow/27438893.cms?from=mdr>> accessed 26 May 2022.

³⁵⁵ Parbat (n 354).

³⁵⁶ Amitav Ranjan, ‘Home Seeks System to Intercept Net Chatter - Indian Express’ (*Indian Express*, 23 June 2013) <<http://archive.indianexpress.com/news/home-seeks-system-to-intercept-net-chatter/1132688>> accessed 26 May 2022.

6. Testing modern surveillance programs against *Puttaswamy*

The legislative framework for surveillance explained in Chapter 3 consists of legislation that has been sporadically updated with rules and regulations, in an attempt to meet the needs of technology and modern society. It is not conceivable that at the time it was enacted, legislation such as the Telegraph Act (1885) or even the IT Act (2000) was intended to enable modern surveillance systems with mass surveillance capabilities. However, the executive authorisation and deployment of newer surveillance programs which may facilitate the practice of mass surveillance has increased in the last decade.

In this chapter, we examine the potential impact of *Puttaswamy* on the legality of India's modern surveillance projects. This will be done by mapping these surveillance projects against the tests of legality, legitimate aim and suitability, necessity and proportionality, and procedural safeguards articulated in *Puttaswamy* and the *Aadhaar Judgment*.

(a) Legality

The threshold of legality requires that any action by the government that restricts fundamental rights must take place within a defined regime of law, i.e., there must be an anchoring legislation, with a clear set of provisions. Thus, executive action that operates to the prejudice of an individual must be authorised by and in accordance with law.³⁵⁷ A consistent line of decisions by international human rights bodies have also determined that surveillance should be authorised, sanctioned or backed by a specific law,³⁵⁸ and countries have followed suit.³⁵⁹

The law should also be clear and publicly accessible, and should enable citizens to

³⁵⁷ *State of MP v Thakur Bharat Singh* (1967) 2 SCR 454; *Bijoe Emmanuel v State of Kerala* (1986) 3 SCC 615; *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

³⁵⁸ *The Sunday Times v United Kingdom* App No 6538/74 (ECtHR, 26 April 1979), [49]; Advisory Opinion OC-6/86 The Word "Laws" in Article 30 of the American Convention on Human Rights (1986).

³⁵⁹ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) Act of 2001 (U.S.)*; *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (U.S.)*; *Investigatory Powers Act 2016 (U.K.)*; *Intelligence and Security Act 2017 (New Zealand)*.

be able to foresee behaviour that would be sanctioned.³⁶⁰ It is important to ensure that the law meets the accessibility and foreseeability standard of legality. All the rules, guidelines, or procedures framed under the laws should be clear.

In situations where the law is itself complex and may not satisfy the requirements of clarity, guidance or rules clarifying its provisions could be accepted as meeting this requirement. For instance, the bulk surveillance regime in the U.K. was upheld partially in *Big Brother*, since there was a clear legislative and foreseeable basis for bulk interception regimes. Although the ECtHR noted that the U.K.'s RIPA is an 'unnecessarily complex' piece of legislation, it acknowledged the guidance to the RIPA's provisions provided by the Interception of Communications Code of Practice, which clarified how the bulk surveillance regime operated in practice.³⁶¹ After noting that the said Code was a public document that was approved by both Houses of Parliament and was published online, the Court accepted that the RIPA's provisions were adequately accessible.³⁶²

Surveillance through the CMS and NETRA have been granted approval by executive action through Cabinet Committees, rather than by a parliamentary statute,³⁶³ and have been challenged before the Delhi High Court for this lack of anchoring legislation.³⁶⁴ These programs do not find mention in any legislation or rules, with the CMS only mentioned in the contractual terms of the licenses between the ISPs and TSPs and the government. The Union Government has taken the view that these surveillance projects protect privacy through the extant legal regime under

³⁶⁰ Office of the High Commissioner of Human Rights, 'The right to privacy in the digital age' A/HRC/27/37 (30 June 2014) [28]; Human Rights Committee, 'Report of the Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' A/HRC/14/46 (17 May 2010) annex, [23].

³⁶¹ *Big Brother Watch v United Kingdom* App No 58170/30 (ECtHR, 25 May 2021) [366].

³⁶² *Big Brother Watch v United Kingdom* App No 58170/30 (ECtHR, 25 May 2021) [366].

³⁶³ Sounak Mitra, 'CCS Nod for Telecom Testing and Security Certification Centre' *Business Standard India* (11 February 2013) <https://www.business-standard.com/article/economy-policy/ccs-nod-for-telecom-testing-and-security-certification-centre-113021101330_1.html> accessed 26 May 2022; PTI, 'NATGRID Gets Cabinet Approval' (NDTV.com, 7 June 2011) <<https://www.ndtv.com/india-news/natgrid-gets-cabinet-approval-457900>> accessed 26 May 2022.

³⁶⁴ Software Freedom Law Centre, 'Legal Challenge by CPIL and SFLC.IN to Surveillance Projects CMS, NATGRID and NETRA' (n 332).

the Telegraph Act and the IT Act, and the accompanying Rules.³⁶⁵

However, it is not clear that these laws are applicable, since the potential bulk interception capabilities of these surveillance mechanisms were never contemplated at the time of the enactment of Section 5(2) of the Telegraph Act or Section 69 of the IT Act. Indeed, there exists scholarly opinion that the Supreme Court's guidelines in PUCL make it clear that Section 5(2) of the Telegraph Act was not intended to carry out mass surveillance, since they require the interception orders to specify the communications that needed to be intercepted ('any message or class of messages') as well as the persons ('any persons or class or persons') and addresses involved.³⁶⁶ This would not be possible in a mass surveillance scenario.

The procedure for electronic surveillance under the IT Interception Rules also requires a written order specifying the information sought.³⁶⁷ These procedures and safeguards are appropriate and applicable for targeted surveillance, but not for mass surveillance, which, by definition, is intended to facilitate the mass collection or monitoring of data and is not directed at any identifiable messages or individuals.

As noted in Chapter 5, the CMS operates without the assistance or cooperation of telecom companies in a manner not contemplated by the Telegraph Act or IT Act, placing it outside the four walls of these statutes. Both laws expressly require interception and information gathering to be conducted *through* designated officers appointed by TSPs. However, under the CMS, the government can access intercepted communications without the involvement of TSPs, in a manner not envisaged by the Telegraph or IT Acts.

The CMS also raises the potential of bulk collection and storage of communications data (including call records), by its very nature, it is uncertain whether the CMS complies with the requirement for specific and limited authorisation.³⁶⁸ As discussed above, the guidelines in PUCL require interception orders to specify

365 Minister of Communications and Information Technology, Answer to Unstarred Question No 595 (Lok Sabha, 2 December 2015) <<http://164.100.24.220/loksabhaquestions/annex/6/AU595.pdf>>; Ministry of Home Affairs, Answer to Unstarred Question No 163 (Lok Sabha, 13 March 2012) <<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=116617&lsno=15>> accessed 31 May 2022; PTI, 'No Blanket Permission given for Surveillance under NETRA, NATGRID: Centre to HC' *The Economic Times* (5 February 2021) <<https://economictimes.indiatimes.com/news/defence/no-blanket-permission-given-for-surveillance-under-netra-natgrid-centre-to-hc/articleshow/80706304.cms?from=mdr>> accessed 26 May 2022.

366 Gautam Bhatia, 'State Surveillance and the Right to Privacy in India: A Constitutional Biography' (2014) 26 *National Law School of India Review* 127.

367 IT Traffic Data Rules, r. 3, 7.

368 Bhatia, 'STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA' (n 366).

the communications to be intercepted ('any message or class of messages) and the persons ('any person or class of persons'),³⁶⁹ suggesting that each instance of surveillance had to be individually authorised. The operation of the CMS however, bypasses the role of service providers,³⁷⁰ allowing the State to directly access the records of TSPs.³⁷¹ In fact, by the Union Government's own statement, one of the functions of CMS is "analysis" of communications metadata such as CDRs.³⁷² Thus, in the absence of additional clarity on the types of, and manner in which communications data is being collected, and whether each instance of data access is individually authorised, the program is susceptible to challenge for operating outside procedures prescribed under Rule 419A of the Telegraph Rules or the IT Interception Rules (both of which requires TSPs, ISPs, or intermediaries to facilitate interception or electronic surveillance pursuant to individual and specific authorisations).

NETRA, too, fails the test of legality since it enables the indiscriminate collection of personal data through trawling global web traffic, including emails, texts, and posts on social media, as opposed to collecting specific information. As we have discussed before, this mass surveillance capability, which allows for the indiscriminate collection of personal data, could not have been sanctioned by the targeted measures that are envisaged by the Telegraph Act or the IT Act.

In response to the legal challenge to CMS, NETRA, and NATGRID before the Delhi High Court, the Union Government has stated that there is 'no blanket permission to any agency for interception or monitoring or decryption' and that 'permission from a competent authority' is required in each case in accordance with the Telegraph Act and the IT Act.³⁷³ However, an argument can still be made that, even with the permission from competent authorities, the bulk collection and storage of personal data by these systems would fall outside the scope of the powers granted to the government under this set of legislation, which was meant for authorising specific, targeted surveillance. For example, NETRA envisages the wholesale, ongoing, and undirected monitoring of internet traffic. If the government has not provided a blanket order to intercept and monitor traffic, it is unclear how the government is ensuring that the ongoing operations of NETRA comply with the grounds for initiating surveillance under the Telegraph Act and IT Act. Thus, if the

³⁶⁹ *ibid.*

³⁷⁰ Kotoky (n 333).

³⁷¹ Bhatia, 'STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA' (n 366).

³⁷² Press Information Bureau, 'Centralised System to Monitor Communications' (n 333).

³⁷³ Short Affidavit on Behalf of Respondents 2, 3 and 4) in *CPIL v Union of India* WP (C) 8998 of 20 (High Court of Delhi), para 7, <<https://d2r2ijn7njrktv.cloudfront.net/IL/uploads/2021/02/05202537/New-centre-vs-uoi.pdf>> accessed 31 May 2022.

operation of these programs itself falls outside the four walls of the two statutes, the mere existence of the statutes authorising *some type of* surveillance does not represent parliamentary authorisation for the programs themselves.

Thus, for all these reasons, surveillance through the CMS and NETRA does not appear to satisfy the legality criterion. To satisfy the constitutionality requirement, it is imperative for the government to either amend the Telegraph Act and IT Act, or to provide a separate statute to specifically authorise the deployment of such surveillance projects. Enacting a separate law will also allow the Union Government to lay down adequate procedural safeguards and data protection norms, and build in accountability and transparency frameworks within the law specifically designed to address the capabilities of these programs.

(b) Legitimate aim

In general, surveillance practices usually pursue legitimate, aims such as the safeguarding of national security, prevention of terrorism, or the prevention and detection of other crime. These aims have been endorsed by regional human rights bodies such as the ECtHR,³⁷⁴ and by the Indian Supreme Court.³⁷⁵ However, mass surveillance projects envisage the constant monitoring of *all* citizens, implicating the criminality of *all* individuals, and implying the government is dealing with a near permanent state of emergency. Such a sweeping mandate may not comport with an identifiable state aim under the legitimate aim test.

This is one of the problems with the NETRA project, since it allows the government to intercept and monitor *all* internet traffic. This raises questions about whether it assumes a near-permanent situation of “public emergency” or “interest of public safety”, as required by the Telegraph Act or the respective grounds under the IT Act. If so, this is unlikely to be countenanced as a legitimate aim.

(c) Suitability

It is important to ensure that the data collected under a mass surveillance regime is utilised only for the particular legitimate aim pursuant to which it was collected.³⁷⁶ There have been documented instances of investigative agencies in other countries misusing their surveillance powers to prevent abuse of parking privileges, sick

³⁷⁴ *Big Brother Watch v United Kingdom* App No 58170/30 (ECtHR, 25 May 2021) [345].

³⁷⁵ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [328] (Chandrachud J).

³⁷⁶ *K S Puttaswamy v Union of India* (2017) 10 SCC 1 [314] (Chandrachud J), [585] (Kaul J).

leave, violations of the smoking ban etc.³⁷⁷ This kind of abuse of highly invasive surveillance powers, where the data collected is used for additional purposes, does not satisfy either the suitability or necessity limbs, and should be prohibited.

However, ensuring such purpose limitation is difficult in the case of the mass surveillance capable projects in India for two reasons. First, there is limited transparency on the CMS and NETRA, which makes it difficult to ascertain their exact functioning or accuracy rates. Second, in the absence of a legislative framework and oversight mechanisms, there is no publicly available framework against which the government's actions can be evaluated.

Thus, it is not possible to state with any certainty that the data collected from these operations is only being utilised for their stated objectives, or that the data is not being shared with other agencies. The problems of purpose limitation can be adequately addressed through the enactment of data protection laws and surveillance legislation, with appropriate safeguards and publicly available frameworks.³⁷⁸ However, as discussed in Chapter 7, India's proposed data protection legislation fails to adequately address this issue.

(d) Necessity and Proportionality

There is sufficient comparative jurisprudence that the necessity and proportionality test in human rights law applies unequivocally to surveillance regimes, to limit their interference with crucial human rights such as the right to privacy, free speech, and association.³⁷⁹ Surveillance measures should be restricted to cases where they are necessary to achieve the government's legitimate aims, i.e., surveillance measures should be the *only* or the *least restrictive* measure that could

³⁷⁷ Big Brother Watch, 'The Grim RIPA' (28th May 2010)

³⁷⁸ Human Rights Committee, 'Concluding Observations on the Fourth Periodic Report of the United States of America' CCPR /C/USA/CO/4 (23 April 2014) <<https://undocs.org/CCPR/C/USA/CO/4>> para. 22. See also *Malone v the United Kingdom* App No 8691/79 (ECtHR, 2 August 1984), [67]-[68]; *Weber and Saravia v Germany* App No 54934/00 (ECtHR, 29 June 2006). Weber listing minimum safeguards that should be set out in statute law.

³⁷⁹ *Murray v the United Kingdom* App No 14310/88 (ECtHR, 28 October 1984), [90]-[91]; C-170 *Chaparro Álvarez and Lapo Íñiguez v Ecuador* (IACHR, 2007); C-177 *Kimel v Argentina* (IACHR, 2008); C-391 *Romero Feris v. Argentina* (IAHRC, 2019), [94]; *K S Puttaswamy v Union of India* (2017) 10 SCC 1; *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1. However, it must also be noted that the formulation and application of the test can vary from region to region – for comparative perspectives on proportionality, see Chandra (n 54).

be used to achieve the stated legitimate aim.³⁸⁰

As per the Bilchitz proportionality formulation adopted in the *Aadhaar Judgment*, the State must (i) identify the range of possible alternative measures that could be adopted; (ii) determine the effectiveness of each of these measures i.e., whether the measures realize the legitimate objectives in a ‘real and substantial manner’; (iii) determine the impact of the particular measures on the concerned right and (iv) make an overall judgement based on the above factors, whether there is a preferable alternative to the government’s choice.³⁸¹

There is some ambiguity on whether the burden to show that an impugned surveillance measure is the only or the least restrictive measure is on the State, or on the individuals challenging the proportionality of the measure.³⁸² To justify the ‘necessity’ of mass surveillance, the State must demonstrate why the use of targeted surveillance measures was ineffective or insufficient, and thus why mass surveillance is *necessary*.

Unlike the minimum procedural safeguards prescribed under Rule 419A of the Indian Telegraph Rules and the IT Interception Rules, NETRA does not require the consideration of lesser intrusive measures, since it is designed to collect, store, and share data *en masse*. The petition filed in the Delhi High Court challenging the constitutionality of CMS, NETRA, and NATGRID argues that the dragnet surveillance measures violate the principles laid down in *Puttaswamy*, since they are not the least intrusive means to achieve the State’s aims, and are disproportionate, without judicial oversight.³⁸³

In fact, less intrusive measures have been developed in the United States after Snowden’s revelations. For instance, the National Security Agency’s (NSA) mass surveillance program has been prohibited from collecting telephone metadata of

380 Electronic Frontier Foundation, ‘International Principles on the Application of Human Rights to Communications Surveillance’ (Electronic Frontier Foundation 2013) <<https://www.eff.org/files/necessaryandproportionatefinal.pdf>> accessed 26 May 2022.

381 *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [148], [157]–[158].

382 See Ankush Rai, ‘Guest Post: Proportionality in Application – An Analysis of the “Least Restrictive Measure”’ (*Indian Constitutional Law and Philosophy*, 8 May 2020) <<https://indconlawphil.wordpress.com/2020/05/08/guest-post-proportionality-in-application-an-analysis-of-the-least-restrictive-measure/>> accessed 27 May 2022; Mariyam Kamil, ‘The Aadhaar Judgment and the Constitution – II: On Proportionality (Guest Post)’ (*Indian Constitutional Law and Philosophy*, 30 September 2018) <<https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/>> accessed 26 May 2022; Chandra (n 44); Electronic Frontier Foundation (n 347).

383 *CPIL v Union of India* WP (C) 8998 of 20 (High Court of Delhi). Writ petition to permanently stop the execution and operation of the surveillance projects namely “CMS”, “NETRA” and “NATGRID”)

U.S. citizens by the USA Freedom Act.³⁸⁴ The NSA now requires a court order to approach TSPs for accessing the same data.³⁸⁵ Approaching the TSPs and ISPs as and when needed for an investigation is the system already in existence in India under Section 5(2) of the Telegraph Act and Section 69 of the IT Act, albeit without the judicial warrant requirement. However, as noted above, the CMS would allow for both the collection of communications data and interception without needing to approach TSPs.

Global jurisprudence around bulk interception regimes is mixed. In *MK vs. France*, the ECtHR rejected the government's argument that retention of fingerprints would help the government against potential identity theft, since it would be tantamount to justifying storage of information of the entire French population, which was disproportionate.³⁸⁶ Similarly, in *S & Marper*, the Court rejected the government's justification for retaining fingerprints for future prevention of crime, since it was a very widely worded purpose, without guarantees against arbitrariness and irrespective of guilt.³⁸⁷

Indian courts have not yet expressly decided the issue of mass surveillance. However, the majority opinion in the *Aadhaar Judgment* held that the requirement for the entire population to link Aadhaar numbers to bank accounts for the purpose of countering money laundering would target 'every resident of the country as a suspicious person' and was disproportionate.³⁸⁸ Thus, the presumption of criminality that is inherent in the profiling and data collection of all citizens under CMS and NETRA is also likely to be ruled as disproportionate.

(e) Procedural Safeguards

Judgments that have upheld bulk interception and collection of information regimes have done so on the premise that they are not *per se* illegal, given the existence of safeguards and oversight mechanisms.³⁸⁹ Some of the procedural safeguards that have been recognised by courts across the world as necessary in any surveillance regime are: (i) purpose limitation (using data only for the stated purpose and destroying records after use); (ii) storage limitation; and (iii) access

384 *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015* (U.S.), s. 103

385 *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015* (U.S.), s. 103

386 App No 19522/09 (ECtHR, 18 April 2013), [37].

387 App No 30562/04 & 30566/04 (ECtHR, 4 December 2008).

388 *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [491].

389 *Big Brother Watch v United Kingdom* App No 58170/30 (ECtHR, 25 May 2021).

control.³⁹⁰

The *Aadhaar Judgment* struck down the archival and retention of Aadhaar authentication transaction data by the Unique Identification Authority of India beyond six months as being disproportionate, without procedural safeguards, and contrary to the right to data erasure or the right to be forgotten.³⁹¹

Surveillance programs such as CMS and NETRA operate in India in the absence of any anchoring legislation or comprehensive data protection law to regulate how these programs can be used, the kinds of data they can collect, or the period for the retention of this data. As discussed in Chapter 7, India's proposed data protection legislation exempts the State from several key obligations and potentially allows the State to retain data indefinitely. In addition, there is a lack of transparency surrounding the inner workings of these programs.

Hence, without statutory safeguards or public accountability, there is nothing preventing these programs from collecting large amounts of data and metadata (including CDRs), and sensitive personal data (such as financial data), regardless of suspicion of or nature of the crimes. It is not clear where this data is stored, how long it is stored for, when it is deleted, and with whom it is being shared. The consequences of the lack of transparency is that the general public will not know if and when a person's data has been collected, whether they have been profiled, or whether and why their personal communication has been intercepted.

Finally, neither the Telegraph Act nor the IT Act, nor even the accompanying rules, clarify these issues with respect to these mass surveillance programs. The secret nature of these surveillance programs is the reason why petitions challenging their constitutionality – whether in the Delhi High Court (challenging CMS, NETRA, and NATGRID)³⁹² or in the Telangana High Court (challenging the Crime and Criminal Tracking Network and Systems and the use of facial recognition systems),³⁹³ are filed as Public Interest Litigations, rather than by affected third parties.

390 *S and Marper v United Kingdom* App No 30562/04 & 30566/04 (ECtHR, 4 December 2008); *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1; *Centrum för Rättvisa v Sweden* App No 35252/08 (ECtHR, 25 July 2021); *Case C-293/12 Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources* [2014] ECR I-238. Invalidating the Data Retention Directive in *Digital Rights Ireland*, terming the requirement to store communications data between six months to two years disproportional.

391 *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1. For a criticism of this finding, please see Anand Venkat, 'The Aadhaar Judgment and Reality – III: On Surveillance (Guest Post)' (*Indian Constitutional Law and Philosophy*, 2 October 2018) <<https://indconlawphil.wordpress.com/2018/10/02/the-aadhaar-judgment-and-reality-iii-on-surveillance-guest-post/>> accessed 26 May 2022.

392 *CPIL v Union of India* WP (C) 8998 of 20 (High Court of Delhi).

393 *S.Q. Masood v State of Telangana* WP (PIL) 191 of 2021 (Telangana High Court).

In addition, there is no *ex-ante* or *ex-post* judicial or parliamentary oversight and authorisation of data collection and profiling,³⁹⁴ and intelligence agencies in India do not have any clear statutory or parliamentary accountability mechanism,³⁹⁵ further reducing any transparency and accountability. Consequently, there is no mechanism to verify government statements that internal checks and balances and procedures (similar to the Telegraph Act or IT Act) are being followed.

Without any legislative framework and procedural safeguards in place, and for the reasons articulated above, surveillance programs such as the CMS and NETRA are unlikely to satisfy the test set out in *Puttaswamy* and the *Aadhaar Judgement*, and are open to constitutional challenges.

POSSIBILITY OF EX POST FACTO REPORTING REQUIREMENTS

Finally, in addition to the need for independent judicial oversight over the authorisation of surveillance, discussed earlier in the report, another area of potential surveillance reform can be providing *post facto* notification and implementing reporting requirements for transparency. The reforms can enable those placed under surveillance to challenge an action if necessary. Sweden's Signals Intelligence Act requires the Försvarets Radioanstalt (National Defence Radio Establishment) to notify citizens if search terms directly related to them have been used, which the Court considered when finding the surveillance regime compatible with European human rights law. Austria,³⁹⁶ Germany,³⁹⁷ Canada,³⁹⁸ and Belgium³⁹⁹ also have notification requirements.

In *Roman Zakharov*, the European Court of Human Rights laid out the elements for an effective remedy to illegal surveillance, holding that the right to an effective remedy will be adversely affected unless there is a right to be notified or at the least to apply for and obtain information from the relevant authorities.⁴⁰⁰ These rights can be incorporated into Indian law.

³⁹⁴ Commissioner for Human Rights, Council of Europe, 'Positions on Counter-Terrorism and Human Rights Protection' (5 June 2015), pp. 10-11

³⁹⁵ Vrinda Bhandari, 'The Pegasus Case Must Be Used to Press for Change in Surveillance Laws' [2021] *The India Forum* <<https://www.theindiaforum.in/article/pegasus-case-must-be-used-press-change-surveillance-laws>> accessed 26 May 2022.

³⁹⁶ Criminal Procedure Code 1975, s. 139 (Austria).

³⁹⁷ Paul DE Hert and Franziska Boehm, 'The Rights of Notification after Surveillance Is over: Ready for Recognition', *Digital Enlightenment Yearbook* (IOS Press 2012).

³⁹⁸ Criminal Code 1985, s. 196 (Canada).

³⁹⁹ Hert and Boehm (n 397) 9.

⁴⁰⁰ *Roman Zakharov v Russia* App No 47143/06 (ECtHR, 4 December 2015), [81].

7. Way Forward and Conclusion

The Indian government has deployed several targeted and modern surveillance systems with mass surveillance capabilities. Rapid technological advancements have enabled the State to conduct surveillance with few limits on scale or duration.⁴⁰¹ The limited statutory safeguards provided for targeted surveillance are not adequate, while the functioning of systems with mass surveillance capabilities takes place almost exclusively outside any legal framework of accountability or oversight.

The lack of judicial or parliamentary oversight of surveillance action, the admissibility of illegally obtained evidence, and the lack of clear and accessible legal frameworks that govern the operation of surveillance systems with mass surveillance capabilities – these are some of the primary concerns highlighted in this report. These concerns are not all new. Discussing the legal structures governing surveillance in India, the Justice Srikrishna Committee Report observed:

*The design of the current legal framework in India is responsible for according a wide remit to intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil liberties. Much intelligence-gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammelled rise of a surveillance society.*⁴⁰²

Despite *Puttaswamy* being a watershed moment for privacy doctrine, in the half-decade since the Court's decision, the promise of a principled and proportionate surveillance framework that incorporates procedural safeguards and adheres to the rule of law has failed to materialise in practice. There are numerous legal challenges to India's surveillance laws and programs pending in various courts, and the outcome of these may yet shape the course of India's surveillance framework. Below, we summarise certain principles that should underpin the next phase of judicial, legislative, and policy developments in this domain.

Application of *Puttaswamy* doctrine

The Supreme Court in *Puttaswamy* has laid down powerful doctrine to ensure the

⁴⁰¹ Human Rights Committee, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' A/HRC/23/40 (17 April 2013), para 33.

⁴⁰² Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 265) 124.

State's surveillance measures respect individuals' right to privacy. Further, given that the decision was delivered by a nine-judge bench of the Supreme Court, it is undoubtedly controlling precedent *vis-à-vis* issues of governmental actions impinging on individual privacy.

The analysis in this report suggests that applying the doctrine set out in *Puttaswamy* will fundamentally reshape alter India's surveillance landscape. Therefore, it is important that courts hearing challenges to India's surveillance landscape engage with and apply the doctrine set out in *Puttaswamy* and the *Aadhaar Judgement*.

The analysis contained in Chapters 4 and 6 points to the fact that the operation of both India's targeted surveillance programs and programs with mass surveillance capabilities do not comply with the legal standards set out in *Puttaswamy*. Most notably, questions remain over why independent or judicial authorisation and oversight for targeted interception under the Telegraph Act and IT Act is not a less rights-restrictive but equally efficacious measure. If it is, India's current regime for targeted surveillance would violate the 'necessity' limb of the proportionality test. In the context of surveillance programs such as CMS and NETRA, their lack of statutory backing would result in a breach of the 'legality' limb of the *Puttaswamy* test.

While it may not be appropriate for courts to legislate themselves, or compel the legislature or executive to adopt specific measures, Article 13 of the Indian Constitution expressly grants courts the power to invalidate governmental measures that impermissibly restrict the fundamental rights of citizens. Where existing surveillance measures do not satisfy the tests laid out by *Puttaswamy* and the *Aadhaar Judgement*, they may be invalidated by courts for impermissibly restricting the rights of individuals.

Need for a law in line with the *Puttaswamy* standard

The standards set out in *Puttaswamy* do not outlaw surveillance. Rather, they require that surveillance be conducted in a proportionate manner, and only where necessary to safeguard the State's legitimate interests. Thus, the government may either amend the Telegraph Act or IT Act, or adopt fresh legislation, in order to authorise surveillance in a manner compliant with current Supreme Court doctrine. What such a law may entail is beyond the scope of the present report, but this report's analysis of how the legal standards of legality, necessity, proportionality, and the need for procedural safeguards interact with surveillance measures may serve as a valuable starting point.

Reconsideration of Data Protection Bill

Given the large volumes of personal data modern surveillance systems have the capability to collect, it is important to have a robust data protection framework in place. However, the DPDP Bill does not provide for judicial oversight or seek to regulate investigative agencies. Clause 18 of the DPDP Bill *exempts* the government and its agencies from having to comply with data protection practices on numerous broad grounds. Further, Clause 18(4) of the Bill potentially allows the State to retain data collected pursuant to surveillance programs or welfare schemes *indefinitely*. This raises unique risks in the context of modern surveillance programs that indiscriminately collect data, as individuals' personal data with no nexus to an investigatory purpose may be retained by the government for extended periods. Thus, the DPDP Bill allows government agencies to not adhere to crucial data protection obligations such as collection limitation, purpose limitation, data minimization or conducting fair and reasonable processing, or employing the requisite security safeguards to protect citizens' personal data.

In fact, the DPDP Bill does not adhere to the minimal safeguards and requirements set out in *Puttaswamy* and in the draft Personal Data Protection Bill, 2018 released by the Srikrishna Committee, which required that any such exemption to government agencies be done as per a law made by Parliament, and be necessary for and proportionate to the interests sought to be achieved by the State.⁴⁰³ However, the Committee also suggested that the government draft a separately law concerning surveillance, to ensure a holistic approach to the privacy risks that surveillance measures raise.

Need for transparency and accountability

The lack of transparency and accountability around the operation of the surveillance systems raises concerns. Given the currently limited publicly available information on surveillance measures, enhanced transparency and accountability measures would ensure adherence with the concept of the rule of law in the Indian Constitution. While a certain level of secrecy may be required to avoid defeating the purpose of surveillance, a certain level of transparency is required to ensure accountability.

In the Indian context, current law states that the specific use of the interception power of the State can be exempted from disclosure under the RTI Act.⁴⁰⁴ However, the Ministry of Home Affairs has refused to respond to RTIs seeking aggregate information about the *total* number of surveillance requests issued

⁴⁰³ *ibid* 150.

⁴⁰⁴ *Neelesh Gajanan Marathe v CPIO, Ministry of Home Affairs* (2018) SCC Online CIC 12916; *S C Sharma v Jt. Secy. (Internal Security)* (2006) SCC Online CIC 125.

during the period of 2016–2018.⁴⁰⁵ According to media reports, although the Ministry first rejected the requests citing national security and active-investigation related exemptions under Sections 8(1)(a), (g), and (h) of the RTI Act, it later stated that the records had been destroyed and that there was no information about the total number of surveillance orders passed in the two-year period the request pertained to.⁴⁰⁶ Disclosures regarding the volume of surveillance and the procedures employed during surveillance would be useful to inform how legal regulation ought to develop.

⁴⁰⁵ Internet Freedom Foundation, ‘Delhi HC Directs MHA to Clarify Its Position on Maintenance of E-Surveillance Data’ (n 154).

⁴⁰⁶ Internet Freedom Foundation, ‘DHC Directs CIC to Decide IFF’s Appeals within 8 Weeks’ (n 155); Internet Freedom Foundation, ‘Delhi HC Directs MHA to Clarify Its Position on Maintenance of E-Surveillance Data’ (n 154).

ANNEXURE: DATA COLLECTION AND SHARING PROGRAMS

1. The National Intelligence Grid

NATGRID, originally established in 2010,⁴⁰⁷ is a surveillance system that will operate under the Ministry of Home Affairs, and is part of the Union Government's efforts to ramp up security in the country after the 26/11 Mumbai terror attacks.⁴⁰⁸ Work on the NATGRID project has been ongoing for several years; however, in March 2022, it was reported that the NATGRID is likely to be implemented soon.⁴⁰⁹

According to the Union Government, NATGRID is conceived as a framework to leverage information technology “to connect approved User Agencies (security/law enforcement) with designated Data providers (Airlines, Banks, SEBI, Railway, Telecom etc.)” to improve India's counter-terrorism capabilities.⁴¹⁰ Thus, the NATGRID involves both data sharing of information regarding individuals already held by government agencies, and data collection from private entities such as airlines and banks. The government reportedly has approved operating procedures and oversight mechanisms that help facilitate access between the user agencies and the data providers, to enable the government to analyse and disseminate intelligence to synergise counterterrorism efforts.⁴¹¹

The agencies approved to use NATGRID by the Cabinet Committee on Security are all Union Government investigative agencies, comprising of the Intelligence Bureau, Research & Analysis Wing, CBI, the Directorate of Revenue Intelligence, the Enforcement Directorate, the Financial Intelligence Unit, the Central Board of Direct Taxes, the Central Board of Excise and Customs, the Directorate General

⁴⁰⁷ Minister of State in the Ministry of Home Affairs, Answer to Unstarred Question No 131 (Lok Sabha, 21 August 2012) <<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=125912&lsno=15>> accessed 31 May 2022.

⁴⁰⁸ ‘National Intelligence Grid to Be Ready by Early 2020’ *The Hindu* (New Delhi, 22 September 2019) <<https://www.thehindu.com/news/national/national-intelligence-grid-to-be-ready-by-early-2020/article29480961.ece>> accessed 26 May 2022.

⁴⁰⁹ ANI, ‘Parliamentary Panel Asks MHA to Fix Timeline for Launch of Counter-Terrorism NATGRID’ *The Times of India* (19 March 2022) <https://timesofindia.indiatimes.com/india/parliamentary-panel-asks-mha-to-fix-timeline-for-launch-of-counter-terrorism-natgrid/articleshow/90318661.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> accessed 26 May 2022.

⁴¹⁰ Minister of State in the Ministry of Home Affairs, Answer to Unstarred Question No 3493 (Lok Sabha, 11 August 2015) <<https://www.mha.gov.in/MHA1/Par2017/pdfs/par2015-pdfs/ls-110815/3493.pdf>> accessed 27 February 2023.

⁴¹¹ Minister of State in the Ministry of Home Affairs, Answer to Unstarred Question No 3493 (Lok Sabha, 11 August 2015) <<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=22670&lsno=16>> accessed 31 May 2022.

of Central Excise and Intelligence, and the Narcotics Control Bureau.⁴¹² These ten agencies will initially be connected to twenty-one data providers, with 1,950 additional organisations to be reportedly linked in subsequent phases.⁴¹³

NATGRID is thus an integrated IT system intended to automate the existing manual processes for collation of information by allowing government agencies to access data through a secure platform from over twenty-one data sources, such as railway or air travel, credit card and bank account transactions, income tax details, and immigration records. Collection of such personal data for crime-related and investigatory purposes will be automated, and made accessible via a centralised database or platform from, which government agencies can access relevant information regarding criminal suspects.

The Income Tax Department will reportedly share ‘bulk information’ including PAN (permanent account number) and personal data such as names, addresses, and dates of birth.⁴¹⁴ Importantly, the government has clarified that NATGRID will not have real-time access to citizens’ data such as passport, driver’s license, and telephone records.⁴¹⁵ However, it does appear that NATGRID facilitates the real-time profiling of individuals, and thus substantially restricts the right to privacy of individuals.

NATGRID has also signed a Memorandum of Understanding with the National Criminal Records Bureau to access its centralised online database of First Information Reports (“**FIR**”) and stolen vehicles. This will give it access to the Crime and Criminal Tracking Network and Systems (“**CCTNS**”) database, which links around 16,930 police stations in India that all file FIRs with the CCTNS.⁴¹⁶

⁴¹² Ministry of Home Affairs, Answer to Unstarred Question No 999 (Rajya Sabha, 4 March 2015) <<https://drive.google.com/file/d/1NmHg0h9kX6OCogicsft1y4XBkkMFuPsH/view>> accessed 31 May 2022.

⁴¹³ PTI, ‘NATGRID to Get PAN, Taxpayer Data Access’ *The Economic Times* (22 June 2017) <<https://economictimes.indiatimes.com/news/economy/policy/natgrid-to-get-pan-taxpayer-data-access/articleshow/59270998.cms>> accessed 26 May 2022.

⁴¹⁴ Vijaita Singh, ‘NATGRID to Have Access to Database That Links around 14,000 Police Stations’ *The Hindu* (New Delhi, 12 July 2020) <<https://www.thehindu.com/news/national/natgrid-to-have-access-to-database-that-links-around-14000-police-stations/article32058643.ece>> accessed 26 May 2022; PTI (n 413).

⁴¹⁵ Ministry of Home Affairs, Answer to Unstarred Question No 999 (Rajya Sabha, 4 March 2015) <<https://drive.google.com/file/d/1NmHg0h9kX6OCogicsft1y4XBkkMFuPsH/view>> accessed 31 May 2022.

⁴¹⁶ Press Information Bureau, ‘Union Home and Cooperation Minister Shri Amit Shah Addressed the 37th Foundation Day Celebrations of National Crime Records Bureau (NCRB) as the Chief Guest in New Delhi Today’ (Press Information Bureau, 11 March 2022) <<https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1805133>> accessed 26 May 2022; Singh (n 414).

There are reports that NATGRID will use data analytics to track suspects,⁴¹⁷ and wants to link social media accounts to its centralised database.⁴¹⁸ It issued an expression of interest, released in 2017, with technical prequalification criteria of 'significant component of data analytics' and 'social media analytics'.⁴¹⁹ It is also concerning that, in 2011, NATGRID was placed outside the purview of the RTI Act,⁴²⁰ thus reducing the transparency of the State's surveillance actions *qua* its citizens.

2. Crime and Criminal Tracking Network

The CCTNS is a comprehensive and integrated system that is aimed at creating a nationwide networking infrastructure for the evolution of an 'IT-enabled-state-of-the-art tracking system' for the investigation of crime and detection of criminals.⁴²¹ It was approved by the Cabinet Committee for Economic Affairs in 2009 and is administered by the National Crime Records Bureau ("NCRB"), an agency that manages crime data for the police.

The CCTNS platform interlinks around 16,390 police stations across the country, and creates a centralised database of crime and criminal related information – such as FIRs and details of investigations, criminal images, and fingerprints, which are collected through the respective states' CCTNS databases.⁴²² All state police are reportedly required to file FIRs in the CCTNS.⁴²³ In addition to the state police, in

⁴¹⁷ PTI, 'NATGRID to Use Big Data & Analytics to Track Suspects' *Business Standard India* (29 December 2013) <https://www.business-standard.com/article/current-affairs/natgrid-to-use-big-data-analytics-to-track-suspects-113122900191_1.html> accessed 26 May 2022.

⁴¹⁸ Vijaita Singh, 'NATGRID Wants to Link Social Media Accounts to Central Database' *The Hindu* (New Delhi, 12 September 2019) <<https://www.thehindu.com/news/national/natgrid-wants-to-link-social-media-accounts-to-central-database/article61986607.ece>> accessed 26 May 2022.

⁴¹⁹ Ministry of Home Affairs, 'Expression of Interest for Selection of Systems Integrators for Implementing Entity Extraction, Visualization & Analytics (EVA) System (29 October 2017) 14' <https://www.mha.gov.in/sites/default/files/EOIEVA_29092017.pdf> accessed 31 May 2022.

⁴²⁰ Ministry of Personnel, Public Grievances and Pensions (Department of Personnel Training) G.S.R. 442(E) dated 9 June 2011 <https://documents.doptirculars.nic.in/D2/D02rti/1_3_2011-IR09062011.pdf> accessed 31 May 2022.

⁴²¹ 'Crime and Criminal Tracking Network & Systems (CCTNS) | National Crime Records Bureau' (National Crime Records Bureau) <<https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns>> accessed 26 May 2022.

⁴²² Press Information Bureau, 'Union Home and Cooperation Minister Shri Amit Shah Addressed the 37th Foundation Day Celebrations of National Crime Records Bureau (NCRB) as the Chief Guest in New Delhi Today' (n 416); Press Information Bureau, 'CCTNS Active in 15152 out of 15985 Police Stations across the Country' (Press Information Bureau, 11 February 2020) <<https://pib.gov.in/PressReleaseDetail.aspx?PRID=1602767>> accessed 26 May 2022.

⁴²³ Singh (n 414).

March 2022, the Union Home Minister proposed that data from Union Government agencies such as the CBI, the Narcotics Control Bureau, and the National Investigation Agency should be integrated with the CCTNS as well.⁴²⁴

The objectives of the CCTNS include (i) the computerisation of the police process (e.g. FIRs, fines, and investigations); (ii) facilitating pan-India search on national databases for crime and criminal records to assist in criminal investigations; and (iii) sharing such data amongst police stations, courts, prisons, prosecution, and forensics departments as part of the Interoperable Criminal Justice System.⁴²⁵

This sharing of data across different branches of the criminal justice system is meant to enable courts and police stations to receive updates about judicial processes in real time. Thus, courts will get notified about FIRs and prosecutorial updates, while the police will get notified about judicial processes such as remand and bail decisions.⁴²⁶ Access to the Interoperable Criminal Justice System dashboard has been provided to Union Government agencies including the National Intelligence Agency, the Narcotics Control Bureau, the CBI, and the NCRB.⁴²⁷

The data protection, data storage, and retention policies of the CCTNS database have not been made publicly available, and do not have specific statutory authorisation. While CCTNS enables easier access to information for investigative agencies and state police across the country, it is unclear whether procedural safeguards or checks and balances are in place. CCTNS follows a principle of centralised planning and decentralised implementation,⁴²⁸ which means that ensuring the safeguarding of data on storage, retention, use, and disclosure are left

⁴²⁴ Press Information Bureau, 'Union Home and Cooperation Minister Shri Amit Shah Addressed the 37th Foundation Day Celebrations of National Crime Records Bureau (NCRB) as the Chief Guest in New Delhi Today' (n 416).

⁴²⁵ Ministry of Home Affairs, 'Crime and Criminal Tracking Network and Systems (CCTNS) (24 April 2018) <https://www.mha.gov.in/sites/default/files/CCTNS_Briefportal24042018.pdf> accessed 24 June 2021; Ministry of Home Affairs, Women Safety Division 'She Raksha' (8 November 2019) 6 <https://www.mha.gov.in/sites/default/files/WSDivision_SheRakshaVol2_08112019pdf.pdf> accessed 26 May 2021.

⁴²⁶ Ministry of Law & Justice, 'Live Electronic Exchange of Data between Courts and Police' (Press Information Bureau, 19 December 2018) <<https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1556649>> accessed 26 May 2022.

⁴²⁷ Ministry of Home Affairs, 'Crime and Criminal Tracking Network and Systems (CCTNS) (24 April 2018) 3 <https://www.mha.gov.in/sites/default/files/CCTNS_Briefportal24042018.pdf> accessed 24 June 2021.

⁴²⁸ Indian Institute of Public Administration, 'Report on the Evaluation of Crime and Criminal Tracking Network and Systems Project' (Indian Institute of Public Administration) <https://www.mha.gov.in/sites/default/files/IIPA-Report-CCTNS_0.pdf> accessed 26 May 2022.

to the discretion of investigative agencies.

Automated facial recognition systems

The CCTNS lays the base layer framework on which surveillance through automated facial recognition systems (“AFRS”) takes place.⁴²⁹ For instance, in the state of Telangana, the images captured through CCTV cameras are compared against the CCTNS database.⁴³⁰ Similarly, CCTV cameras have been deployed widely in cities such as New Delhi, Hyderabad, and Chennai.⁴³¹ Extensive use of CCTV cameras coupled with facial recognition technology, linked to criminal databases, contribute to the mass surveillance of citizens without any legal basis or procedural safeguards.

In 2019, the NCRB released a Request for Proposal for an AFRS for use by the police in India.⁴³² According to the Request for Proposal, the AFRS will help in “*automatic identification and verification based on digital images, photos, digital sketches, video frames and video sources by comparison of selected facial features of the image from the existing crime and criminal databases.*”⁴³³ AFRSs have been pitched as helpful in facilitating criminal investigations and detection of criminals and helping in identifying missing persons, unidentified dead bodies and unknown children or persons.

AFRSs reportedly operates by using image and visual biometric and facial data from various sources such as police stations’ records, including the CCTNS database, to

⁴²⁹ *ibid.*

⁴³⁰ Express News Service, ‘TSCOP App to Use Facial Recognition’ *The New Indian Express* (3 August 2018) <<https://www.newindianexpress.com/cities/hyderabad/2018/aug/03/tscop-app-to-use-facial-recognition-1852485.html>> accessed 26 May 2022.

⁴³¹ Jayant Pankaj, ‘CCTV Surveillance Is Rising in India, World, but Crime Rates Remain Unaffected’ (*The Wire*, 5 January 2022) <<https://thewire.in/rights/cctv-surveillance-is-rising-in-india-world-but-crime-rates-remain-unaffected>> accessed 28 March 2023.

⁴³² Karishma Mehrotra, ‘Automated Facial Recognition: What NCRB Proposes, What Are the Concerns’ *The Indian Express* (10 July 2019) <<https://indianexpress.com/article/explained/automated-facial-recognition-what-ncrb-proposes-what-are-the-concerns-5823110/>> accessed 26 May 2022.

⁴³³ National Crime Records Bureau, ‘Request For Proposal To Procure National Automated Facial Recognition System (AFRS)’ <<https://ncrb.gov.in/sites/default/files/tender/AFRSRFPDate22062020UploadedVersion.pdf>> accessed 26 May 2022.

find matches.⁴³⁴ This database is intended to be searchable and enable matching, linking and verification of facial images, and also include metadata.⁴³⁵ It is supposed to have the technical capability of matching facial images regardless of ‘modified facial features’ such as through plastic surgery or makeup.⁴³⁶ It is also required to be compatible with the National Automated Fingerprint Identification System.⁴³⁷

Importantly, while the original Request for Proposal had indicated that the AFRS would be fed with data from CCTV, newspapers and ‘data sent by people’,⁴³⁸ this requirement appears to have been dropped in the revised Request for Proposal released subsequently.⁴³⁹ The revised Request for Proposal now specifically states that ‘*this project does not involve installation of CCTV cameras nor will it connect to any existing CCTV camera anywhere*’.⁴⁴⁰ Therefore it is unclear what data the AFRS will be comparing against the CCTNS database. The revised Request for Proposal indicates that access to the AFRS will be given to Union Government agencies, such as the NCRB, as well as state agencies like the police.⁴⁴¹

Despite the Request for Proposal suggesting that AFRSs will not be connected to CCTV cameras, one of the few known use cases of AFRS is in fact by the Delhi police who reportedly used it to screen crowds, especially in protest gatherings, to create a photo database that can be used for routine criminal investigations.⁴⁴² As per news reports, the Delhi police has taken video footage of crowds at protest events with drones, and used this footage to create a dataset of ‘select protesters’,

⁴³⁴ Deeptiman Tiwary, ‘MHA Plans to Link Fingerprint, Face Recognition Data from All Police Stations to Central System’ *The Indian Express* (5 August 2018) <<https://indianexpress.com/article/india/mha-plans-to-link-fingerprint-face-recognition-data-from-all-police-stations-to-central-system-5292110/>> accessed 26 May 2022; Vidushi Marda, ‘Every Move You Make’ [2019] *India Today* <<https://www.indiatoday.in/magazine/up-front/story/20191209-every-move-you-make-1623400-2019-11-29>> accessed 26 May 2022.

⁴³⁵ National Crime Records Bureau (n 433) 3.

⁴³⁶ *ibid.*

⁴³⁷ ETGovernment, ‘NAFIS Will Be Operational Soon and Aid Police Forces in Crime Detection: MoS Home G. Kishan Reddy - ET Government’ ([ETGovernment.com](https://government.economictimes.indiatimes.com/news/digital-india/nafis-will-be-operational-soon-and-aid-police-forces-in-crime-detection-mos-home-g-kishan-reddy/78653613), 14 October 2020) <<https://government.economictimes.indiatimes.com/news/digital-india/nafis-will-be-operational-soon-and-aid-police-forces-in-crime-detection-mos-home-g-kishan-reddy/78653613>> accessed 26 May 2022.

⁴³⁸ National Crime Records Bureau (n 433) 3.

⁴³⁹ *ibid.* 2.

⁴⁴⁰ National Crime Records Bureau (n 433).

⁴⁴¹ *ibid.* 7.

⁴⁴² Jay Mazoomdaar, ‘Delhi Police Film Protests, Run Its Images through Face Recognition Software to Screen Crowd’ (*The Indian Express*, 28 December 2019) <<https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/>> accessed 26 May 2022.

'habitual protesters', and 'rowdy elements'.⁴⁴³ It has also been reported that while the initial focus of AFRS was on maintaining security during public events with large gatherings such as Independence Day, it soon expanded to other law and order purposes.⁴⁴⁴

Lack of legislative authorisation

CCTNS was approved by the Cabinet Committee on Economic Affairs in 2009,⁴⁴⁵ and the AFRS was approved by the 'CCTNS Cabinet Note of 2009'.⁴⁴⁶ Neither is supported by an anchoring legislation that authorises the deployment of facial recognition, and therefore, neither is likely to pass the test of legality in *Puttaswamy*. Cabinet notes are not legal authorisations that can justify the restriction of fundamental rights.⁴⁴⁷

In December 2021, the Minister of State for Home Affairs informed Parliament that facial recognition is regulated by the IT Act,⁴⁴⁸ even though no specific provision of the IT Act regulates facial recognition. To the extent that the IT Act regulates facial recognition, it is through its classification of facial recognition data as sensitive personal data, under Section 43A and the IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. However, these Rules and Section 43A apply to private entities and do not apply to the government, and hence, cannot be relied upon to suggest statutory authorisation for government collection of facial images and facial data of citizens.

It is also unclear whether facial recognition technology satisfies the standards of accessibility and foreseeability, essential requirements to satisfy the test of legality. For example, the U.K. Court of Appeal struck down the use of facial recognition technology by the Southwest Police in *R vs. Ed Bridges*, even though the U.K. had enacted the Data Protection Act, 2018; a Surveillance Camera Code of Practice; and local policies on the ground. The Court held that the use of facial recognition failed the foreseeability and accessibility test, observing:⁴⁴⁹

⁴⁴³ *ibid.*

⁴⁴⁴ *ibid.*

⁴⁴⁵ 'Crime and Criminal Tracking Network & Systems (CCTNS) | National Crime Records Bureau' (n 421).

⁴⁴⁶ National Crime Records Bureau, NCRB Response to IFF Legal Notice received from Internet Freedom Foundation, page 1 <<https://drive.google.com/file/d/0B3J0iAyRzCGxRXViUWcya3RXS0hXb3cxeDJYQU5DWnZKZnhj/view?resourcekey=0-DY2SxktJLnw9EkC8rZsQ9A>> accessed 31 May 2022.

⁴⁴⁷ Bhandari (n 11).

⁴⁴⁸ Ministry of Home Affairs, Answer to Unstarred Question No 1589' (Lok Sabha, 7 December 2021) <<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=29933&lsno=17>> accessed on 12 May 2022.

⁴⁴⁹ *R (Edward Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 [91].

The first is what was called the ‘who question’ at the hearing before us. The second is the ‘where question’. In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watch-list nor is it clear that there are any criteria for determining where AFR can be deployed.

At the time of writing, India has not adopted a data protection legislation, and the proposed legislation released by MEITY exempts the government and its agencies from data protection obligations on very broad grounds.⁴⁵⁰ Further, there is limited transparency and no anchoring legislation that governs the use of AFRS in India.

3. National Identity and Aadhaar

Countries across the world have begun deploying technology solutions for easy identification, authentication, and verification of individuals for various purposes. India is no exception, with the country seeking to develop a comprehensive digital ID system (a ‘Unique ID’) since 2009-10.⁴⁵¹

Although identity systems and registers existed even in the pre-digital era (such as the Population Census, National Population Register, and the National Register of Citizens), the advent of digital technologies enabling the capturing of unique biometric data encouraged the government to supplement and *effectively* substitute the older identity systems with digital technology. Biometrics are unique biological identifiers in humans, such as fingerprints, iris scans, and even facial features of an individual, and are considered unique to each individual.⁴⁵²

In 2009-2010 the Government of India introduced the Aadhaar scheme as a unique identification project, administered by the Unique Identification Authority of India, for all residents of the country. The stated purpose of the project was to reduce wastage in public welfare schemes by weeding out duplicates and individuals

⁴⁵⁰ Digital Personal Data Protection Bill, 2022 < <https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>>, clause 18.

⁴⁵¹ Unique Identification Authority of India, ‘Vision & Mission’ (Unique Identification Authority of India | Government of India) <<https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/vision-mission.html>> accessed 26 May 2022; Billy Perrigo, ‘India Is Collecting a Vast Database of Eye Scans and Fingerprint Records’ (Time, 28 September 2018) <<https://time.com/5409604/india-aadhaar-supreme-court/>> accessed 26 May 2022; ‘Aadhaar through the Years, a Quick Timeline’ (The Week, 26 September 2018) <<https://www.theweek.in/news/india/2018/09/26/aadhaar-through-the-years-quick-timeline.html>> accessed 26 May 2022.

⁴⁵² Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 [“**Aadhaar Act**”], s. 2(g).

who have passed away.⁴⁵³ The project aimed to enrol the entire population of the country by collecting demographic data (name, date of birth, address) and capturing biometric data (fingerprints, iris scans and photographs).⁴⁵⁴ After such enrolment, a unique ID number was issued along with an Aadhaar card to each individual. The biometric data was then to be used to authenticate and verify the identity of the beneficiaries of public welfare schemes.

Although Aadhaar is voluntary, it is mandatory for those residents who file income tax and those who access government welfare subsidies, benefits, or services.⁴⁵⁵ The Aadhaar Act and the accompanying regulations regulate the storage and sharing of biometric and demographic information, and the manner and purpose of using such data.⁴⁵⁶

In the *Aadhaar Judgement*, the Supreme Court struck down a portion of Section 57 of the Aadhaar Act, which permitted private companies to access the Aadhaar database and verify the identity of individuals.⁴⁵⁷ However, subsequent to this, when the Union Government amended the Act in 2019, the Government permitted private entities to verify users' identity with Aadhaar numbers on a voluntary basis, provided that they complied with privacy safeguards.⁴⁵⁸ This amendment has since been challenged before the Supreme Court.⁴⁵⁹

The establishment and provision of national identity numbers (or Aadhaar numbers) to residents in India has resulted in the creation of the world's largest centralised database of personal data – the Central Identities Data Repository – which includes sensitive personal biometric data.⁴⁶⁰ In fact, one of the grounds for challenging the constitutionality of the Aadhaar Act was that it enabled the creation of a surveillance State, where every resident could be kept under surveillance by linking everyday activities, such as banking and telecom, to their

⁴⁵³ *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [296].

⁴⁵⁴ Aadhaar Act, s. 2(h), 2(j).

⁴⁵⁵ Prevention of Money Laundering Act, 2002, s. 7. Upheld in *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1.

⁴⁵⁶ Aadhaar Act, s. 29, 32(1), 33, Aadhaar (Authentication) Regulations 2016, r. 18(2) and 18(3); Aadhaar (Data Security) Regulations, r. 3(2).

⁴⁵⁷ *K S Puttaswamy (Aadhaar 5J) v Union of India* (2019) 1 SCC 1 [257].

⁴⁵⁸ 'What Has Been Changed in the Aadhaar Amendment Bill?' (SFLC.in, 1 August 2019) <<https://sflc.in/what-has-been-changed-aadhaar-amendment-bill>> accessed 27 February 2023.

⁴⁵⁹ 'SC Issues Notice On Plea Against Amendment Allowing Use Of Aadhaar Data By Private Entities' (n 275).

⁴⁶⁰ Siobhan Heanue, 'Aadhaar, the World's Largest Biometric Identity Database, Approved by India's Supreme Court' *ABC News* (26 September 2018) <<https://www.abc.net.au/news/2018-09-26/aadhaar-biometric-identity-database-approved-by-indian-court/10309052>> accessed 26 May 2022.

Aadhaar number.⁴⁶¹

The petitioners also challenged the seeding of Aadhaar in several distinct databases, which would result in the aggregation of data silos, enabling the State to create accurate and complete profiles of individuals and thereby violate their privacy. Finally, the petitioners argued that records about authentication of Aadhaar numbers and other identity information could enable tracking and surveillance of individuals, and reveal information about their geographic location.⁴⁶²

However, the majority opinion in the *Aadhaar Judgment* rejected these submissions and held that the Aadhaar scheme did not result in the creation of a surveillance State, nor did it help the State create profiles of individuals (simply on the basis of their identity information).⁴⁶³ In his dissent, Chandrachud J. disagreed with this conclusion, holding that the “architecture of Aadhaar poses a risk of potential surveillance activities through the Aadhaar database.”⁴⁶⁴ He noted that “when Aadhaar is seeded into every database, it becomes a bridge across discreet data silos, which allows anyone with access to this information to re-construct a profile of an individual’s life. This is contrary to the right to privacy and poses severe threats due to potential surveillance.”⁴⁶⁵

Many scholars and activists also raised concerns about the surveillance being enabled by Aadhaar and criticised the Court’s conclusions on surveillance, raising concerns regarding the linking of Aadhaar data across different databases to consolidate information about an individual.⁴⁶⁶

These concerns of surveillance, particularly of linking Aadhaar data, also seem to be borne out by recent reports regarding the linking of Aadhaar data with various programs. For instance, there have been multiple ground reports about India’s ‘CoWin’ (COVID-19) vaccination portal being allowed to use Aadhaar data without

⁴⁶¹ K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1 [2].

⁴⁶² K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1 [164] (Sikri J).

⁴⁶³ K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1 [931].

⁴⁶⁴ K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1 [1539] (Chandrachud J).

⁴⁶⁵ K S Puttaswamy (*Aadhaar 5J*) v Union of India (2019) 1 SCC 1 [1539] (Chandrachud J).

⁴⁶⁶ Jean Dreze, ‘Dissent and Aadhaar’ (*The Indian Express*, 8 May 2017) <<https://indianexpress.com/article/opinion/columns/dissent-and-aadhaar-4645231/>> accessed 26 May 2022; Vrinda Bhandari and Renuka Sane, ‘A Critique of the Aadhaar Legal Framework’ (2019) 31 *National Law School of India Review* 1; Usha Ramanathan, ‘Privacy Activist Usha Ramanathan On How Aadhaar Has Taken Over Our Lives’ (*HuffPost*, 26 September 2019) <https://www.huffingtonpost.in/entry/one-year-after-aadhaar-judgement-we-are-still-not-listening_in_5d8bb628e4b0ac3cdda24659> accessed 26 May 2022.

proper notice or consent from the individuals.⁴⁶⁷

More recently, in December 2021, the Union Government amended the Representation of People Act, 1951 to facilitate the linking of an individual's Aadhaar number with their electoral roll data if it is 'required'.⁴⁶⁸ The amendment states that an individual's name cannot be deleted from the electoral roll, nor can an individual be denied inclusion on the voter roll solely due to their inability to provide their Aadhaar number.⁴⁶⁹ However, to avoid being excluded from the electoral roll, individuals must demonstrate "such sufficient cause as may be prescribed" as to why they are unable to provide their Aadhaar identity.⁴⁷⁰ The accompanying regulation to this amendment have not yet been prescribed, so there is no clarity on what may be considered a "sufficient cause" for not sharing one's Aadhaar identity.

4. National Health Stack

The NITI Aayog, the Government's premier think-tank, released a consultation paper about a proposed National Health Stack ("NHS") that would serve as the base for a digital health technology ecosystem. The National Health Stack is envisaged as a platform that would "seamlessly link to support national health electronic registries, a coverage and claims platform, a federated personal health records framework, a national health analytics platform as well as other horizontal components."⁴⁷¹ The base data for the platform would consist of individual health records that would be logged at primary health care centres in rural and urban areas.

The NHS is intended to help the government's flagship initiative for achieving universal health coverage, the Ayushman Bharat Yojana, and is meant to facilitate seamless data portability and access, so people can be covered and receive health care anywhere in the country. Thus, the National Health Stack is envisaged as a 'set of building blocks' that is essential for healthcare service delivery as a common

⁴⁶⁷ Advait Palepu, 'Understanding The Government's Push For Aadhaar Linkage With CoWIN' (MediaNama, 8 June 2021) <<https://www.medianama.com/2021/06/223-national-health-id-aadhaar-cowin-vaccination/>> accessed 26 May 2022; Smriti Parsheera, 'As Health Goes Digital in India, Where Does Privacy Stand?' (Scroll.in, 20 March 2023) <<https://scroll.in/article/1045509/as-health-goes-digital-in-india-where-does-privacy-stand>> accessed 28 March 2023.

⁴⁶⁸ The Election Laws (Amendment) Act, 2021, s. 4.

⁴⁶⁹ The Election Laws (Amendment) Act, 2021, s. 4.

⁴⁷⁰ The Election Laws (Amendment) Act, 2021, s. 4.

⁴⁷¹ NITI Aayog, 'National Health Stack: Strategy and Approach' (2018) 5 <https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Documents-for-consultation.pdf>

public goods.⁴⁷²

The NHS consists of:

- National Health Electronic Registries, a master health data set for the nation;
- a Coverage and Claims platform, a platform to support and expand government health insurance schemes and facilitate fraud detection;
- a Federated Personal Health Records Framework, to facilitate access to personal health data by patients, as well as make it available for medical research;
- a National Health Analytics Platform for initiatives such as predictive analytics to support smart health policy making; and
- other components that will include Digital Health ID, Health Data Dictionaries, and a payments gateway shared by all health programs.⁴⁷³

The Digital Health ID is meant to provide voluntary unique identification for every user participating in the system. Enrolment can take place using government issued IDs such as Aadhaar, and once an individual is enrolled, the Digital Health ID can be used to access services. A potential area for concern is that the project contemplates interlinking the Digital Health ID and Aadhaar, since the document also states that even without the Digital Health ID, a user can be identified and verified using their Aadhaar if necessary, for the purposes of accessing services.⁴⁷⁴

There are numerous privacy issues in the proposed National Health Stack and Digital ID. To begin with, the absence of clear guidelines regarding data anonymization and utilisation may potentially imperil the privacy of the patient. Without an authorising legal framework, data protection law or data protection authority in place, there are few privacy safeguards to protect individuals

⁴⁷² NITI Aayog, 'National Health Stack: Strategy and Approach' (July 2018) <https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf> page 11

⁴⁷³ NITI Aayog, 'National Health Stack: Strategy and Approach' (July 2018) <https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf> page 11

⁴⁷⁴ NITI Aayog, 'National Health Stack: Strategy and Approach' (July 2018) <https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf> page 28 and 29

from misuse.⁴⁷⁵ While the NHS Blueprint (the architectural document for the implementation of the NHS) states that patient data will be anonymized at the time of sharing with Health Data Fiduciaries, it does not place any restrictions on how private entities may use this data or explain how this anonymization process will take place.⁴⁷⁶

Moreover, the NHS Blueprint states that user consent will be obtained – either through One Time Passwords or Aadhar verification. Although this requirement is a step in the right direction, the Government must ensure that the consent given is ‘informed consent’. That means making sure that patients are properly aware of the risks associated with disclosing their health data.

Finally, the NHS Blueprint envisions the development and use of Application Programming Interfaces (APIs) by service providers. This approach poses a threat to user privacy as there have been numerous instances where sensitive data has been leaked through unsecured APIs.⁴⁷⁷ There are further associated security concerns with storing the health data of Indians on the NHS, including a risk to national security.⁴⁷⁸ Therefore, it is essential to integrate checks and balances into the NHS to ensure patient data is protected and concerns of profiling, surveillance, and misuse of sensitive health data are addressed.

5. National E-Transport Project

The purpose of the National E-Transport Project is three-fold: (i) digitize existing manual information on vehicle registration and drivers’ licenses in Road Transport Offices all across the country; (ii) automate and deploy standardized software across India for such vehicle registration and drivers’ licenses; and (iii) compile these databases of registrations and licenses into a state registry and a national

⁴⁷⁵ Prasad Banerjee, ‘Digital Health IDs Face Privacy Challenge’ (*mint*, 6 September 2021) <<https://www.livemint.com/technology/tech-news/digital-health-ids-face-privacy-challenge-11630867394534.html>> accessed 26 May 2022; Srinivas Kodali, ‘Why National Health ID Without Laws Is Another “Aadhaar Fiasco”’ (*The Quint*, 10 September 2020) <<https://www.thequint.com/voices/opinion/national-health-id-national-health-data-management-policy-aadhaar-data-privacy-information-technology-industry>> accessed 26 May 2022.

⁴⁷⁶ Mithun MK, ‘The Risks of Storing Health Records of 1.3 Billion Indians on the National Health Stack’ (*The News Minute*, 20 October 2021) <<https://www.thenewsminute.com/article/risks-storing-health-records-13-billion-indians-national-health-stack-156707>> accessed 26 May 2022.

⁴⁷⁷ Ericka Chickowski, ‘2018 Sees API Breaches Surge With No Relief in Sight’ (*Security Boulevard*, 4 December 2018) <<https://securityboulevard.com/2018/12/2018-sees-api-breaches-surge-with-no-relief-in-sight/>> accessed 28 March 2023.

⁴⁷⁸ Suprita Anupam, ‘National Health Stack: ISPIRT’s Attempt To Replicate India Stack (Deja Vu Anyone?)’ (*Inc42 Media*, 18 July 2020) <<https://inc42.com/features/national-health-stack-ispirts-attempt-to-replicate-india-stack-deja-vu/>> accessed 26 May 2022; MK (n 476).

registry.⁴⁷⁹ As a part of its mission statement, the National E-Transport Project also aims to introduce a smart card system for recording and authorising the inter-state movement of transport vehicles.⁴⁸⁰

A significant consequence of the National E-Transport Project was the development and popularisation of databases like *Vahan* (for vehicular registration) and *Sarathi* (for driving licenses).⁴⁸¹ *Vahan* provides easy access to any individual who wishes to verify details of a vehicle with its license plate, including any outstanding payments, challans, or if it is stolen property.⁴⁸² However, the mass centralisation and open access nature of data on *Vahan* creates a potential for surveillance and misuse.

For instance, there were many reports that during the Delhi riots in 2020, *Vahan* was used to selectively identify and vandalize vehicles belonging to the Muslim community.⁴⁸³ Subsequently, the Ministry of Road Transport and Highways informed the media that it was working to partially conceal the names of vehicle owners on the *Vahan* database.⁴⁸⁴

The Ministry of Road Transport & Highways released a Bulk Data Sharing Policy in 2019, that contemplated sharing anonymised data with investigative agencies and

⁴⁷⁹ National Informatics Centre, 'eTransport' <<https://www.nic.in/products/etransport/>> accessed 21 July 2021; Ministry of Road Transport and Highways (Parivahan Sarathi) <<https://sarathi.parivahan.gov.in/SarathiReport/sarathiHomePublic.do>> accessed 21 July 2021.

⁴⁸⁰ Ministry of Road Transport and Highways (Parivahan Sewa) 'About Us' <<https://parivahan.gov.in/parivahan/en/content/about-us>> accessed 21 July 2021.

⁴⁸¹ National Informatics Centre, 'e-Transport MMP: Steering a Smart Generation' (2019) 2 <https://informatics.nic.in/uploads/pdfs/15dd6ff0_2128_if_etransport.pdf> accessed 31 May 2022.

⁴⁸² Ministry of Road Transport and Highways, *Vahan* NR e-Services, 'Know Your Vehicle Details' <<https://vahan.nic.in/nrservices/faces/user/citizen/citizenlogin.xhtml>> accessed 21 July 2021; *Vahan* Citizen Service, 'Know Your Pending eChallan/Blacklist Details' <https://vahan.parivahan.gov.in/vahanservice/vahan/ui/appl_status/form_Know_Regn_Status.xhtml> accessed 31 May 2022.

⁴⁸³ Aihik Sur, 'Delhi Violence: Miscreants Use Apps to Find RTO Data to Target People' (*The New Indian Express*, 27 February 2020) <<https://www.newindianexpress.com/states/telangana/2020/feb/27/delhi-violence-miscreants-use-apps-to-find-rto-data-to-target-people-2109051.html>> accessed 26 May 2022; Sreemoyee Mukherjee, 'How Poor Data Protection Can Endanger Communities During Communal Riots' *The Wire* (6 March 2020) <<https://thewire.in/rights/vahan-database-protection-riots>> accessed 26 May 2022.

⁴⁸⁴ Nishtha Saluja, 'Transport Ministry to Partially Conceal Names of Vehicle Owners on *Vahan* Database' *The Economic Times* (27 February 2020) <<https://economictimes.indiatimes.com/news/economy/policy/transport-ministry-to-partially-conceal-names-of-vehicle-owners-on-vahan-database/articleshow/74338287.cms?from=mdr>> accessed 26 May 2022.

private entities such as automobile industries, banks, and finance companies.⁴⁸⁵ Under this policy, access to the *Vahan* and *Sarathi* databases had been shared with various law enforcement agencies, the Home Ministry, finance, insurance and freight organisations, and automobile manufacturers, which generated stated revenues of over Rs. 100 crores for the Union Government.⁴⁸⁶

The policy was criticised on various privacy-related grounds, including because it enabled the triangulation of data (by linking the *Vahan* or *Sarathi* database with other datasets), thus permitting the identification of individuals – which could result in discrimination such as an increase in insurance premiums.⁴⁸⁷

Although it was intended to support the transport and automobile industry, the policy was recalled by the Ministry in June 2020, citing reasons of potential misuse of personal information and privacy concerns.⁴⁸⁸ While this is a welcome move, the surveillance risks from *Vahan* and *Sarathi* still exist.

More worryingly, the Union Government has clarified that although the Bulk Data Sharing Policy had been discontinued, there is no proposal ‘under consideration’ for seeking the deletion of the data that had already been shared with, or collated by private entities.⁴⁸⁹ Other privacy concerns have also been raised regarding the new FASTag system, which centralises all data collection with the Union Government and banks, captures photographs, and links vehicle data with bank accounts.⁴⁹⁰

485 Ministry of Road Transport and Highways, Bulk Data Sharing Policy & Procedure (No. RT-11036/46/2014-MVL) (2019) Clause 2 <<https://parivahan.gov.in/parivahan/sites/default/files/NOTIFICATION%26ADVISORY/8March%202019.pdf>> accessed 31 May 2022; ‘Centre Made Rs 100 Crore by Sharing Vehicle Data with Private Companies: Nitin Gadkari’ (*Business Today*, 12 February 2021) <<https://www.businesstoday.in/latest/economy-politics/story/centre-made-rs-100-crore-by-sharing-vehicle-data-with-private-companies-nitin-gadkari-287427-2021-02-12>> accessed 26 May 2022.

486 *ibid.*

487 Shashidhar K J, ‘An Assessment of the Bulk Data Sharing Policy of the Ministry of Road Transport and Highways’ (Observer Research Foundation 2019) <https://www.orfonline.org/wp-content/uploads/2019/12/ORF_IssueBrief_332_DataSharing.pdf> accessed 26 May 2022.

488 Nishtha Saluja, ‘Transport Ministry Scraps Bulk Data Sharing Policy’ *The Economic Times* (24 June 2020) <<https://economictimes.indiatimes.com/industry/auto/auto-news/transport-ministry-scraps-bulk-data-sharing-policy/articleshow/76549779.cms?from=mdr>> accessed 26 May 2022.

489 ‘Centre Made Rs 100 Crore by Sharing Vehicle Data with Private Companies: Nitin Gadkari’ (n 485).

490 Aman Rawat, ‘Gadkari’s Surveillance Comments Raise Privacy Concerns Around E-Toll Collection’ (*Inc42 Media*, 15 October 2019) <<https://inc42.com/buzz/gadkaris-surveillance-comments-raise-privacy-concerns-around-e-toll-collection/>> accessed 26 May 2022; Srikanth Lakshmanan, ‘FASTag: Will Datafication of India’s Tolls Boost Highway Development?’ *The Wire* (14 December 2019) <<https://thewire.in/political-economy/fastag-will-datafication-of-indias-tolls-boost-highway-development>> accessed 26 May 2022.

6. Digi Yatra

Digi Yatra is an initiative by the Ministry of Civil Aviation that emerged out of the need to digitise passenger air travel for maximising efficiency. The Digi Yatra project is a voluntary facial recognition tool for quick identification of passengers for air travel, by linking facial recognition with the ticket and the boarding pass of a passenger. Digi Yatra is intended to transform air travel by eliminating the requirement of a ticket, boarding pass, or an identity document at various check points inside the airport. This system is meant to reduce queue times, enable faster and simpler processing, and make the process seamless, paperless, and hassle free.⁴⁹¹ As per the Ministry of Civil Aviation, the first phase of Digi Yatra is planned to be implemented at Kolkata, Varanasi, Pune, Vijayawada, Bangalore, Delhi, and Hyderabad Airports by March 2023.⁴⁹²

The service will be operated by way of a Common Digi Yatra Platform, to be built like a shared national infrastructure with offering services such as enrolment, authentication, consented profile sharing, and accessibility for airports and applications to integrate on the platform.⁴⁹³ The long-term goal of the project is to integrate digital and biometric solutions in the process of entering and leaving airports. Passengers have the option of linking their Aadhaar numbers to airlines for faster airport entry and automated check-ins.⁴⁹⁴

While Digi Yatra is currently voluntary, there is a concern that the two-tiered model of services provided will actively encourage passengers to link their Aadhaar and consent to facial recognition, without fully realising or being informed of the risks of providing such sensitive personal information to the State.

⁴⁹¹ Ministry of Civil Aviation, 'Digi Yatra: Reimagining Air Travel in India' (9 August 2018) 6-7 <<https://www.civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf>> accessed 31 May 2022.

⁴⁹² Ministry of Civil Aviation, Answer to Unstarred Question No 3532 (Rajya Sabha, 4 April 2022) <<https://www.medianama.com/wp-content/uploads/2022/04/AU3532.pdf>> accessed 31 May 2022; Ministry of Civil Aviation, 'Facial Recognition System(FRS) Is to Be Implemented in Phased Manner' (Press Information Bureau, 4 April 2022) <<https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1813139>> accessed 26 May 2022.

⁴⁹³ Ministry of Civil Aviation, 'Digi Yatra: Reimagining Air Travel in India' (9 August 2018) 10-11 <<https://www.civilaviation.gov.in/sites/default/files/Digi%20Yatra%20Policy%2009%20Aug%2018.pdf>> accessed 31 May 2022.

⁴⁹⁴ 'Digi Yatra- A New Digital Experience for Air Travellers| National Portal of India' (*India.gov.in*) <<https://www.india.gov.in/spotlight/digi-yatra-new-digital-experience-air-travellers>> accessed 26 May 2022.

7. Criminal Procedure (Identification) Act, 2022

In April 2022, India adopted the Criminal Procedure (Identification) Act, 2022. The Act empowers the government to collect “measurements” from any persons who have been arrested for an offence, detained under a preventive detention statute, or convicted of an offence.⁴⁹⁵ “Measurements” can include “*finger impressions, palm-print impressions, foot-print impressions, photographs, iris and retina scan, physical, biological samples and their analysis, behavioural attributes including signatures, handwriting.*”⁴⁹⁶ However, only individuals who have been arrested for offences against women or children or offences punishable by imprisonment for more than seven years are compelled to provide biological samples.⁴⁹⁷

The NCRB can collect, store, process, and share the information collected for the purposes of crime prevention, detection, investigation, or prosecution.⁴⁹⁸ Records may be stored for up to seventy-five years from the date of collection.⁴⁹⁹ However, where a person who had their “measurements” recorded has: (i) not been previously convicted of an offence; (ii) and is released without trial (or discharged or acquitted); their records may be destroyed unless a court (for reasons recorded in writing) directs otherwise.⁵⁰⁰

The collection of personal data such as fingerprints and retina scans for the purpose of identifying individuals is an interference with individual privacy, and therefore, like the other measures discussed here, must satisfy the test of proportionality. Experts have characterised the Act as disproportionate, particularly due to: (i) the broad range of individuals who could have their “measurements” taken, even where the taking of such “measurements” has no nexus with crime prevention; and (ii) the extended time for which the information may be retained by the State.⁵⁰¹ They also note that in the absence of a data protection law, the potential for the misuse of such personal data is high.⁵⁰²

⁴⁹⁵ Criminal Procedure (Identification) Act, 2022, s. 3.

⁴⁹⁶ Criminal Procedure (Identification) Act, 2022, s. 2(1)(b).

⁴⁹⁷ Criminal Procedure (Identification) Act, 2022, s. 3 (proviso).

⁴⁹⁸ Criminal Procedure (Identification) Act, 2022, s. 4(1).

⁴⁹⁹ Criminal Procedure (Identification) Act, 2022, s. 4(2).

⁵⁰⁰ Criminal Procedure (Identification) Act, 2022, s. 4(2) (proviso).

⁵⁰¹ ‘An Analysis of the Criminal Procedure (Identification) Act, 2022’ (Project 39A 2022) <<https://static1.squarespace.com/static/5a843a9a9f07f5ccd61685f3/t/634d22c3b82adb4257926c79/1665999595973/P39A+Brief+-+Criminal+Procedure+%28Identification%29+Act%2C+2022+%281%29.pdf>> accessed 27 February 2023.

⁵⁰² *ibid.*



978-93-84272-43-2