INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

FROM SURVEILLANCE TO SECURITY: A CRITICAL STUDY OF TELECOM LAWS IN COUNTERING CYBER TERRORISM IN INDIA

AUTHORED BY - ADITHYA V S

Abstract

India's telecommunications system has grown over the years, this is done by modernizing governance and national security, aside from this it also fights cyber terrorism. This paper learns the role of Indian telecommunications laws mainly that are from the Indian Telegraph Act, 1885 and Information Technology Act, 2000, in understanding the use of surveillance as a method for fighting cyber terrorism. In this paper we compare and learn between "surveillance" employed as a way of monitoring versus "security" in a category of protective measures, this is done by showing potential conflict between state power and individual liberty.

Using a doctrinal and analytical approach this paper finds whether telecom surveillance can fight cyber terrorism and figure out various concerns including encryption, cross-border data transfer and technological limitations. Issues related to constitutionality, mainly, the issue of privacy that comes under Article 21 and lack of good judicial oversight are also checked. Findings show that even though surveillance systems equip the government with many capabilities there is no base to support the that the surveillance is good at fighting cyber terrorism. Due to these systems being too susceptible to the risk of government overreach.

The paper expresses that the current surveillance-centric model should shift to a more balanced, security-centric system that includes legal safeguards, technological preparedness and multi-stakeholder collaboration. It concludes by recommending legislative reform, enhanced accountability mechanisms, and the development of comprehensive cybersecurity strategies that respect fundamental rights while addressing emerging threats.

Keywords: Cyber Terrorism, Telecom Surveillance, Privacy, National Security, Indian Telecom Law.

1. Introduction

India's socio-economic and security situation has drastically altered by the rapid proliferation of both digital communications technology and telecom infrastructure. India currently has over one billion mobile subscribers and has seen enormous growth in the number of people with access to the Internet; therefore, telecom networks now represent the foundation of how all governments conduct their business, how consumers transact with companies, and how people communicate with friends or family members.[1] The dramatic and unprecedented growth of arrestees has resulted in an increase in the number of potential targets for ER tumors and others attempting to cause harm through cyber terrorism. Cyber terrorism is the use of computers and the Internet to use acts of terrorist violence. Cyberterrorism is aimed on the use of telecom services to communicate, coordinate recruit new members and send deceptive messages to a large number of audiences.[2] As a result, the Indian government has increasingly relied upon telecom-based surveillance techniques (e.g., intercepting phone calls, collecting metadata, monitoring Internet traffic, etc.) as an instrument within its overall anti-terrorism strategy.[3]

It is important to differentiate between the concepts of "surveillance" and "security." Surveillance is the observation and collection of data, often conducted in advance of threats, to identify them. Security is a wider concept to prevent and protect individuals and the state from suffering harm.[4] While surveillance can be a tool used to facilitate security, they are not synonymous concepts. The difference between these two concepts is of particular importance in democratic societies, as surveillance powers get expanded, and such expansion includes concerns about privacy and autonomy, freedom of speech, etc. The relationship between national security requirements and civil liberties has also been well-debated especially considering constitutional protections afforded

[1] Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators* (2023).
[2] Maura Conway, *Cyberterrorism: Reality, Rhetoric and Capability*, 7 First Monday (2002).
[3] Information Technology Act, 2000, §§ 69, 69A, 69B (India).
[4] David Lyon, *Surveillance Studies: An Overview* 13–15 (2007).

by Article 21 of the Indian Constitution, as held in the case of Justice K.S. Puttaswamy v. Union of India.[5]

The focus of this current research is to investigate an emerging issue: there is very little clarity if the surveillance powers provided to the state under Indian telecom laws (Indian Telegraph Act, 1885 and Information Technology Act, 2000) are providing adequate deterrents against cyber terrorism or if that they provide a source for state intrusion beyond what is legally justified.[6] One of the major issues related to the increasing normalisation of surveillance is the issues of proportionality, accountability, and the uses that may result from surveillance; this is especially true where there is an absence of any real oversight of the use of surveillance.[7]

The aim of this research is to answer three main questions. First, how do Indian telecommunications laws facilitate surveillance to combat cyber terrorism? Second, is the existing system of surveillance effective in accomplishing its intended objectives as a security measure? Third, do this surveillance frameworks provide an adequate balance with the fundamental rights of privacy and free expression?
There are three main objectives of this study: to analyse the telecommunications law framework governing surveillance of telecommunications in India; to determine the effectiveness of the legal framework in addressing cyber terrorism; and to evaluate the constitutional and ethical implications of providing surveillance of telecommunications.

This study will be limited to examining the legal framework for surveillance of telecommunications in India, so there will be only limited reference to other jurisdictions (i.e., comparative analysis) where relevant. This study will focus specifically on telecommunications laws and the role of such laws in enabling surveillance, rather than examining the broader issues of cybersecurity regulation. Due to the limited availability of publicly accessible materials on surveillance practices and cyber terrorism cases in India, there will be limitations to the empirical evaluation of this study.

[5] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
[6] Indian Telegraph Act, 1885, § 5(2) (India); Information Technology Act, 2000, § 69.
[7] Usha Ramanathan, *Privacy and the Constitution*, 3 Nat'l L. Sch. India Rev. 127 (2010).

2. Literature Review

Current academic literature on telecommunications surveillance and cyberterrorism consists of an interdisciplinary collection of works that include legal theory, technology governance, and security studies. The study of surveillance has provided an important theoretical basis to understand how the state exercises its forms of power in the digital age. Scholars such as Michel Foucault view surveillance as a means of discipline, control, and the continued power of the state through active observation.[8] David Lyon further develops this idea, asserting that modern forms of digital surveillance are embedded within our everyday technological communication infrastructures extending beyond traditional roles of government, and therefore enabling governments to monitor large amounts of data.[9] This creates an ongoing debate in the context of cyber governance regarding "security versus liberty," where governments justify the expansion of their surveillance powers citing national security, often at the expense of individual liberty.[10] Conversely, legal scholars argue that the potential for government abuse must be measured against the constitutional protections available to individuals to prevent excessive use of government powers.[11]

Cyber terrorism is a growing and important academic field of study; however, while definitions exist there is currently no agreed-upon definition of what constitutes cyber terrorism, though it is understood that cyber terrorism involves the use of ICTs to commit or threaten violence or disruption for an ideological/political reason.[12] According to scholars such as Maura Conway, the fear of cyber terrorism has largely been based on exaggerated fears of mass scale attacks. In fact, Conway argues that digital tools (such as computers, tablets, and smartphones) have become increasingly sophisticated over time; therefore terrorist organisations have been able to use ICTs to help organise their crimes through communication networks.[13] Another scholar, Gabriel Weimann, states how the use of Internet and telecommunications networks has played an important role in allowing terrorists to operate without central authority and across national borders, significantly increasing the complexity of counter-terrorism efforts due to all the new

[8] Michel Foucault, *Discipline and Punish: The Birth of the Prison* 195–228 (Alan Sheridan trans., 1977).
[9] David Lyon, *Surveillance Studies: An Overview* 21–45 (2007).
[10] Jack M. Balkin, The Constitution in the National Surveillance State, 93 Minn. L. Rev. 1 (2008).
[11] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 131–34 (2012).
[12] Dorothy E. Denning, Cyberterrorism, 23 Georgetown J. Int'l Aff. 29 (2000).
[13] Maura Conway, Against Cyberterrorism, 8 Commc'ns ACM 21 (2017).

technologies being used today. Many studies highlight how telecommunications infrastructure has played an enabling role in facilitating cyber terrorism as well as being a site for potential regulation.[14]

The Indian legal framework for telecom surveillance is based on colonial-era law and later added to, with new laws introduced in the modern era. The Indian Telegraph Act of 1885 gives the government with powers to intercept communications for reasons of public safety and national security.[15] The system is made stronger using various provisions in Sections 69, 69A and 69B of the Information Technology Act of 2000 which allow the state to intercept, monitor, decrypt and block digital communications.[16] Aside from this, the Intermediary Guidelines and Digital Media Ethics Code Rules 2021 makes sure that due diligence duties of intermediaries and compliance with the governments requests to remove data.[17] Many researchers have said that the nature of these provisions allows for potential abuse, as the regulations do not provide sufficient procedural safeguards.[18]

Judicial developments are major when it comes to the development of the various laws that are around surveillance as shown by the landmark ruling of Justice K.S. Puttaswamy v. Union of India regarding concerns of privacy this ruling made for privacy as a fundamental right according to Article 21 of the Constitution.[19] Besides this the Supreme Court has made considerations regarding proportionality: all state actions that limit or infringe on privacy must be determined through a proportionality standard with regard to legality, necessity, and proportionality.[20] The response from scholars has included analysis on how each of these principles is applied to surveillance mechanisms in India, and how current Indian laws do not adequately provide for oversight, checks upon the power to collect information by governmental authorities or for accountability.[21] The

[14] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* 69–102 (2006).
[15] Indian Telegraph Act, 1885, § 5(2) (India).
[16] Information Technology Act, 2000, §§ 69, 69A, 69B (India).
[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India.
[18] Apar Gupta & Raman Jit Singh Chima, Internet Shutdowns and Freedom of Expression in India, 9 Indian J.L. & Tech. 1 (2013).
[19] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
[20] Id.
[21] Gautam Bhatia, *Privacy in the Age of the Internet: Indian Constitutional Law and the Right to Privacy*, 5 NUJS L. Rev. 1 (2012).

available literature that compares other countries and jurisdictions reveals how these countries/jurisdictions structure their surveillance laws with respect to national security. In the United States, for example, the USA PATRIOT Act has significantly increased the power of the government to engage in surveillance since the 9/11 attacks due to the government's ability to collect bulk data and monitor individuals at expanded levels;[22] in addition to this, the United Kingdom has an entire act dedicated to surveillance—The Investigatory Powers Act of 2016—containing provisions for, among other things, bulk interception and bulk data retention and judicial oversight.[23] Although there is concern about the level of surveillance power provided through these frameworks, there exists a competing concern regarding how those frameworks contain additional checks and balances in place by virtue of the judicial oversight. Therefore, both the examples of the U.S. and U.K.'s surveillance law provide useful analysis for India.[24]

Although there is an abundance of literature available regarding surveillance law in India, there remains a vast research void. Most of the available scholarship regarding surveillance law in India has a broad emphasis related to intermediary liability or privacy, with not much consideration focused specifically on telecommunications laws as countermeasures for cyber terrorism.[25] Additionally, very little empirical and doctrinal analysis exists regarding whether or not surveillance measures established pursuant to telecommunications frameworks (i.e., those that impose limitations for the purpose of compliance with law enforcement investigations) provide the desired result of improving security, or whether they place undue limitations on fundamental rights.[26] As such, this study illustrates the need for a focused and critical analysis of telecommunications laws regarding telecommunications surveillance explicitly in connection with cyber terrorism.

[22] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.
[23] Investigatory Powers Act 2016, c. 25 (UK).
[24] Christopher Kuner et al., Systematic Government Access to Private-Sector Data, 2 Int'l Data Privacy L. 1 (2012).
[25] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015).
[26] Lawrence Lessig, *Code and Other Laws of Cyberspace* 120–25 (1999).

3. Methodology

Utilising a combination of both a doctrinal research approach which identifies "Black Letter Law" and a critical analysis approach to better ascertain the role that telecommunications laws play in counteracting cyber terrorism in India. Black Letter Law is where one studies legal provisions, principles or precedents as these occur in statutes or judgements. "Black Letter Law" analysis will be beneficial for conducting the present study because this analysis method facilitates a complete analysis of both relevant statutes and judicial decisions related to the Telecommunications Act's regulation of surveillance and its constitutional implications.[27] In addition, a critical analysis methodology will permit the researcher to assess whether the telecommunications laws enacted by the Government of India provide sufficient barriers against expanding state surveillance powers prior to authorising state surveillance activities.[28]

In order to analyse the legal requirements for the telecommunications surveillance framework in India, this study uses primary and secondary sources. Primary sources consist of key legislative instruments (the Indian Telegraph Act, 1885, and the IT Act, 2000) which form the foundation of the telecommunications surveillance framework in India.[29] Both of these statutes are learned along with sections of the IT Act, e.g., 69, 69A and 69B this includes interception, monitoring and blocking of digital communications, which is relateed to interception and monitoring of digital communications and blocking digital communications.[30]

Judicial decisions related to privacy, surveillance or national security. Justice K. S. Puttaswamy v. Union of India, which shows the influence of constitutional principles on state surveillance abilities, it also provides an understanding of how state surveillance are limited by the constitution-based principles.[31]

Secondary sources are very important in providing context and insight into primary legal sources. Secondary sources can take many forms this can include peer-reviewed journal articles, academic

[27] Terry Hutchinson, Doctrinal Research: Researching the Jury, 3 Int'l J.L. Context 221, 223–25 (2007).
[28] Upendra Baxi, The Rule of Law in India, 6 Sur Int'l J. Hum. Rts. 7 (2007).
[29] Indian Telegraph Act, 1885 (India); Information Technology Act, 2000 (India).
[30] Information Technology Act, 2000, §§ 69, 69A, 69B (India).
[31] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

commentaries, government reports and policy papers which is related to surveillance, cyber terrorism and digital governance.[32] These secondary sources provide an analysis of how surveillance systems work and they provide detailed data on the success of surveillance systems and the impact of such frameworks. Together, primary and secondary sources are integrated to provide a thorough understanding of both the legal framework and the practical effects of that framework on citizens.

This study employs a tripartite analytical framework. The first part is a review of relevant statutory provisions to determine the scope and meaning of these laws, including those relevant to telecommunications support for surveillance.[33] The second part is a constitutional analysis using the proportionality test, as established by the Supreme Court of India, for assessing whether any restriction on fundamental rights is valid.[34] That test determines whether there is a rational relationship between national security interests and individual rights and how to balance the two principals.[35] The third part is an incomplete comparative analysis focusing on regulation of surveillance in the US and UK to derive applicable lessons for India.[36]

While useful, the above framework has inherent limitations. The first limitation pertains to the government's limited transparency regarding its surveillance operations, as most actions taken by government agencies related to surveillance are secret and cannot be disclosed.[37] The second limitation relates to the lack of publicly available statistics regarding incidents of cyber terrorism or the effectiveness of various surveillance operations in deterring such actions. The above restrictions preclude putting together any empirical analysis. Therefore, the study will rely more heavily on doctrinal and theoretical evaluation than empirical evidence.

[32] David Lyon, *Surveillance Studies: An Overview* 161–65 (2007).
[33] Rupert Cross, *Statutory Interpretation* 1–3 (3d ed. 1995).
[34] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 131–34 (2012).
[35] Christopher Kuner et al., Systematic Government Access to Private-Sector Data, 2 Int'l Data Privacy L. 1 (2012).
[36] Usha Ramanathan, State Surveillance and the Right to Privacy in India, 4 Nat'l L. Sch. India Rev. 127 (2010).
[37] Maura Conway, Determining the Role of the Internet in Violent Extremism and Terrorism, 6 Stud. Conflict & Terrorism 77 (2017).

4. Findings / Analysis

4.1 Understanding Cyber Terrorism in the Telecom Context

The development of digital communications networks has caused cyberterrorism to develop considerably. Telecommunication infrastructure has developed as an essential component for terrorist activities in the present day. Researchers have discovered that the use of encrypted communication channels is growing among terrorist organizations; therefore, they make use of messaging applications, VPN's, and telecommunications to communicate without the fear of detection.[38] This is especially true due to encryption providing secure transmission of sensitive information; therefore, it has become increasingly difficult for state authorities to intercept or decode communications from terrorists without advanced technological capabilities.[39]

Using telecommunications networks people often push recruitment and distribution of propaganda. Extremist organizations often take advantage of online platforms and mobile systems to communicate with many audience and target vulnerable people with narratives made for them, the best example for this is online messaging campaigns.[40] As per Gabriel Weimann, internet and mobile networks have become main tools for harming individuals and due to this it allows terrorist groups to operate on a global scale and establish a large presence online.[41] The telecommunications systems allows terrorist groups to coordinate attacks by allowing them to communicate with operatives in real-time.[42] This shows us that telecommunications are facilitators of illegal acts and due to this regulations are necessary to regulate their usage.

4.2 Telecom Surveillance Framework in India

The Indian Telegraph Act, 1885 and the Information Technology Act, 2000 govern the surveillance of telecommunications in India. Under Section 5(2) of the Indian Telegraph Act, the Indian government has the ability to intercept communication in the interests of public safety or

[38] Maura Conway, Determining the Role of the Internet in Violent Extremism and Terrorism, 6 Stud. Conflict & Terrorism 77 (2017).
[39] Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* 45–48 (2011).
[40] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* 75–90 (2006).
[41] Id.
[42] Dorothy E. Denning, Cyberterrorism, 23 Georgetown J. Int'l Aff. 29 (2000).

national security.[43] This section, while passed before the era of modern telecommunications, is still the basis for the legal interception of telephone calls; however, it raises issues of its ability to sufficiently protect public safety or national security in light of new forms of crime associated with technology such as cyber crimes.[44]

The Information Technology Act expanded the scope of state surveillance technology by allowing for the interception, monitoring and decryption of any information created, sent or stored on any computer resource. Section 69 of the Act allows for the interception, monitoring and decryption of all data on computers and on other devices.[45] In addition, Section 69A allows the government to stop the public from using certain websites or from seeing certain information based on reasons of public safety or national security. Section 69B allows for the collection and monitoring of computer traffic data for the purpose of securing cyberspace. As a whole, these provisions create a broad framework of state surveillance and monitoring of cyber activities.[46]

The Telecommunications Service Providers (TSPs) are an important component in the implementation of these surveillance policies. When ordered to do so by the state, TSPs must comply with government orders for the interception and monitoring of communications and must maintain the necessary infrastructure to provide lawful access to communications.[47] TSPs must also meet requirements for data retention so as to allow law enforcement access to stored user data during specific timeframes.[48] While these requirements provide the state more ability to monitor communications, they also raise significant issues regarding individual privacy and the security of customer data.

4.3 Effectiveness of Surveillance in Countering Cyber Terrorism

There is ongoing debate regarding the effectiveness of telecommunications surveillance for countering cyber terrorism. Supporters argue that surveillance acts as a proactive measure enabling

[43] Indian Telegraph Act, 1885, § 5(2) (India).
[44] Apar Gupta, Surveillance and the Indian Telegraph Act, 4 Indian J.L. & Tech. 1 (2011).
[45] Information Technology Act, 2000, § 69 (India).
[46] Information Technology Act, 2000, §§ 69A, 69B (India).
[47] Telecom Regulatory Authority of India, *Recommendations on Privacy, Security and Ownership of Data* (2018).
[48] Id.

law enforcement to identify and respond to suspicious activity to prevent crime before it can take place.[49] Law enforcement in many jurisdictions have attributed intelligence gathering through intercepting and monitoring to assisting them with preventing terrorist acts.[50] However, surveillance also functions reactively, responding to incidents after they have occurred, rather than preventing them from happening.[51]

Although there is limited empirical data with regard to India on the effectiveness of surveillance due to the confidential nature of intelligence operations; existing studies from around the world show that while surveillance can provide safety, several technological and operational barriers will restrict the ability of surveillance to effectively contribute to providing safety.[52] One such barrier is the prevalence of encryption and anonymizing technology, which makes it increasingly difficult for agencies to access valuable information.[53] Additionally, as digital communications cross national borders, it makes it difficult to enforce laws when the data may be transmitted or maintained outside of their jurisdiction and subject to different legal standards.[54]

Limitations in technology are barriers for using surveillance systems effectively. The amount of data generated by telecommunications is too much for any one person or location to find relevant threats without the use of sophisticated analysis tools. This raises issues of both under-inclusion (not identifying a potential threat) as well as over-inclusion (collecting a large amount of irrelevant or excess information).[55] The number of limitations technological surveillance creates indicates that reliance solely on this method may not be enough to protect against cyber terrorism.

4.4 Constitutional and Legal Concerns

The Indian Telecommunications Act's increased surveillance authority raises important constitutional issues, especially regarding Article 21's right to privacy. In K.S. Puttaswamy v.

[49] Paul Rosenzweig, Cybersecurity and Public Policy, 3 J. Nat'l Sec. L. & Pol'y 1 (2009).
[50] Id.
[51] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* 139–42 (2015).
[52] Id.
[53] Susan Landau, supra note 2, at 89–92.
[54] Christopher Kuner et al., Systematic Government Access to Private-Sector Data, 2 Int'l Data Privacy L. 1 (2012).
[55] Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* 156–60 (2013).

Union of India, the Supreme Court ruled that privacy is a fundamental right, and there are three basic principles that must be satisfied before any government agency can violate someone's privacy – legality, necessity, and proportionality.[56] However, many have criticized the existing telecommunications law provisions allowing government surveillance for failing to meet all three legal standards since there are typically no reasonable safeguards in place to protect privacy rights.[57]

Typically, one of the major concerns regarding government surveillance is that several governments across different jurisdictions require independent judicial oversight of any government intercepting order, whereas the Government of India (GoI) typically only obtains executive approval before issuing a government intercepting order, thus creating opportunities for abuse of power.[58] Many scholars believe that a lack of independent judicial oversight erodes the accountability of government agencies and increases the likelihood of arbitrary government surveillance.[59]

In addition to the issue of judicial oversight, mass surveillance creates serious problems regarding the discouragement of free speech and participation in democracy. By creating an environment where everyone is subject to mass surveillance, the government can potentially collect and analyze vast amounts of data regarding individuals not necessarily linked to any criminal activity, thereby violating fundamental rights.[24] These concerns highlight the need for a more balanced approach that safeguards both security and civil liberties.

4.5 Key Gaps Identified

The study highlights numerous deficits in the contemporary legal structure. Firstly, current law places too heavy an emphasis on using surveillance as the primary means of combating cyber terrorism and does place an appropriate amount of emphasis on implementing proactive cyber security strategies (e.g., building capacity, creating a threat intelligence programme, encouraging

[56] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
[57] Gautam Bhatia, *Privacy in the Age of the Internet* 210–15 (2019).
[58] Id.
[59] Usha Ramanathan, State Surveillance and the Right to Privacy in India, 4 Nat'l L. Sch. India Rev. 127 (2010).

international co-operation) to combat cyber terrorism.[60] Secondly, there is no clearly defined mechanism or enough safeguards to ensure accountability so that these broad, vaguely defined statutory powers will not be abused, thereby increasing the risk of being misused.[61]

Finally, the fact that there remains reliance on legislation developed for long before the advent of the internet such as the Indian Telegraph Act 1885 clearly demonstrates how far removed the current legal structure is from the realities of the modern day threat evolved through technology.[62] The fast pace with which technology develops means that a more flexible regulatory approach must be taken, including consideration for legal, technological, and policy perspectives. In the absence of such reforms, telecom laws will forever be ineffective in combating the threat of cyber terrorism as the risk of undermining fundamental rights increases.

[60] Id.
[61] Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934 (2013).
[62] Paul Rosenzweig, supra note 12.

5. Discussion

The association between surveillance and safety continues to present one of the most debated topics in modern cyber governance. States are turning increasingly towards using surveillance as a means to combat cyber terrorism; however, it is highly disputed whether the increase in the level of surveillance will actually provide an increase in safety from those types of attacks. Through both empirical and theoretical works, it has been shown that while surveillance may assist in gathering intelligence, the ability for surveillance to help in the prevention of cyber terrorist activities is significantly hampered due to structural and technological constraints.[63] Cyber terrorists execute their plots mostly by way of communication and propaganda, and they implement coordination through these various means instead of using large-scale direct cyber-attacks. This reduces the use of mass surveillance systems as a way to deter threats.[64] Also, there has been research to show that threats that are perceived to be serious will generate an increase in the public's support for surveillance even though the effectiveness of such systems cannot be determined.[65]

The increased use of surveillance creates concerns regarding the potential evolution into a "surveillance state," in which expansive monitoring powers can become commonplace.[66] Scholars assert that excessive reliance on surveillance can erode democratic values by enabling pervasive government control over individual behaviour and communication.[67] The accumulation of metadata and communications records – even without content interception – can reveal detailed patterns of individual activities, enhancing concerns regarding privacy and autonomy. In such a context, surveillance may become an end in itself, rather than an appropriate means of achieving security objectives.[68]

[63] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* 139–42 (2015).
[64] David P. Fidler, Cyberspace, Terrorism and International Law, 21 J. Conflict & Sec. L. 475 (2016).
[65] Keren L. G. Snider et al., Terrorism, Perceived Threat, and Support for Surveillance, 22 Int'l J. Env't Res. Pub. Health 1634 (2025).
[66] Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934 (2013).
[67] Bruce Schneier, Metadata = Surveillance, IEEE Sec. & Privacy (2014).
[68] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 131–34 (2012).

Therefore, it is critical to strike a balance between national security and fundamental rights. The proportionality test, which has been established in constitutional law, offers a good framework for assessing surveillance measures. This test mandates that any limitations of rights must meet three criteria: legality, necessity and proportionality.[69] As applied to telecommunications surveillance statute in India, the proportionality test reveals significant deficiencies in the existing legal framework. Although surveillance law is created by key statutes such as the Indian Telegraph Act and the Information Technology Act, there are questions about the necessity and proportionality of broad and indiscriminate surveillance authority.[70] Moreover, the absence of extensive safeguards and independent oversight further complicates the assessment of the validity of such measures.[71]

The need for surveillance as an approach to Cybersecurity should take into account other possible Cybersecurity measures. Research suggests that there is no one approach like surveillance, that will solve the complex nature of Cyber threats.[72] Therefore a combination of Technical, Organizational, and Legal measures will be needed to adequately combat these threats. Over reliance on one method like surveillance could distract authorities from developing more effective strategies through, for example; capacity building, threat intelligence sharing and international cooperation. Due to the worldwide nature of Cyber terrorism, it is often impossible for authorities to use only domestic surveillance and successfully counter or prevent Cross-Border Cyber Terrorism.[73]

The need for Oversight and Accountability is reflected in comparative experiences with different Democracy's Surveillance Frameworks.[74] Many Democracies implement quarterly judicial authorizations of Surveillance Authorizations, have a legislative process that reviews the past quarter's authorizations, and a committee that conducts independent audits of Authorizations to

[69] Usha Ramanathan, State Surveillance and the Right to Privacy in India, 4 Nat'l L. Sch. India Rev. 127 (2010).
[70] Giuseppe Cascavilla et al., Counter-Terrorism in Cyber-Physical Spaces, arXiv (2023).
[71] Yuchong Li, A Comprehensive Review Study of Cyber-Attacks and Cyber Security, 2021.
[72] Pardis Moslemzadeh Tehrani et al., Cyber Terrorism Challenges: The Need for a Global Response, 29 Comput. L. & Sec. Rev. 207 (2013).
[73] Christopher Kuner et al., Systematic Government Access to Private-Sector Data, 2 Int'l Data Privacy L. 1 (2012).
[74] International Principles on the Application of Human Rights to Communications Surveillance (2014).

ensure State powers are being used within Constitutional limits.[75] The development of International Human Rights Principles has influenced these frameworks in that they require that all authorizations for Surveillance be based upon necessity and proportionality – there exists a general consensus among Nations that Security must be balanced with Individual Rights. These attributes provide examples for India where the existing Surveillance Framework relies heavily upon Executive Approval with little or no transparency.[76]

India needs its telecom surveillance laws to be reformed from a policy standpoint. The Indian Telegraph Act (1885) will not be able address the face the complex cyber threats.[77] In order to allow legal reform to happen there needs to be a clear procedural safeguard and improved transparency. Independent oversight of the law will help remove the bad usage of surveillance powers. Cybersecurity strategies will also need more than just surveillance, it also requires measures that need to be undertaken and this is including protecting systems which involves public and private entities together and being innovative with technology.[78]

In order to sum up everything that has been stated so far, this paper shows the importance of changing from a model that is surveillance based toward a model that is focused on security and respecting rights.[79] Surveillance should one of many options we have to make counter-terrorism strategy; it should not to be the focal point. Legal protections, technology-based protections and fundamental rights should all be included for any organization to be both security effective and democratically legitimate. The continued growth of surveillance will damage the values that surveillance was created to protect if this type of transition does not take place.[80]

[75] Apar Gupta, Surveillance and the Indian Telegraph Act, 4 Indian J.L. & Tech. 1 (2011).
[76] Gautam Bhatia, *Privacy in the Age of the Internet* 210–15 (2019).
[77] Id.
[78] Leandros Maglaras et al., Threats and Protection of Cyber Infrastructures, arXiv (2019).
[79] Id.
[80] Jack M. Balkin, The Constitution in the National Surveillance State, 93 Minn. L. Rev. 1 (2008).

6. Conclusion & Recommendations

This research indicates that India's telecom laws provide vast surveillance powers to the government through legislation like the Indian Telegraph Act of 1885, and the Information Technology Act of 2000.[81] The laws permit the government to intercept, monitor, and collect data without getting the consent of any person in order to protect national security, but it is unclear whether these laws will enable the government to adequately prevent internet terrorism.[82] This study shows that the current surveillance systems can gather information for the purpose of intelligence, but their ability to gather information is limited by advancements in technology (for example, encryption) and by the global nature of cyber crimes.[83] The ability of the government to gather information in such a fashion presents both a constitutional and ethical dilemma with respect to how the government is infringing on an individual's right to privacy and because there are no effective oversight systems for the government to follow.[84]

The findings of this report lead to a number of recommendations. The first is that independent judicial oversight of surveillance authorizations needs to be implemented in order to provide accountability as well as to prevent the misuse and abuse that can come from these types of investigations.[85] The second recommendation is that there must be reform to the old laws (mainly the Indian Telegraph Act of 1885) in order to bring the legal framework for dealing with authorities that use advanced technology in line with the current technological reality.[86] The third recommendation is that the authorities should create clear frameworks for transparency and accountability, in addition to clearly defining the procedures for these types of investigations, such as creating clear mechanisms for reporting back to the judiciary.[87] In addition, the focus should be on building the capabilities of the state in technology, using proactive strategies to defend against

[81] Indian Telegraph Act, 1885, § 5(2) (India); Information Technology Act, 2000, §§ 69, 69A, 69B (India).
[82] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* 139–42 (2015).
[83] Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* 89–92 (2011).
[84] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India); Usha Ramanathan, State Surveillance and the Right to Privacy in India, 4 Nat'l L. Sch. India Rev. 127 (2010).
[85] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* 131–34 (2012).
[86] Apar Gupta, Surveillance and the Indian Telegraph Act, 4 Indian J.L. & Tech. 1 (2011).
[87] Gautam Bhatia, *Privacy in the Age of the Internet* 210–15 (2019).

cyber attacks rather than using passive strategies through surveillance.[88] Finally, there is a need for a multi-stakeholder approach to addressing cyber terrorism; this should include the government's cybersecurity strategy, the telecom service provider's role in providing affordable access to technology and services, and the technology platforms that support those services.[89] There also exists an obvious need for a comprehensive cybersecurity legislative framework that harmonizes surveillance with other security matters while taking into account fundamental rights.[90] In addition, further research is needed to evaluate the effectiveness of surveillance as a counter-terrorism tool, in order to facilitate the use of fact-based policy-making processes.[91]

[88] Maura Conway, Determining the Role of the Internet in Violent Extremism and Terrorism, 6 Stud. Conflict & Terrorism 77 (2017).
[89] Paul Rosenzweig, Cybersecurity and Public Policy, 3 J. Nat'l Sec. L. & Pol'y 1 (2009).
[90] Christopher Kuner et al., Systematic Government Access to Private-Sector Data, 2 Int'l Data Privacy L. 1 (2012).
[91] Yuchong Li, A Comprehensive Review Study of Cyber-Attacks and Cyber Security, 2021.